Polynomials with Height 1 and Prescribed Vanishing at 1

Peter Borwein and Michael J. Mossinghoff

CONTENTS

We study the minimal degree d(m) of a polynomial with all coefficients in $\{-1, 0, 1\}$ and a zero of order m at 1. We determine d(m) for m $\leq$ 10 and compute all the extremal polynomials. We also determine the minimal degree for m = 11 and m = 12 among certain symmetric polynomials, and we find explicit examples with small degree for m $\leq$ 21. Each of the extremal examples is a pure product polynomial. The method uses algebraic number theory and combinatorial computations and relies on showing that a polynomial with bounded degree, restricted coefficients, and a zero of high order at 1 automatically vanishes at several roots of unity.

1. INTRODUCTION

In this paper we study polynomials having all their coefficients in $\{-1, 0, 1\}$ and having a zero of specified multiplicity at $x = 1$. For a polynomial $f(x) = \sum_{k=0}^{d} a_k x^k$, let $H(f)$ denote the height of f,

$$H(f) = \max_{0\leq k\leq d} |a_k| .$$

Let $L(f)$ denote the length of f,

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

so if f has height 1, $L(f)$ is simply the number of monomials of f. For a positive integer m, let

$$d(m) = \min\{\deg(f) : (x-1)^m \mid f(x) \text{ and } H(f) = 1\}.$$

Certainly $d(m) \leq 2^m - 1$, since the polynomial

$$\prod_{k=0}^{m-1} \left(x^{2^k} - 1\right) \qquad (1\text{–}1)$$

has height 1. In fact, $d(m)$ satisfies the much better bounds

$$m^2 \ll d(m) \ll m^2 \log m. \qquad (1\text{–}2)$$

Keywords: polynomial; zero; $-1, 0, 1$ coefficients; pure product
AMS Subject Classification: Primary 11C08, 12D10; Secondary 11B83, 11Y99

The upper bound is proved by Bloch and Pólya [1932] using a combinatorial argument. The lower bound is a recent result of Borwein, Erdélyi, and Kós [Borwein et al. 1999]. It improves the previous lower bound of $m^2/\log m$, which follows from a theorem of Schur [1933] on the number of real zeros of a polynomial. This is a small but very interesting gap: closing it would have considerable ramification in Diophantine approximation. The quantity $d(m)$ is also studied by Mignotte [1982] and by Bombieri and Vaaler [1987] in the more general context of bounding the height of an integer polynomial with given degree and prescribed vanishing at particular algebraic numbers. In this paper, we determine the exact value of $d(m)$ for several m, and determine the extremal polynomials.

Finding a polynomial with height 1 and a zero of multiplicity m at $x = 1$ is equivalent to determining two disjoint sets of nonnegative integers

$$R = \{r_1, r_2, \dots, r_n\}, \quad S = \{s_1, s_2, \dots, s_n\}$$

satisfying

$$\sum_{k=1}^{n} r_k^i = \sum_{k=1}^{n} s_k^i$$

for every i with $0 \le i < m$: given such a pair of sets, the polynomial $\sum_{k=1}^{n}(x^{r_k} - x^{s_k})$ has the required properties. The problem of determining $d(m)$ then is equivalent to finding such a pair of sets where $\max\{t : t \in R \cup S\}$ is as small as possible. This problem is similar to the problem of Prouhet, Tarry, and Escott regarding equal sums of like powers (see [Borwein and Ingalls 1994], for instance), but in this latter problem the objective is to minimize n—more precisely, to find a solution with $n = m$.

This question is also related to a conjecture of Erdős and Szekeres regarding the supremum norm of pure product polynomials on the unit circle. A *pure product* is a polynomial of the form

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

where the e_k are positive integers. We denote such a polynomial by $[e_1, e_2, \dots, e_m]$. Let $\|f\|_\infty$ denote the supremum of the function $f(x)$ on the unit circle. Erdős and Szekeres [1959] define

$$A(m) = \min_{e_1,\dots,e_m} \big\|[e_1, \dots, e_m]\big\|_\infty$$

and prove that $\lim_{m\to\infty} A(m)^{1/m} = 1$. They have conjectured that $A(m) \gg m^c$ for any constant c. The best known upper bound on $A(m)$, due to Belov and Konyagin [1996], states that $\log A(m) \ll \log^4 m$. If $f(x)$ is a polynomial with height 1, then easily $\|f\|_\infty \le L(f) \le \deg(f) + 1$, so the Erdős–Szekeres conjecture and (1–2) together imply that the polynomials we seek cannot be pure products for m sufficiently large. It is interesting that for several small m the best known polynomials are in fact pure products.

In contrast with the cases $m \le 6$ and $m = 8$, Maltby [1997] shows that pure products cannot solve the Prouhet–Tarry–Escott problem for

$$m \in \{7, 9, 10, 11\}.$$

In all other cases, the only known lower bound is the trivial one, $L([e_1, \dots, e_m]) \ge 2m$.

Boyd [1997a; 1997b] investigates the similar problem of determining the smallest degree $d_1(m)$ of a polynomial having all coefficients in $\{-1, 1\}$ and a zero of order m at $x = 1$. In view of (1–1), Byrnes asked if $d_1(m)$ is ever smaller than $2^m - 1$. Boyd proves that the answer is yes precisely when $m \ge 6$, determines the value of $d_1(m)$ for $m \le 7$, and shows that $d_1(m) \ge \exp\bigl(\sqrt{m}(1 + o(1))\bigr)$. Some of Boyd's methods are adapted here for investigating the problem of height 1 polynomials.

In Section 2, we describe some searches for polynomials having the desired properties and determine upper bounds for $d(m)$ for $m \le 21$. In Section 3, we show that the extremal polynomials we seek must satisfy a number of divisibility conditions, and we use these requirements in Section 4 to construct an algorithm for finding these polynomials and determining $d(m)$. We discuss the results of our searches in Section 5.

2. UPPER BOUNDS

We employ two search strategies to determine upper bounds for $d(m)$ for several values of m.

2A. Lattice Reduction

We say a polynomial $f(x)$ of degree d is *reciprocal* if $f(x) = \pm x^d f(1/x)$. Let $f(x)$ be a reciprocal polynomial, and suppose we wish to determine a reciprocal multiple of $f(x)$ of low height. Select a positive integer n, and set

$$g_0(x) = x^{2n} + 1,$$
$$g_k(x) = x^{2n} + x^{2n-k} + x^k + 1 \text{ for } 1 \le k < n,$$
$$g_n(x) = x^{2n} + x^n + 1,$$

so that $\{g_k(x)\}_{k=0}^n$ is a linearly independent set of reciprocal polynomials. Let

$$h_k(x) = f(x)g_k(x)$$

for each k, and write

$$h_k(x) = \sum_{i=0}^{2n+d} c_{k,i}x^i.$$

Let $\boldsymbol{a}_k$ be the integer vector consisting of half the coefficients of $h_k(x)$,

$$\boldsymbol{a}_k = \left(c_{k,0}, c_{k,1}, \ldots, c_{k,n+\lfloor d/2\rfloor}\right).$$

Then $\{\boldsymbol{a}_0, \boldsymbol{a}_1, \ldots, \boldsymbol{a}_n\}$ spans an $(n+1)$-dimensional lattice in $\mathbb{Z}^{n+1+\lfloor d/2\rfloor}$, and we may use a lattice reduction algorithm to find a reduced basis for this lattice. The reduced basis encodes linear combinations of the $h_k(x)$, hence reciprocal multiples of $f(x)$, with low height.

We use the LLL algorithm [Lenstra et al. 1982] in Maple to perform the lattice reduction. Because our multipliers $g_k(x)$ have even degree, we try this method using both $f(x) = (x-1)^m$ and $f(x) = (x-1)^m(x+1)$, using several different values for n for each m attempted. If no multiples with height 1 are found, we employ a greedy algorithm to attempt to construct one. We first use lattice reduction to construct a few multiples of $(x-1)^m$ of moderately small height using a modest value for n, then use the method again to search for multiples of these polynomials with smaller height. After a few iterations (at most three in practice), we hope to discover a multiple of $(x-1)^m$ with height 1.

We find height 1 multiples of $(x-1)^m$ for every $m \le 18$ using this method. It is interesting that the best example found using this method is a pure product for every m except $m = 15$ (in this case, the best example is the pure product

$$[1, 2, 3, 4, 5, 6, 7, 7, 8, 9, 10, 11, 13, 17, 19]$$

multiplied by the noncyclotomic polynomial $x^{28} + x^{24} + x^{21} + x^{18} + x^{17} + x^{14} + x^{11} + x^{10} + x^7 + x^4 + 1$). This suggests a second method of searching.

2B. Pure Product Search

In this search, we look for a height 1 multiple of $(x-1)^m$ by testing various pure products of length m. Given m, let

$$A = \{1\} \cup \{p : p \text{ is prime and } p \le m+1\}$$

and

$$B = \left(\{b : 4 \le b \le m{+}1\} \setminus \max\{a : a \in A\}\right)$$
$$\cup \{b : b \equiv 1 \bmod 2 \text{ and } m{+}2 \le b \le \tfrac{3}{2}(m{+}1)\}.$$

We found considerable success testing all pure products having the form

$$\prod_{a\in A}(x^a - 1) \prod_{c\in C}(x^c - 1),$$

where C is a subset of B of cardinality $m - |A|$. The sets A and B were selected through experimentation after studying the polynomials produced by lattice reduction.

This search finds new polynomials for $m = 15$ and $m = 16$ with degree smaller than the best examples found using lattice reduction, new examples for $m = 8$ and $m = 13$ with the same degree as those found using the previous method, and new examples for $m = 19$ and $m = 21$. Despite several variations on the sets A and B, no examples were found for $m = 20$ or $m > 21$.

Table 1 lists the best examples found for each m. Each one is a pure product. Figure 1 displays a plot of d/m^2 versus m for these polynomials.

3. DIVISIBILITY CONDITIONS

Bombieri and Vaaler [1987] determine a lower bound on the degree of a polynomial having low height and prescribed vanishing at 1. They show that

$$4d \log H(f) \ge m^2(1 + o(1)), \tag{3–1}$$

provided $d \to \infty$ and $m \to \infty$ in such a way that $m/d \to 0$ and $\sqrt{d \log d}/m \to 0$. They prove this by showing that such a polynomial must be divisible by certain cyclotomic polynomials $\Phi_p(x)$ with p prime. Amoroso improves this bound, replacing the constant 4 in (3–1) with approximately 1.44, by showing that certain $\Phi_n(x)$ with n composite are also required divisors [Amoroso 1995].

In this section, we derive some explicit divisibility conditions on polynomials having height 1 and a zero of high order at 1. Let $\zeta_n = \exp(2\pi i/n)$, and

m	d	$L(f)$	$f(x)$
1	1	2	[1]
2	3	4	[1,2]
3	6	6	[1,2,3]
4	11	8	[1,2,3,5]
5	15	12	[1,2,3,4,5]
6	22	12	[1,2,3,4,5,7]
7	30	20	[1,2,3,4,5,7,8]
8	41	24	[1,2,3,4,5,7,8,11]
	41	28	[1,2,3,5,6,7,8,9]
9	48	28	[1,2,3,4,5,6,7,9,11]
10	61	32	[1,2,3,4,5,6,7,9,11,13]
11	69	44	[1,2,3,4,5,6,7,8,9,11,13]
12	93	52	[1,2,3,4,5,6,7,9,11,13,15,17]
13	112	50	[1,2,3,4,5,6,7,9,11,13,15,17,19]
	112	60	[1,2,3,5,6,7,8,9,11,11,13,17,19]
	112	74	[1,2,3,5,5,7,8,9,11,12,13,17,19]
14	120	64	[1,2,3,4,5,6,7,8,9,11,13,15,17,19]
15	141	72	[1,2,3,4,5,6,7,9,10,11,13,14,16,17,23]
16	159	84	[1,2,3,4,5,7,7,9,10,11,12,13,16,17,19,23]
17	185	100	[1,2,3,4,5,6,7,9,10,11,13,14,16,17,19,23,25]
18	207	104	[1,2,3,4,5,6,7,9,10,11,13,15,16,17,19,21,23,25]
19	245	112	[1,2,3,4,5,6,7,8,9,11,13,15,17,19,21,23,25,27,29]
21	294	130	[1,2,3,4,5,6,7,9,10,11,13,15,16,17,19,21,23,25,27,29,31]

TABLE 1. Height 1 multiples of $(x-1)^m$ with smallest known degree.

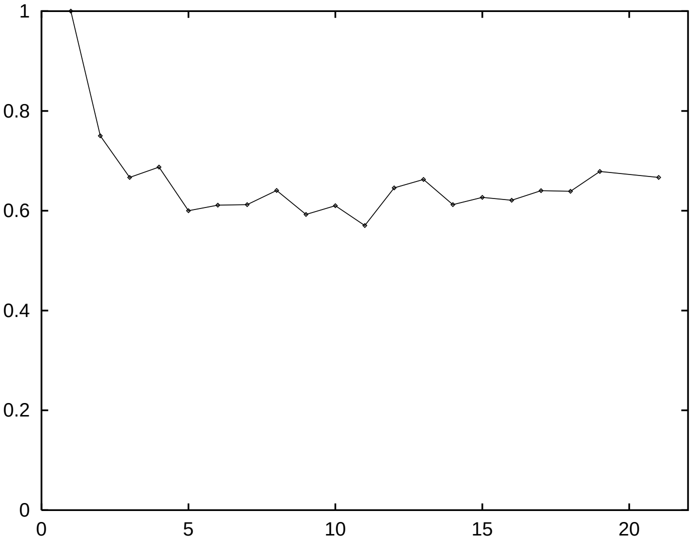

FIGURE 1. d/m^2 versus m for height 1 multiples of $(x-1)^m$ of smallest known degree.

let $N(\alpha)$ denote the norm of the algebraic number α. The first result is essentially the same as [Boyd 1997a, Theorem 1], and appears in essence in the proof of [Bombieri and Vaaler 1987, Theorem 6].

Theorem 3.1. *If* $(x-1)^m \,|\, f(x)$ *and* p *is a prime number satisfying*

$$\frac{\log p}{p-1} > \frac{\log L(f)}{m}$$

then $\Phi_p(x) \,|\, f(x)$.

Proof. Since $N(\zeta_p - 1) = p$, we have $p^m \,|\, N(f(\zeta_p))$, so if $f(\zeta_p) \neq 0$, then $|N(f(\zeta_p))| \geq p^m$. By the triangle inequality, $|N(f(\zeta_p))| \leq L(f)^{p-1}$, so $f(\zeta_p) \neq 0$ implies that $\log(p)/(p-1) \leq \log(L(f))/m$. This proves the theorem. □

Using the formulas $N(\zeta_{p^k}-1) = p$ and $N(\Phi_{p^i}(\zeta_{p^k})) = p^{\varphi(p^i)}$ for $1 \leq i < k$, one may prove more generally that

$$\frac{\log p}{p^{k-1}(p-1)} > \frac{\log L(f)}{m + p^{k-1} - 1}$$

implies that $\Phi_{p^k}(x) \,|\, f(x)$.

We require two well-known facts from algebraic number theory.

Lemma 3.2. *Let* m *be a positive integer and* p *a prime number, and let* $q = \lfloor m/(p-1) \rfloor$. *Then* $p^q \,|\, (\zeta_p - 1)^m$ *in the ring* $\mathbb{Z}[\zeta_p]$.

Lemma 3.3. *If* $f(x)$ *is a polynomial with integer coefficients and* p *is a prime number, then* $N(f(\zeta_p)) \equiv f(1)^{p-1} \bmod p$.

The proof of Lemma 3.2 may be found for example in [Boyd 1997b]. Lemma 3.3 is immediate from the proof of [Edwards 1977, Exercise 4.2.6]. We use these results to prove the following theorems concerning required cyclotomic divisors.

Theorem 3.4. *Suppose* $f(x)$ *is a polynomial having degree* d, *height* 1, *and a zero of order* m *at* $x = 1$. *Let* $p \leq m+1$ *be an odd prime number, and let* $q = \lfloor m/(p-1) \rfloor$.

(i) *If* $q = 1$ *and* $d \leq (p^2-5)/2$ *then* $\Phi_p(x) \,|\, f(x)$.
(ii) *If* $q > 1$ *and* $d \leq p(p^q+1)/2 - 2$ *then* $\Phi_p(x) \,|\, f(x)$.

Proof. Suppose $q = 1$. Write $f(x) = \sum_{k=0}^{d} a_k x^k$, and

$$f(\zeta_p) = \sum_{i=0}^{p-1} A_i \zeta_p^i, \quad A_i = \sum_{j \equiv i \bmod p} a_j. \tag{3–2}$$

Since $H(f) = 1$ and $d+1 \le (p^2-3)/2$, it follows that

$$|A_i| \le \begin{cases} \frac{1}{2}(p+1) & \text{if } 0 \le i \le \frac{1}{2}(p-5), \\ \frac{1}{2}(p-1) & \text{if } \frac{1}{2}(p-3) \le i \le p-1. \end{cases}$$

Using the fact that $\zeta_p^{p-1} = -\sum_{i=0}^{p-2} \zeta_p^i$, we write $f(\zeta_p)$ in terms of the standard integral basis:

$$f(\zeta_p) = \sum_{i=0}^{p-2} B_i \zeta_p^i, \quad B_i = A_i - A_{p-1}. \tag{3–3}$$

By Lemma 3.2, we have $p \,|\, B_i$ for each i. If $|A_{p-1}| < (p-1)/2$, then $|B_i| \le |A_i| + |A_{p-1}| < p$, hence $B_i = 0$ for each i, and $f(\zeta_p) = 0$. Suppose then without loss of generality that $A_{p-1} = -(p-1)/2$. Then $A_i \in \{(p+1)/2, -(p-1)/2\}$ for each i. Since $f(1) = 0$, we have $\sum_{i=0}^{p-1} A_i = 0$, and therefore exactly $(p-1)/2$ of the A_i must equal $(p+1)/2$, and the remaining $(p+1)/2$ must be $-(p-1)/2$. This is impossible, since at most $(p-3)/2$ of the A_i may equal $(p+1)/2$.

Now suppose $q > 1$, and let A_i and B_i be as above. We have $|A_i| \le (p^q+1)/2$ for $0 \le i \le p-2$, and $|A_{p-1}| \le (p^q-1)/2$. Since $p^q \,|\, B_i$ for each i, we deduce in the same way that $|A_{p-1}| < (p^q-1)/2$ implies $B_i = 0$ for each i. On the other hand, if $A_{p-1} = -(p^q-1)/2$, then $A_i \in \{(p^q+1)/2,\ -(p^q-1)/2\}$ for each i, and clearly $\sum_{i=0}^{p-1} A_i \ne 0$, a contradiction. □

By strengthening the condition on p slightly, we can weaken the condition on the degree and obtain a stronger result.

Theorem 3.5. *Suppose $f(x)$ is a polynomial having degree d, height 1, and a zero of order m at $x = 1$. Let $p \le m$ be a prime number, and let $r = \lfloor (m-1)/(p-1) \rfloor$. If $d \le p^{r+1} - p$ then $\Phi_p(x) \,|\, f(x)$.*

Proof. Let

$$f(\zeta_p) = \sum_{i=0}^{p-1} A_i \zeta_p^i = \sum_{i=0}^{p-2} B_i \zeta_p^i$$

as in (3–2) and (3–3). Suppose first that $d < p^{r+1} - p$. Then $|A_i| \le p^r - 1$ for each i, and we may assume without loss of generality that $A_{p-1} \le 0$. Then the definition of the B_i and Lemma 3.2 imply that B_i lies in $\{0, p^r\}$ for each i. Let $b_i = B_i/p^r$, and define $w(x) = \sum_{i=0}^{p-2} b_i x^i$. Then $N(f(\zeta_p)) = p^{r(p-1)} N(w(\zeta_p))$, but $p^m \,|\, N(f(\zeta_p))$, so $p \,|\, N(w(\zeta_p))$. Using Lemma 3.3, we conclude $p \,|\, w(1)$. Since $\deg(w) \le p-2$ and $w(x)$ has $\{0,1\}$ coefficients, we must have that $w(x) = 0$. Thus $\Phi_p(x) \,|\, f(x)$.

If $d = p^{r+1} - p$, we need only consider the case $|A_0| = p^r$. Because $|A_i| < p^r$ for $i > 0$ and $p^r \,|\, B_i$ for each i, we must have $A_i = 0$ for $i > 0$. But then $|f(1)| = p^r$. □

We remark that using Theorem 3.5 and the prime number theorem it is straightforward to prove that $d(m) > (\frac{1}{2} - \varepsilon) m^2 / \log m$ for $m > m_0(\varepsilon)$, for arbitrary positive ε. Of course, the lower bound (1–2) is substantially stronger.

Next, we obtain a condition for the fourth cyclotomic polynomial.

Theorem 3.6. *Let $f(x)$ and m be as in the previous theorem. If $m \ge 2$ and $d \le 2^{\lfloor (m+3)/2 \rfloor} - 2$ then $\Phi_4(x) \,|\, f(x)$.*

Proof. Suppose $m \ge 2$ and $d < 2^{\lfloor (m+3)/2 \rfloor} - 2$. Then $L(f) < 2^m$, so $\Phi_2(x) \,|\, f(x)$ by Theorem 3.1. Because $(i-1)^2 = -2i$ and $(i-1)(i+1) = -2$, we conclude that $2^{\lfloor (m+1)/2 \rfloor} \,|\, f(i)$ in $\mathbb{Z}[i]$. But

$$\max\{|\operatorname{Re} f(i)|, |\operatorname{Im} f(i)|\} \le \lceil (d+1)/2 \rceil,$$

so $2^{\lfloor (m+1)/2 \rfloor} > d/2 + 1$ implies that $f(i) = 0$.

Suppose that $d = 2^{\lfloor (m+3)/2 \rfloor} - 2$ and $f(i) \ne 0$. Then $|\operatorname{Re} f(i)| = 2^{\lfloor (m+1)/2 \rfloor}$ and $\operatorname{Im} f(i) = 0$. Assuming f to be monic, we have

$$f(x) = \sum_{k=0}^{d/2} x^{2k} + x g(x^2),$$

where $g(x)$ has $\{-1, 0, 1\}$ coefficients and $\deg(g) \le d/2 - 1$, so $|g(1)| \le d/2$. But $f(1) = 0$ implies that $g(1) = -d/2 - 1$, a contradiction. □

The next theorem summarizes the required cyclotomic divisors of the polynomials we seek for several m, when the polynomial has degree bounded by that of the best known examples from Table 1.

Theorem 3.7. *For each m in the following table, if $f(x)$ is a polynomial with height 1, a zero of order m at $x = 1$, and degree $d \le d_0(m)$, then $\Phi_n(x) \,|\, f(x)$ for each n in the set $R(m)$.*

m	$d_0(m)$	$R(m)$
3	6	$\{2,3\}$
4	11	$\{2,5\}$
5	15	$\{2,3,5\}$
6	22	$\{2,3,5,7\}$
7	30	$\{2,3,4,5,7\}$
8	41	$\{2,3,5,7\}$
9	48	$\{2,3,4,5,7\}$
10	61	$\{2,3,4,5,7,11\}$
11	69	$\{2,3,4,5,7,11\}$
12	92	$\{2,3,4,5,7,11,13\}$

Proof. Theorem 3.1 guarantees $n = 2$ for each m in the table, $n = 3$ for $6 \le m \le 12$, and $n = 5$ for $m = 11$ and 12. Theorem 3.4 yields $n = 5$ for $m = 8$, 9, and 10, and $n = 7$ for $m = 6$ and 12. Theorem 3.5 supplies $n = 3$ for $m = 3$, $n = 5$ for $m = 5$, $n = 7$ for $m = 7$ and 8, and $n = 11$ for $m = 11$ and 12. Theorem 3.6 adds $n = 4$ for $m = 7$ and $9 \le m \le 12$.

For $m = 5$ and $n = 3$, Theorem 3.1 covers every case except $d = 15$ and $L(f) = 16$. We may discard this case, since [Boyd 1997a] shows that a polynomial with $\{-1,1\}$ coefficients and a zero of order 5 at $x = 1$ must have degree at least 31.

Three cases remain for $n = 5$. Using (3–2) and (3–3) again, write $f(\zeta_5) = \sum_{i=0}^{4} A_i\zeta_5^i = \sum_{i=0}^{3} B_i\zeta_5^i$, and assume $A_4 \le 0$. For $m = 4$ and $d \le 11$, we have that $|A_i| \le 3$ for $i = 0$ or 1 and $|A_i| \le 2$ for $i = 2$, 3, or 4. Since $5 \mid B_i$ for each i, either $A_i = 0$ for each i, or $A_0 = A_1 = 3$ and $A_2 = A_3 = A_4 = -2$. In the latter case, $f(x) = 1+x-x^2-x^3-x^4+x^5+x^6-x^7-x^8-x^9+x^{10}+x^{11}$, and this polynomial does not have a zero of order 4 at $x = 1$. For $m = 6$ and $d \le 22$, we have $|A_i| \le 5$ for $i \in \{0,1,2\}$ and $|A_i| \le 4$ for $i \in \{3,4\}$, so $B_i \in \{-5,0,5\}$ for $i \in \{0,1,2\}$ and $B_i \in \{0,5\}$ for $i \in \{3,4\}$. Let $b_i = B_i/5$, and write $w(x) = \sum_{i=0}^{3} b_ix^i$. Since $5^6 \mid N(f(\zeta_5))$, we have $25 \mid N(w(\zeta_5))$, and testing the 108 possibilities for $w(x)$ reveals that only two have this property: $w(x) = 0$ and $w(x) = 1-x-x^2+x^3$. In the latter case, $A_4 = \sum_{i=0}^{3} b_i = 0$, so $A_3 = 5$, which is not allowed. Hence $\Phi_5(x) \mid f(x)$. The analysis for $m = 7$ is similar: we determine that $B_i \in \{-5,0,5,10\}$ for each i, and $5^7 \mid N(f(\zeta_5))$ implies that $f(\zeta_5) = 0$.

A similar argument yields $n = 7$ for $m = 10$ and $m = 11$. The case $n = 7$ for $m = 9$ is somewhat more complicated. As above, we find we must determine all polynomials $w(x) = \sum_{i=0}^{5} b_ix^i$ with $b_i \in \{-1,0,1,2\}$ having $343 \mid N(w(\zeta_7))$. There are exactly eight such polynomials, and this implies that $f(\zeta_7) = 0$ or $\pm 7\zeta_7^i(1+\zeta_7-\zeta_7^2+\zeta_7^3-\zeta_7^4-\zeta_7^5)$ for some i. In the latter case, for a given i all of the coefficients a_k of $f(x)$ are determined except for those with $k \equiv i+6 \pmod 7$, and these coefficients must sum to zero. Therefore, there are $7\sum_{j=0}^{3}\binom{7}{2j}\binom{2j}{j} = 2751$ possibilities for $f(x)$ with $f(\zeta_7) \ne 0$. Using Maple, we verify that none of these polynomials has a zero of order 9 at $x = 1$.

A different argument is required for the remaining two cases. For $n = 11$ and $m = 10$, Theorem 3.4 guarantees $\Phi_{11}(x) \mid f(x)$ for $d \le 58$. Suppose $59 \le d \le 61$, and let $j = d-59$. Proceeding as above, we find that $f(\zeta_{11}) \ne 0$ implies that $A_{10} = -5$ and $A_i \in \{-5,6\}$ for $0 \le i \le 9$, so five of the A_i are 6, and the other six are -5. This yields $\binom{5+j}{j}6^j$ exceptional polynomials for each j, a total of 793 polynomials. None has a zero at $x = 1$ of order greater than 2.

Finally, for $n = 13$, $m = 12$, and $d \le 92$, we have $|A_i| \le 8$ for $i = 0$ or 1, and $|A_i| \le 7$ for $2 \le i \le 12$. As above, we find that $f(\zeta_{13}) \ne 0$ implies that six of the A_i are -7 and the remaining seven are 6. A simple counting argument shows that there are 145 233 455 136 such polynomials, and a program checking each one determines that none has a zero at $x = 1$ with order greater than 6. □

Last, the following conditions on $f(x)$ are occasionally useful.

Theorem 3.8. *Let $f(x)$ and m be as above.*

(i) $L(f) \ge 2m$.
(ii) *If $\Phi_2(x)\Phi_4(x) \mid f(x)$ then $2^{\lceil m/4\rceil} \mid f(\zeta_8)$.*
(iii) *If $\Phi_3(x) \mid f(x)$ then $3^{\lceil (m-3)/6\rceil} \mid f(\zeta_9)$.*

Proof. Part (i) is an elementary result in the Prouhet–Tarry–Escott problem [Borwein and Ingalls 1994]. Part (ii) is proved by noting that $2 \mid (\zeta_8-1)^4$ and $\zeta_8^4-1 = -2$, and part (iii) follows from observing that $3 \mid (\zeta_9-1)^6$ and $3 \mid (\zeta_9-1)^3(\zeta_9^3-1)$. □

4. THE ALGORITHM

Given positive integers m and d, our algorithm determines all polynomials $f(x)$ having $\deg(f) = d$, $H(f) = 1$, and $(x-1)^m \mid f(x)$. Our method has two principal steps.

Step 1. Compute the product of the required factors of any such $f(x)$, reduced modulo 2. For $m \leq 12$, use Theorem 3.7 to calculate

$$r(x) \equiv (x-1)^m \prod_{n \in R(m)} \Phi_n(x) \bmod 2.$$

Step 2. For each $g(x)$ having $\{0,1\}$ coefficients with $\deg(g) = d - \deg(r)$ and $g(0) = 1$, let

$$h(x) \equiv g(x) r(x) \bmod 2.$$

Search for polynomials $f(x)$ with $\{-1,0,1\}$ coefficients satisfying $f(x) \equiv h(x) \bmod 2$ and

$$(x-1)^m \,|\, f(x).$$

The required factors of $f(x) = \sum_{k=0}^{d} a_k x^k$ enforce several relations on the coefficients. The zero of order m at $x = 1$ implies

$$\sum_{k=0}^{d} \binom{k}{i} a_k = 0, \quad 0 \leq i < m, \tag{4–1}$$

and for each prime p for which $\Phi_p(x)$ must divide $f(x)$, we have

$$\sum_{k \equiv i \bmod p} a_k = 0, \quad 0 \leq i < p. \tag{4–2}$$

In fact, we also obtain (4–2) with $p = 4$ for several m.

In Step 2, suppose $h(x) = \sum_{k=0}^{d} \alpha_k x^k$. We use the conditions (4–1) and (4–2) in two ways to reduce the number of polynomials $f(x)$ we must test for this $h(x)$. Both of these techniques are adapted from methods used in [Boyd 1997a; 1997b]. First, let p_0 be the largest prime p for which $\Phi_p(x)$ is a required divisor of $f(x)$, define $S_j = \{k : \alpha_k \neq 0 \text{ and } k \equiv j \bmod p_0\}$ for $0 \leq j < p$, and let $n_j = |S_j|$. By (4–2), half the coefficients of $f(x)$ indexed by the elements of a set S_j must be 1 and the other half must be -1. Thus, assuming that the leading coefficient of $f(x)$ is 1, the number of polynomials to test is

$$\frac{1}{2} \prod_{j=0}^{p_0 - 1} \binom{n_j}{n_j/2}.$$

We use the revolving door algorithm [Nijenhuis and Wilf 1978] to enumerate all subsets of cardinality $n_j/2$ of the S_j. To minimize the overhead associated with nesting up to p_0 levels of revolving door routines, we arrange the S_j so that the smallest sets are used in the outermost levels and the largest in the innermost levels.

Second, we use these equations to solve for some of the unknown coefficients. Let l be a nonnegative integer to be chosen later, and select l integers k_1, k_2, …, k_l with $0 \leq k_i < d$ and l equations from (4–1) and (4–2) according to the following constraints.

1. For each i, $\alpha_{k_i} = 1$, and the coefficient of a_{k_i} in the ith equation selected is nonzero.
2. If $l \leq m$, then select the equations $0 \leq i < l$ from (4–1); otherwise, select all the equations from (4–1) and $l - m$ equations from (4–2).
3. When choosing the k_i, first select every element from the set S_j of largest cardinality, then select from sets of successively smaller cardinality. This greatly reduces the number of sign combinations we must test for $h(x)$, while allowing us to use the revolving door algorithm to test a reduced number of sign combinations in all but at most one of the remaining congruence classes. If only a portion of some set S_j is selected, we use a Gray code [Nijenhuis and Wilf 1978] to enumerate sign combinations for the remaining coefficients in this set.
4. Use at most $p - 1$ equations for each p for which (4–2) is valid. (Using p equations yields a linear dependency with the equation $i = 0$ of (4–1).)

Let C be the $l \times (d+1)$ coefficient matrix associated with the selected equations, and let M be the $l \times l$ matrix consisting of columns k_1, k_2, …, k_l of C. If M is nonsingular, compute

$$M^{-1} = \frac{1}{q} Q,$$

where Q is an integer matrix and q is a positive integer. If M is singular, then discard a redundant relation and repeat the computation. Since any $m \times m$ submatrix of the coefficient matrix of the equations in (4–1) is nonsingular, we are assured of finding an invertible matrix eventually. Finally, compute $B = QC$ and write $B = (b_{ij})$.

Now set $a_k = 0$ if $\alpha_k = 0$ or $k = k_i$ for some i, and set $a_d = 1$. For each tested assignment of ±1 on the remaining coefficients, compute

$$\beta_j = \sum_{k=0}^{d} a_k b_{jk} \tag{4–3}$$

for $1 \leq j \leq m'$, where m' is a integer to be selected later satisfying $1 \leq m' \leq m$. By using the revolving door method, the value of each β_j for the current polynomial being tested differs from that of the previous polynomial in a simple way: if a_r was changed from -1 to $+1$ and a_s from $+1$ to -1, then we may update the value of β_j using

$$\beta_j \leftarrow \beta_j + 2(b_{jr} - b_{js}).$$

The updating operation is similar for those coefficients enumerated using a Gray code: if a_r changes sign, then we perform $\beta_j \leftarrow \beta_j \pm 2b_{jr}$ for each j, where the sign is given by the new value of a_r.

If $\beta_j = \pm q$ for $1 \leq j \leq m'$, compute (4–3) and test if $\beta_j = \pm q$ for $m' < j \leq m$. If all of these conditions are satisfied, set $a_{k_j} = \beta_j / q$ for $1 \leq j \leq l$, and $f(x)$ is a solution.

We find that choosing $m' = 2$ and $l = l(h) = \max\{0, L(h) - 22\}$ minimizes the total computation time. Choosing m' to be this small discards most $f(x)$ after only a small amount of computation, and choosing l this way appears to strike the right balance between solving for some coefficients and enumerating the possibilities for others.

Finally, our algorithm uses Theorem 3.8 to avoid degenerate cases and to avoid testing $h(x)$ under other special circumstances. Also, for $m \geq 11$ we avoid testing $h(x)$ if $L(g)$ is odd and $L(h') < 2^{m-1}$, since in this case $(x+1)^2 \,|\, f(x)$ by Theorem 3.1.

We implement our algorithm in C++, using the NTL library [Shoup 1998] for big integer arithmetic in the computation of the matrices to avoid overflow.

5. RESULTS

We use our algorithm to compute $d(m)$ and determine all of the extremal polynomials for $m \leq 10$. For $m \leq 3$, it is clear that Table 1 lists the best polynomials.

For $m = 4$, we use Step 1 of our algorithm to compute $r(x) = x^9 + x^5 + x^4 + 1$. By Theorem 3.8, any solution must have at least eight terms, so $d = 9$ is impossible. For $d = 10$, there is only one candidate polynomial modulo 2 in Step 2, $h(x) \equiv (x+1)r(x) \bmod 2$. We discard this possibility because $L(h) = 6$. For $d = 11$, there are only two choices for $g(x)$: $x^2 + 1$ and $x^2 + x + 1$. Both yield polynomials with length 8. Thus, by Theorem 3.1, if $f(x)$ is a solution congruent to one of these polynomials modulo 2, then $\Phi_3(x) \,|\, f(x)$. Therefore, the only possibility for $d = 11$ is $(x-1)^4 \Phi_2(x) \Phi_3(x) \Phi_5(x)$. This is precisely the pure product for $m = 4$ listed in Table 1.

For $5 \leq m \leq 10$, our algorithm finds that Table 1 again contains all of the extremal polynomials. Table 2 summarizes our computations, listing for each m the total number of polynomials $h(x)$ considered having degree d, with $d(m-1) < d \leq d(m)$, the number of height 1 polynomials $f(x)$ tested by changing signs of coefficients of the $h(x)$, and the approximate time required to perform the computations on a Silicon Graphics MIPS R10000 computer.

m	$d(m)$	$\#h(x)$	$\#f(x)$	Time
5	15	2	12	< 1 s
6	22	3	44	< 1 s
7	30	216	8824	< 1 s
8	41	507 180	603 212 632	1 h
9	48	16 502 311	39 597 473 936	60 h
10	61	4 944 018	25 387 052 272	70 h

TABLE 2. Summary of complete search.

Computing $d(m)$ for $m > 10$ appears to be too difficult using our method, but we can obtain some partial information by searching a restricted set of polynomials. We say a polynomial $f(x) = \sum_{k=0}^{d} a_k x^k$ is *weakly symmetric* if $|a_k| = |a_{d-k}|$ for each k. We use our program to search for weakly symmetric multiples of $(x-1)^m$ for $m = 11$ and $m = 12$ by amending Step 2 of our algorithm to test only symmetric polynomials $g(x)$. We verify that there is exactly one weakly symmetric monic polynomial of degree $d \leq 69$ having height 1 and a zero of order 11 at $x = 1$, and we determine that there are no weakly symmetric multiples of $(x-1)^{12}$ with height 1 and degree less than 93. A summary of the computations required to verify these facts appears in Table 3.

The preponderance of pure product polynomials as extremal examples in our results might lead one

m	$\#h(x)$	$\#f(x)$	Time
11	82 835	686 706 480	2.5 hours
12	5 491 989	213 959 621 244	4 weeks

TABLE 3. Summary of weakly symmetric search.

to suspect that the Erdős–Szekeres conjecture is not true. While we hesitate to make this speculation based on the limited data obtained here, it would be interesting to gather additional data on this conjecture. To this end, we mention a few natural problems suggested by this research.

1. Determine if $d(20) < 294$.
2. Find an m so that at least one polynomial with height 1, a zero of order m at 1, and degree $d(m)$ is not a pure product.
3. Prove or disprove that for each m there exists a reciprocal polynomial with height 1, a zero of order m at 1, and degree $d(m)$.

ACKNOWLEDGMENTS

We thank David Boyd for helpful discussions on this topic, Michael Filaseta for suggesting improvements to the manuscript, and the referees for helpful comments.

REFERENCES

[Amoroso 1995] F. Amoroso, "Polynomials with prescribed vanishing at roots of unity", *Boll. Un. Mat. Ital. B* (7) **9**:4 (1995), 1021–1042.

[Belov and Konyagin 1996] A. S. Belov and S. V. Konyagin, "An estimate of the constant term of a nonnegative trigonometric polynomial with integer coefficients", *Mat. Zametki* **59** (1996), 627–629. In Russian; translation in *Math. Notes* **59** (1996), 451–453.

[Bloch and Pólya 1932] S. Bloch and G. Pólya, "On the roots of certain algebraic equations", *Proc. London Math. Soc.* **33** (1932), 102–114.

[Bombieri and Vaaler 1987] E. Bombieri and J. D. Vaaler, "Polynomials with low height and prescribed vanishing", pp. 53–73 in *Analytic number theory and Diophantine problems* (Stillwater, OK, 1984), edited by A. C. Adolphson et al., Prog. Math. **70**, Birkhäuser, Boston, 1987.

[Borwein and Ingalls 1994] P. Borwein and C. Ingalls, "The Prouhet–Tarry–Escott problem revisited", *Enseign. Math.* (2) **40**:1-2 (1994), 3–27.

[Borwein et al. 1999] P. Borwein, T. Erdélyi, and G. Kós, "Littlewood-type problems on $[0,1]$", *Proc. London Math. Soc.* (3) **79**:1 (1999), 22–46.

[Boyd 1997a] D. W. Boyd, "On a problem of Byrnes concerning polynomials with restricted coefficients", *Math. Comp.* **66**:220 (1997), 1697–1703.

[Boyd 1997b] D. W. Boyd, "On a problem of Byrnes concerning polynomials with restricted coefficients, II", preprint, 1997.

[Edwards 1977] H. M. Edwards, *Fermat's last theorem: A genetic introduction to algebraic number theory*, Graduate Texts in Math. **50**, Springer, New York, 1977.

[Erdős and Szekeres 1959] P. Erdős and G. Szekeres, "On the product $\prod_{k=1}^{n}(1-z^{a_k})$", *Acad. Serbe Sci. Publ. Inst. Math.* **13** (1959), 29–34.

[Lenstra et al. 1982] A. K. Lenstra, H. W. Lenstra Jr., and L. Lovász, "Factoring polynomials with rational coefficients", *Math. Ann.* **261**:4 (1982), 515–534.

[Maltby 1997] R. Maltby, "Pure product polynomials and the Prouhet–Tarry–Escott problem", *Math. Comp.* **66**:219 (1997), 1323–1340.

[Mignotte 1982] M. Mignotte, "Estimations élémentaires effectives sur les nombres algébriques", pp. 364–371 in *Journées Arithmétiques* 1980 (Exeter, 1980), edited by J. V. Armitage, London Math. Soc. Lecture Note Ser. **56**, Cambridge Univ. Press, Cambridge, 1982.

[Nijenhuis and Wilf 1978] A. Nijenhuis and H. S. Wilf, *Combinatorial algorithms for computers and calculators*, 2nd ed., Academic Press, New York, 1978.

[Schur 1933] I. Schur, "Untersuchungen über algebraische Gleichungen, I: Bemerkungen zu einem Satz von E. Schmidt", *Sitzungsber. Preuss. Akad. Wiss., Phys.-Math. Kl.* (1933), 403–428. Reprinted as pp. 240–265 in his *Gesammelte Abhandlungen*, vol. 3, Springer, Berlin, 1973.

[Shoup 1998] V. Shoup, "NTL: A library for doing number theory", software, 1998. See www.shoup.net/ntl.

Peter Borwein, Department of Mathematics and Statistics, Simon Fraser University, Burnaby, B.C., Canada V5A 1S6 (pborwein@cecm.sfu.ca)

Michael J. Mossinghoff, Department of Mathematics, UCLA, Los Angeles, California 90095, United States (mjm@math.ucla.edu)

Received March 22, 1999; accepted in revised form December 29, 1999