MATHEMATICS OF COMPUTATION
Volume 66, Number 220, October 1997, Pages 1697–1703
S 0025-5718(97)00892-2

ON A PROBLEM OF BYRNES CONCERNING POLYNOMIALS WITH RESTRICTED COEFFICIENTS

DAVID W. BOYD

ABSTRACT. We consider a question of Byrnes concerning the minimal degree n of a polynomial with all coefficients in $\{-1, 1\}$ which has a zero of a given order m at $x = 1$. For $m \leq 5$, we prove his conjecture that the monic polynomial of this type of minimal degree is given by $\prod_{k=0}^{m-1}(x^{2^k} - 1)$, but we disprove this for $m \geq 6$. We prove that a polynomial of this type must have $n \geq e^{\sqrt{m}(1+o(1))}$, which is in sharp contrast with the situation when one allows coefficients in $\{-1, 0, 1\}$. The proofs use simple number theoretic ideas and depend ultimately on the fact that $-1 \equiv 1 \pmod 2$.

1. INTRODUCTION

This paper deals with polynomials with all coefficients in $\{-1, 1\}$. In particular, we are interested in the minimum degree of such a polynomial which has an m-fold zero at the point $x = 1$. In [4], Byrnes asks for a proof or disproof of the conjecture that the polynomial of this type with minimal degree is

$$B_m(x) = \prod_{k=0}^{m-1}(x^{2^k} - 1), \tag{1}$$

which has degree $2^m - 1$. He states that " ... even a proof that the degree of such a P must be exponential in m would be of interest". This problem arises in connection with the design of antenna arrays and notch filters [3].

One of our results here is that Byrne's conjecture is true for $m \leq 5$ and false for all $m \geq 6$. The latter result is proved by exhibiting a polynomial of degree 47 for which $m = 6$. We are also able to show that if $n = \deg(P)$, then $n \geq \exp(\sqrt{m}(1 + o(1)))$, which combines with the example (1) to show that there are constants $c_1 > 0$ and $c_2 < \infty$ for which

$$c_1 e^{\sqrt{m}} \leq n \leq c_2 e^m. \tag{2}$$

This result is in sharp constrast with the situation where the coefficients are all in $\{-1, 0, 1\}$. Here the best result known is that there are constants $c_3 > 0$ and $c_4 < \infty$ for which

$$c_3 m^2 \leq n \leq c_4 m^2 \log m. \tag{3}$$

Received by the editor November 16, 1995.
1991 *Mathematics Subject Classification.* Primary 11C08, 12D10; Secondary 94A99, 11Y99.
Key words and phrases. Polynomial, zero, antenna array, notch filter.
This research was supported by a grant from NSERC .

The existence of the polynomials giving the upper bound in (3) follows from the box principle by a familiar argument (as in [2] or [5]). The lower bound in (3) is a recent result of Borwein, Erdélyi and Kós [2].

The case of $\{-1,1\}$-coefficients is apparently more rigid than that of $\{-1,0,1\}$-coefficients. This is reflected in our methods which are more number theoretical than combinatorial. As Peter Borwein has pointed out to me, the difference between the two situations is not due to the relative size of the two sets $\{-1,1\}$ and $\{-1,0,1\}$ since our results apply equally well to polynomials with coefficients restricted to $\{-3,-1,1,3\}$, for example.

Let $\mathcal{P}(N)$ denote the set of polynomials with all coefficients in $\{-1,1\}$, leading coefficient 1, and with $\deg(P) = N-1$. (It will be clear that N is a more natural variable than $\deg(P)$). Let $\mathcal{P}(N,m)$ denote the subset of $\mathcal{P}(N)$ consisting of P divisible by $(x-1)^m$ (or by some higher power of $x-1$). Our main results give lower bounds for N in terms of m for $P \in \mathcal{P}(N,m)$.

The proof of all of our results depends on the obvious fact that if $P \in \mathcal{P}(N)$, then $P(x) \equiv 1 + x + \cdots + x^{N-1} \pmod 2$. In spite of the simplicity of this idea, it gives us the useful results of Lemmas 1 to 3 which lead easily to the lower bounds of Corollary 2 and Theorem 1. For example, we find that if $m \geq 2^k$, then N must be divisible by 2^{k+1}, in keeping with the observed high divisibility of N by 2 in $B_m(x)$. However, a consequence of Lemma 2 is that if we consider the set of N which are not divisible by a given prime p then $N \geq (p^{1/(p-1)})^m$ showing that the only possible remedy for exponential growth of N with m is to have N divisible by as many primes as possible.

The proof of Byrne's conjecture for $m \leq 5$ requires a certain amount of computation. In particular, it is necessary to enumerate some of the sets $\mathcal{P}(N,m)$. Since the cardinality of $\mathcal{P}(N)$ is 2^{N-1}, it is clear that such computations must be designed carefully. Our most successful approach uses two algorithms from Nijenhuis and Wilf, [6], namely the Gray code ordering of all the subsets of an N-set and the "revolving door" ordering of all the k-subsets of an N-set, where here $k = N/2$. This is described in §3. We naturally have carried out more computations than necessary for the proof of Theorem 4. In particular, we show that the counterexample for $m = 6$ with $N = 48$ has the minimal degree. We do not know if it is the only example of that degree but it is the only symmetric (reciprocal) example. A complete enumeration of $\mathcal{P}(32,4)$, which has 39 elements, shows that only one of these has $m = 5$, namely the canonical example $B_5(x)$. By contrast, $\mathcal{P}(40,4)$ has 2207 elements, only one of which has $m = 5$.

2. The main results

Let us write $A_N(x) = 1 + x + \cdots + x^{N-1} = (x^N - 1)/(x-1)$ so that if $P \in \mathcal{P}(N)$, then $P \equiv A_N \pmod 2$. We define $A_0(x) = 0$.

Lemma 1. *If $P \in \mathcal{P}(N)$ and $Q \in \mathcal{P}(M)$ and if $Q(x)$ divides $P(x)$, then M divides N.*

Proof. Suppose $N = qM + r$, with $0 \leq r < M$. By the division algorithm for polynomials over the integers, we have the obvious identity

$$A_N(x) = A_M(x)A_q(x^M) + A_r(x). \tag{4}$$

Since $P(x) \equiv A_N(x)$ and $Q(x) \equiv A_M(x)$ modulo 2, we thus have

$$P(x) \equiv Q(x)A_q(x^M) + A_r(x) \pmod 2. \tag{5}$$

If $Q(x)$ divides $P(x)$ over $\mathbb{Z}$, then it must divide $P(x)$ over $\mathbb{Z}/(2)$. But (4) shows that the remainder on division of $P(x)$ by $Q(x)$ over $\mathbb{Z}/(2)$ is $A_r(x)$, which vanishes modulo 2 only when $r = 0$. Thus $M|N$. □

Corollary 1. *Let p be prime and let ζ_p denote a pth root of unity. If $P \in \mathcal{P}(N)$ and $P(\zeta_p) = 0$, then p divides N.*

Proof. The minimal polynomial of ζ_p over the integers is $A_p(x)$ which is in $\mathcal{P}(p)$. The condition that $P(\zeta_p) = 0$ is equivalent to $A_p(x)$ dividing $P(x)$, which by Lemma 1 requires that $p|N$. □

Lemma 2. *If $\mathcal{P}(N, m)$ is nonempty and if 2^k is the highest power of 2 dividing N, then $m \le 2^k - 1$.*

Proof. Write $N = 2^k M$ with M odd. Suppose $P \in \mathcal{P}(N, m)$. Then, writing $t = x - 1$, the Taylor expansion of P at 1 is of the form

$$P(1 + t) = c_m t^m + c_{m+1} t^{m+1} + \dots. \tag{6}$$

On the other hand, modulo 2, we have

$$\begin{aligned} P(1+t) \equiv A_N(1+t) &= t^{-1}((1+t)^N - 1) = t^{-1}((1+t)^{2^k M} - 1) \\ &\equiv t^{-1}((1+t^{2^k})^M - 1) \equiv t^{2^k - 1} + \dots. \end{aligned} \tag{7}$$

Comparing (6) and (7) we see that $m \le 2^k - 1$. □

Corollary 2. *If $\mathcal{P}(N, m)$ is nonempty and if $m \ge 2^k$, then 2^{k+1} divides N.*

Theorem 1. *If $\mathcal{P}(N, m)$ is nonempty and if p is a prime which does not divide N, then $N \ge (p^{1/(p-1)})^m$.*

Proof. If $P \in \mathcal{P}(N, m)$, then $P(x) = (x - 1)^m Q(x)$ for some polynomial Q with integer coefficients. By Corollary 1, $P(\zeta_p) \ne 0$. Hence $0 \ne P(\zeta_p) = (\zeta_p - 1)^m Q(\zeta_p)$. Computing the norm of $P(\zeta_p)$ by taking the product over all conjugates of ζ_p (i.e. over all roots of $A_p(x)$), we obtain an equation in non-zero integers:

$$0 \ne \prod P(\zeta_p^j) = \pm p^m \prod Q(\zeta_p^j), \tag{8}$$

using the well-known fact that $\prod(1 - \zeta_p^j) = A_p(1) = p$. Estimating $|P(\zeta_p^j)| \le N$ and $|\prod Q(\zeta_p^j)| \ge 1$ gives $N^{p-1} \ge p^m$, which completes the proof. □

Theorem 2. *If $\mathcal{P}(N, m)$ is nonempty, then $N \ge \exp(\sqrt{m}(1 + o(1)))$.*

Proof. Let x be a parameter to be chosen shortly. Then $\prod_{p \le x} p = e^{\theta(x)} = e^{x(1+o(1))}$, where $\theta(x)$ is Chebyshev's theta function and the final statement is equivalent to the Prime Number Theorem, [1, p.79]. If $N < \prod_{p \le x} p$, then clearly there is some $p \le x$ for which p does not divide N. Such a p will be guaranteed if we take $x = \log N(1 + o(1))$ and then by Theorem 1,

$$N \ge (p^{1/(p-1)})^m \ge x^{m/x}. \tag{9}$$

Taking logs we have

$$(\log N)^2 \ge m(\log\log N)(1 + o(1)) \ge m(1 + o(1)), \tag{10}$$

which gives the desired inequality. □

Remark 1. It is easy to obtain a more explicit result than given in Theorem 1. One simply replaces the use of the prime number theorem by an inequality of Chebyshev's type $\theta(x) > ax$, to obtain $N > \exp(\sqrt{m/a})$ by the same argument. Explicit values of a may be found in [7]. Note that what is actually proved in (10) is $m \le (\log N)^2/\log\log N(1+o(1))$ so we could have claimed a slightly better asymptotic result, e.g. $N \ge \exp(\sqrt{m\log m}(1+o(1)))$. However, for values of N and m which are useful in practice, it is preferable to use the results of Lemma 2 and Theorem 1 directly (as in §3).

Theorem 3. *For $m \le 5$, the polynomial $B_m(x)$ of (1) is the unique monic polynomial of smallest degree with an m-fold zero at 1.*

Proof. The case $m = 1$ is obvious. If $m = 2$, then N is divisible by 4 by Corollary 2, hence $N = 4$ is the minimal possible. Since the required example must be divisible by $(x-1)^2$, it is clear that $B_2(x)$ is the only choice. For $m = 3$, N must be divisible by 4 by Corollary 2, but $N = 4$ would mean $P(x) = (x-1)^3$ which does not have all coefficients in $\{-1, 1\}$. Thus $N = 8$ is minimal for $m = 3$ so $B_3(x)$ is of the minimal degree. Enumerating $\mathcal{P}(8, 3)$ shows that $B_3(x)$ is unique (for more details see §3).

For $m = 4$, Corollary 2 implies that N is divisible by 8. But $N = 8$ is ruled out by Theorem 1 since $3 \nmid N$ implies $N \ge (3^{1/2})^4 = 9$. Thus $N = 16$ is minimal and hence $B_4(x)$ is a minimal degree example. An enumeration of $\mathcal{P}(16, 4)$ shows it is unique.

For $m = 5$, we again have $8|N$ and hence must consider $N = 16, 24$ and 32. An enumeration shows that $\mathcal{P}(N, 5)$ is empty for $N = 16$ and 24 and consists of $B_5(x)$ for $N = 32$. □

Theorem 4. *Byrnes' conjecture is false for $m \ge 6$. For $m = 6$, the minimal value of N is* 48.

Proof. In §3, we exhibit a reciprocal polynomial $P(x)$ in $\mathcal{P}(48, 6)$ showing that $B_6(x)$ is not of minimal degree. An enumeration shows that $\mathcal{P}(N, 6)$ is empty for $N = 8, 16, 24, 32$, and 40 and hence $N = 48$ is minimal for $m = 6$. The polynomial $P(x)B_{m-6}(x^{48})$ is in $\mathcal{P}(3\times 2^{m-2}, m)$ for $m \ge 7$ showing that for $m \ge 7$, the minimal $N \le 3 \times 2^{m-2} < 2^m$. □

3. Computations

We now describe the methods used to enumerate some of the sets $\mathcal{P}(N, m)$. The largest such set we completely enumerated was $\mathcal{P}(40, 4)$ which took just under one week of computation on a fast workstation. Since $|\mathcal{P}(40)| = 2^{39} \approx .5 \times 10^{12}$, it should be clear that an efficient method of enumeration is necessary. We first introduce some notation: if $P(x) = \sum_{j=1}^{N} a(j)x^{j-1}$, then $P(1+t) = \sum_{i=1}^{N} c(i)t^{i-1}$ with

$$c(i) = \sum_{j=1}^{N} a(j)\binom{j-1}{i-1}. \tag{11}$$

It is clear that if $P(1) = 0$, then N must be even and have $N/2$ coefficients equal to $+1$ and $N/2$ equal to -1. To specify P completely, we need only know the subset of j for which $a(j) = -1$ and hence an $N/2$-subset of the $(N-1)$-set $\{1, \ldots, N-1\}$ (since we take $a(N) = 1$ always). Thus, we can immediately reduce the search from

$|\mathcal{P}(N)| = 2^{N-1}$ to $|\mathcal{P}(N,1)| = \binom{N-1}{N/2}$ polynomials. For $N = 40$, we thus need only examine about $.7 \times 10^{11}$ polynomials rather than $.5 \times 10^{12}$. In general one saves a factor approximately $\sqrt{\pi N/2}$.

Nijenhuis and Wilf have given a "revolving door" algorithm in which the k-subsets of $\{1, \ldots, N\}$ are enumerated in a list $S_1, S_2, \ldots$ which is such that $S_1 = \{1, \ldots, k\}$ and each set differs from the previous set by the addition of one element *in* and the omission of an element *out*. In fact, they supply a FORTRAN subroutine NXKSRD for this purpose in [6, p.34].

We can use this to enumerate $\mathcal{P}(N,m)$ as follows: having initialized a_j to be -1 for $1 \le j \le N/2$ and $+1$ otherwise, initialize c_i for $1 \le i \le m$ using (11). Generate the $N/2$-subsets of $\{1, \ldots, N-1\}$ using NXKSRD. The $P(x)$ corresponding to S_{k+1} differs from that corresponding to S_k by having $a(in) = -1$ and $a(out) = 1$. Hence the $c(i)$ can be updated by the simple rule

$$c(i) \leftarrow c(i) - 2\binom{in-1}{i-1} + 2\binom{out-1}{i-1}, \tag{12}$$

for $1 \le i \le m$. If one stores the array $2\binom{j-1}{i-1}$, each step (12) requires only two additions. We need only test whether $c(i) = 0$ for $1 \le i \le m$ and output the corresponding polynomials. In fact we computed $c(i)$ for $1 \le i \le m+2$ at each stage, in order to more easily recognize elements of $\mathcal{P}(N, m+1)$ and $\mathcal{P}(N, m+2)$ within $\mathcal{P}(N,m)$.

This method is easily adapted to the enumeration of $\mathcal{P}_s(N,m)$ consisting of the symmetric (or reciprocal) polynomials in $\mathcal{P}(N,m)$. In this case $P(x) = x^{N/2}Q(x) + Q^*(x)$, where $Q \in \mathcal{P}(N/2)$ and $Q(1) = 0$. (Here $Q^*(x) = x^{N/2-1}Q(1/x)$.) Thus this requires an enumeration of the $N/4$-subsets of an $(N/2-1)$-set.

If $P(x)$ is antisymmetric, then $P(x) = x^{N/2}Q(x) - Q^*(x)$, where now it is not necessarily the case that $Q(1) = 0$. In this case, we enumerate all subsets of the corresponding $(N/2-1)$-set using the Gray code order as described in [6, p.18]. Here the formula corresponding to (10) requires only a single addition and the generation of each subset is about twice as fast as with the revolving door algorithm, but one enumerates $2^{N/2-1}$ sets rather than $\binom{N/2-1}{N/4}$. We denote the set of antisymmetric polynomials in $\mathcal{P}(N,m)$ by $\mathcal{P}_a(N,m)$.

It is easily seen that if $P(x)$ is symmetric, then the order of vanishing of P at $x = 1$ is even while if $P(x)$ is antisymmetric, the order of vanishing is odd.

Let $C(N,m)$, $C_s(N,m)$ and $C_a(N,m)$ be the cardinalities of $\mathcal{P}(N,m)$,$\mathcal{P}_s(N,m)$ and $\mathcal{P}_a(N,m)$, respectively. For the proof of Theorem 2, we computed $C(8,2) = 4$ and $C(8,3) = 1$, the one element here being $B_3(x)$ of (1). Similarly, $C(16,3) = 7$ and $C(16,4) = 1$, the one element here being $B_4(x)$. We have $C(24,4) = 8$, with 6 of these being symmetric. But $C(24,5) = 0$, a fact used in the proof of Theorem 2. For $N = 32$, we have $C(32,4) = 39$ and $C(32,5) = 1$. The unique element of $\mathcal{P}(32,5)$ is $B_5(x)$ which is also the only antisymmetric member of $\mathcal{P}(32,4)$. Of the remaining 38 elements of $\mathcal{P}(32,4)$, 20 are symmetric.

For $N = 40$, we have $C(40,4) = 2207$, $C_s(40,4) = 258$ and $C(40,5) = 1 = C_a(40,4)$. The unique element of $\mathcal{P}(40,5)$ has coefficients

$$a(21), \ldots, a(40) = 1, -1, -1, 1, -1, -1, 1, 1, -1, 1, 1, 1, 1, -1, -1, -1, -1, -1, 1, 1.$$

This $P(x)$ factors as $(x-1)^5(x+1)^2\Phi_5(x)\Phi_{10}(x)P_{20}(x)$, where $\Phi_k(x)$ is the minimal polynomial of the primitive kth roots of 1 and P_{20} is an irreducible polynomial of degree 20 having coefficients

$$1, 3, 5, 7, 8, 9, 9, 9, 8, 7, 7, 7, 8, 9, 9, 9, 8, 7, 5, 3, 1.$$

From $P(x)$, we can construct $x^{40}P(x) - P(x)$, an element of $\mathcal{P}(80, 6)$. It is interesting that 33 of the polynomials in $\mathcal{P}(40, 4)$ have $c(5) = \pm 20$. These can be concatenated in pairs to yield at least $33 \times 32 = 1056$ elements of $\mathcal{P}(80, 5)$. Similarly, we can concatenate $P(x)$ with $B_5(x)$ to yield $x^{32}P(x) \pm B_5(x)$ each of which is in $\mathcal{P}(72, 5)$.

We remarked above that the computation of $\mathcal{P}(40, 4)$ required about one week of computation on a fast workstation. The computation of $\mathcal{P}(48, 5)$ thus would require about 234 weeks or about 4 1/2 years of computation using the same algorithm. Thus, for $N > 40$, we were content to enumerate $\mathcal{P}_s(N, m)$ and $\mathcal{P}_a(N, m)$. For example $C_a(48, 5) = 41$ while $C_s(48, 5) = C_s(48, 6) = 1$ which provides the counterexample of Theorem 3. The unique element $P(x)$ of $\mathcal{P}_s(48, 6)$ has coefficients

$$\begin{aligned} &a(25), \ldots, a(48) \\ &\quad = -1, -1, 1, 1, -1, -1, -1, 1, 1, -1, 1, 1, 1, 1, 1, -1, -1, 1, -1, -1, -1, -1, 1, 1. \end{aligned}$$

It factors as $(x-1)^6(x+1)^3\Phi_3(x)\Phi_4(x)\Phi_6(x)\Phi_8(x)P_{28}(x)$, where $P_{28}(x)$ is an irreducible polynomial of degree 28 with positive (and unimodal) coefficients. We can use P and the elements of $\mathcal{P}_a(48, 5)$ together with $\mathcal{P}(40, 5)$ to construct many elements of $\mathcal{P}(88, 5)$, and of course an element of $\mathcal{P}(96, 7)$ as in Theorem 4.

For $N = 56$, we have $C_s(56, 6) = 0$, $C_a(56, 5) = 71$ and $C_a(56, 7) = 0$ so there are no symmetric or antisymmetric P with $N = 56$ and $m > 5$. For $N = 64$, we have $C_s(64, 6) = 3$, one of these being $B_6(x)$. The other two have irreducible factors of degrees 52 and 54 respectively. We have $C_a(64, 5) = 619$ and $C_a(64, 7) = 0$. For $N = 72$, we have $C_s(72, 6) = 44$, $C_a(72, 5) = 14870$ and $C_a(72, 7) = 0$. For $N = 80$, $C_s(80, 6) = 50$.

We can apply Lemma 2 and Theorem 1 to give upper bounds on the maximal m for which $\mathcal{P}(N, m)$ is non-empty. Let us denote this value by $m^*(N)$. Then

$$m^*(N) \le \min(2^k - 1, \log N / \log(p^{1/(p-1)})), \tag{13}$$

where 2^k is the largest power of 2 dividing N and p is the smallest prime not dividing N. It is interesting to ask whether $N = 96$ is the smallest N with $m = 7$. By Lemma 2 we need only consider N divisible by 8. From (13), we obtain $m^*(N) \le 7$ for $N = 56, 64, 72, 80$ and 88, so $5 \le m^*(56) \le 7$, $6 \le m^*(64) \le 7$, $6 \le m^*(72) \le 7$, $6 \le m^*(80) \le 7$ and $5 \le m^*(88) \le 7$, where the lower bounds come from the constructions mentioned in the previous paragraphs . On the other hand, for those N divisible by 3×2^4, we must use $p = 5$ in (13) and combining this with Theorem 4 gives only $6 \le m^*(48) \le 9$ and $7 \le m^*(96) \le 11$, which leaves open the intriguing but unlikely possibility that $N = 48$ could yield $m = 7$.

References

[1] T.M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, Berlin and New York, 1976. MR **55:**7892

[2] P. Borwein, T. Erdélyi & G. Kós, *Polynomials with Restricted Coefficients* (to appear).

[3] J.S. Byrnes & D.J. Newman, *Null Steering Employing Polynomials with Restricted Coefficients*, IEEE Trans. Antennas and Propagation **36** (1988), 301–303.

[4] J.S. Byrnes, *Problems on Polynomials with Restricted Coefficients Arising from Questions in Antenna Array Theory*, Recent Advances in Fourier Analysis and Its Applications (J.S. Byrnes & J.F. Byrnes, eds.), Kluwer Academic Publishers, Dordrecht, 1990, pp. 677–678.

[5] M. Mignotte, *Sur les polynômes divisibles par* $(X-1)^n$, Arithmetix **2** (1980), 28–29.

[6] A. Nijenhuis & H.S. Wilf, *Combinatorial Algorithms*, Academic Press, Orlando, 1978. MR **88a:**68076

[7] J.B. Rosser & L. Schoenfeld, *Approximate formulas for some functions of prime number theory*, Illinois J. Math **6** (1962), 69–94. MR **25:**1139

Department of Mathematics, University of British Columbia, Vancouver, B.C., Canada V6T 1Z2

E-mail address: boyd@math.ubc.ca