ON A PROBLEM OF BYRNES CONCERNING POLYNOMIALS WITH RESTRICTED COEFFICIENTS, II

DAVID W. BOYD

ABSTRACT. As in the earlier paper with this title, we consider a question of Byrnes concerning the minimal length $N^*(m)$ of a polynomial with all coefficients in $\{-1, 1\}$ which has a zero of a given order m at $x = 1$. In that paper we showed that $N^*(m) = 2^m$ for all $m \leq 5$ and showed that the extremal polynomials for were those conjectured by Byrnes, but for $m = 6$ that $N^*(6) = 48$ rather than 64. A polynomial with $N = 48$ was exhibited for $m = 6$, but it was not shown there that this extremal was unique. Here we show that the extremal is unique. In the previous paper, we showed that $N^*(7)$ is one of the 7 values $48, 56, 64, 72, 80, 88$ or 96. Here we prove that $N^*(7) = 96$ without determining all extremal polynomials. We also make some progress toward determining $N^*(8)$. As in the previous paper, we use a combination of number theoretic ideas and combinatorial computation. The main point is that if ζ_p is a primitive pth root of unity where $p \leq m + 1$ is a prime, then the condition that all coefficients of P be in $\{-1, 1\}$, together with the requirement that $P(x)$ be divisible by $(x - 1)^m$ puts severe restrictions on the possible values for the cyclotomic integer $P(\zeta_p)$.

1. INTRODUCTION

Let $\mathcal{P}(N)$ denote the set of polynomials with all coefficients in $\{-1, 1\}$, leading coefficient 1, and with length $L(P) = N$ so that $\deg(P) = N - 1$. As usual, $L(P)$ denotes the sum of the absolute values of the coefficients of P which here is just the number of nonzero coefficients of P. As we saw in [Bo], this is a more natural parameter than the degree. We will use the notation $P(x) = \sum_{i=1}^{N} a_i x^{i-1}$ for the coefficients of $P(x)$.

We are interested in the minimum value of N for which a $P \in \mathcal{P}(N)$ has an m-fold zero at the point $x = 1$. 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 $x - 1$). For given N, let $m^*(N)$ denote the largest m for which $\mathcal{P}(N, m)$ is nonempty. Similarly, for given m, let $N^*(m)$ denote the smallest N for which $\mathcal{P}(N, m)$ is nonempty.

In [By] Byrnes asked for a proof or disproof of the conjecture that $N^*(m) = 2^m$, which would be attained for

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

which has $N = 2^m$. In [Bo] we showed that this conjecture is true for $m \leq 5$ but false for all $m \geq 6$ and that in fact $N^*(6) = 48$. As part of the proof, we exhibited a symmetric (i.e., reciprocal) polynomial with $N = 48$ and $m = 6$ which had been found by an exhaustive search of all symmetric polynomials with $N = 48$ vanishing at $x = 1$. This is the unique symmetric polynomial in $\mathcal{P}(48, 6)$ but it was not shown that it was the unique polynomial in $\mathcal{P}(48, 6)$. Indeed, with the algorithm used in [Bo], it would have taken roughly five years of computation on the workstation used there (a SUN Sparcstation 10) to exhaustively search $\mathcal{P}(48, 1)$ to determine all elements of $\mathcal{P}(48, 6)$. All computing times quoted in this paper will refer to computations on this machine. A rough guide to the speed of the algorithms used is that a search of a set of 10^{10} polynomials requires one day's computation on this machine.

In this paper we use a number of new ideas to improve the algorithm and the bounds of [Bo]. Recall that in [Bo], we were able to get bounds on m in terms of N for $P \in \mathcal{P}(N, m)$ by proving that if p is a prime which does not divide N and if ζ_p is a primitive pth root of unity, then $P(\zeta_p) \neq 0$. Then using the fact that $(\zeta_p - 1)^m$ divides $P(\zeta_p)$, and taking norms gives the inequality

$$(2) \qquad\qquad N^{p-1} \geq |\mathrm{Norm} P(\zeta_p)| \geq p^m = \mathrm{Norm}(\zeta_p - 1)^m.$$

Here $\mathrm{Norm} P(\zeta_p) = \prod_{j=1}^{p-1} P(\zeta_p{}^j)$.

Here we improve on this idea by observing that we know much more about $P(\zeta_p)$ and $(\zeta_p - 1)^m$ than simply their norms. In fact (see Lemma 3), in the ring $\mathbb{Z}[\zeta_p]$, $(\zeta_p - 1)^m$ is divisible by p^r for $r = \lfloor m/(p-1) \rfloor$, and hence $P(\zeta_p)$ is divisible by p^r in $\mathbb{Z}[\zeta_p]$. On the other hand, if we write $P(\zeta_p) = B_1 + B_2 \zeta_p + \cdots + B_{p-1} \zeta_p{}^{p-2}$, the integers $B_1, \ldots, B_{p-1}$ satisfy some severe restrictions since the coefficients of $P(x)$ lie in $\{-1, 1\}$. In particular, we know the parity of the B_j and bounds on their magnitude. Combining this with the fact that p^r divides B_j for each j, the number of possibilities for $P(\zeta_p)$ can be shown to be rather small. With a suitable choice of the prime p, this can sometimes be used to show that $\mathcal{P}(N, m)$ is empty or else to reduce the enumeration of $\mathcal{P}(N, m)$ to a feasible computation. Note that in contrast to (2), we can get useful information from this approach even if p divides N. Also, the method extends to other classes of polynomials with restricted coefficients, e.g., the case of coefficients in $\{-1, 0, 1\}$.

An important point is that given a possible value $\beta = P(\zeta_p)$, there is a simple explicit way to enumerate the $P \in \mathcal{P}(N, 1)$ for which $P(\zeta_p) = \beta$. Indeed, if N_j is the number of elements in the finite arithmetic progression $j, j + p, j + 2p, \ldots$ with $j + np \leq N$, then there are K_j with $0 \leq K_j \leq N_j$ so that K_j of the coefficients a_{j+np} of $P(x)$ must be -1 and the remaining $N_j - K_j$ must be $+1$. Thus $P(x)$ is determined by selecting a K_j-subset of the N_j-set $\{j, j + p, \ldots, j + (N_j - 1)p\}$ for all $j = 1, 2, \ldots, p$. An efficient way to do this enumeration is to use the revolving door algorithm of Nijenhuis and Wilf [NW], much as in [Bo].

For example, consider $N = 48$ and $m = 6$. If $P \in \mathcal{P}(48, 6)$, then we can show that $P(\zeta_3) = 0$ and hence that $x^3 - 1$ divides $P(x)$. The subset of $P \in \mathcal{P}(48, 1)$ for which $x^3 - 1$ divides $P(x)$ is roughly $1/15$ the size of $\mathcal{P}(48, 1)$; hence, it could be enumerated in about 15 weeks of computation. (In Section 4, we describe how some elementary linear algebra can reduce this to about 1 week of computation).

A better choice of p in this case is $p = 5$. If $P \in \mathcal{P}(48, 6)$, we will see that $\pm P(\zeta_5)$ is one of the three possibilities

$$\beta_1 = -10 + 10\zeta_5^2 - 5\zeta_5^3 + 5\zeta_5^4,$$

$$\beta_2 = 10 - 10\zeta_5 + 10\zeta_5{}^2 - 5\zeta_5{}^3 - 5\zeta_5{}^4,$$

or

$$\beta_3 = 10\zeta_5 - 5\zeta_5{}^3 - 5\zeta_5{}^4.$$

Indeed, if $m \geq 7$, only $P(\zeta_5) = \beta_1$ is possible. There are only 326592 polynomials $P \in \mathcal{P}(48, 1)$ which satisfy $\pm P(\zeta_5) = \beta_1$, and a few seconds of computation shows that none of these have $m = 7$, i.e., that $|\mathcal{P}(48, 7)| = 0$. The enumeration of $P \in \mathcal{P}(48, 1)$ for which $\pm P(\zeta_5) = \beta_k$ for $k = 2$ and 3 takes about 12 minutes and shows that $|\mathcal{P}(48, 6)| = 1$, so that the polynomial found in [Bo] is the unique element of $\mathcal{P}(48, 6)$.

In a similar way, we can use $p = 5$ to enumerate $\mathcal{P}(48, 5)$. In this case we find that there are ten possibilities for $\pm P(\zeta_5)$, in addition to $\beta_1, \beta_2, \beta_3$, most of which can be handled with a few seconds of computation. The only possibility that leads to a substantial computation is $\pm P(\zeta_5) = -5\zeta_5{}^3 + 5\zeta_5{}^4$ which is satisified by 97 polynomials $P \in \mathcal{P}(48, 5)$, as one checks after 39 hours of computation. The end result is that $|\mathcal{P}(48, 5)| = 102$.

Generally, the most useful prime to use in a given situation is the smallest p which does not divide N. However, sometimes larger primes can be used effectively. For example, because $48 = 7^2 - 1$, it turns out that $p = 7$ is quite effective for $P \in \mathcal{P}(48, 7)$. In this case one can show that $P(\zeta_7) = B_1 + B_2\zeta_7 + \cdots + B_6\zeta_7{}^5$, where 3 of the B_j must be $+7$ and 3 must be -7. Thus there are only 200 possible P to check and none of these has order of vanishing at $x = 1$ higher than 3, again showing $|\mathcal{P}(48, 7)| = 0$.

Another simple idea can be used in conjunction with the above to reduce the computation even further. Choose m of the coefficients of P and use linear algebra to solve the equations $P(1) = P'(1) = \cdots = P^{(m-1)}(1) = 0$ for these m coefficients. If these are chosen appropriately, we can still use the same basic algorithm but on a smaller set of coefficients, saving a factor of close to $1/2^m$. (We do not quite achieve this factor for reasons that will be clear when the more detailed description of the algorithm is given in Section 4). For example, with $N = 48$, $m = 5$ and $p = 3$, this reduces 15 weeks of computation to slightly over 2 weeks and provides a second verification of the result $|\mathcal{P}(48, 5)| = 102$.

In [Bo] we showed that the only possibilities for $N^*(7)$ are $48, 56, 64, 72, 80, 88$, and 96. We have just described how one rules out $N = 48$. By using the prime $p = 2$, we can rule out three of the remaining possibilities rather easily. In [Bo] we observed that if 2^k is the largest power of 2 dividing N, then the order m of vanishing of $P \in \mathcal{P}(N)$ at $x = 1$ satisfies

(3) $$m \leq 2^k - 1.$$

The proof of this result depended on the obvious fact that if $P \in \mathcal{P}(N)$, then $P(x) \equiv 1 + x + \cdots + x^{N-1} \pmod{2}$. Thus the factorization of P over $\mathbb{F}_2$ is known. For a certain range of N and m, we show here that if $P \in \mathcal{P}(N, m)$, then $P(-1) = 0$, i.e., $x + 1$ divides P. In this case (3) can be improved to $m \leq 2^k - 2$. If $2^k = 8$, this will allow us to show that $m \leq 6$ if $8 \| N$ and $N < 2^m$ (Lemma 1). This rules out

$N = 56, 72$, and 88 as candidates for $m = 7$, leaving only the possibilities $N = 64$, 80, and 96. Note that this depends on the lucky fact that 7 is one less than a power of 2 and hence will not be useful again until one is considering $m = 15$.

In [Bo] we had shown that $6 \leq m^*(64) \leq 7$ and that $6 \leq m^*(80) \leq 7$. Here we show that $m^*(64) = 6$ and $m^*(80) = 6$ by considering the possibilities for $P(\zeta_3)$. Combined with the results for $N = 48$ described above, this shows that $N^*(7) = 96$. Two polynomials in $\mathcal{P}(96, 7)$ can be constructed from the unique element P of $\mathcal{P}(48, 6)$, namely $(x^{48} - 1)P(x)$ and $(x - 1)P(x^2)$. It is unlikely that these exhaust $\mathcal{P}(96, 7)$, but an enumeration of this set does not seem feasible using the current methods.

The methods developed here allow one to narrow the possibilities for $N^*(8)$ to $N = 96, 144, 160, 176$, or 192. We illustrate this by computing bounds for $m^*(N)$ for those multiples of 16 in $96 \leq N \leq 256$. In some cases, the bounds determine $m^*(N)$, e.g., $m^*(128) = 7$, but do not allow an enumeration of $\mathcal{P}(N, m^*(N))$.

Some other values of $m^*(N)$ can be determined by combining the constructions given in [Bo] with the methods of this paper. For example we show that $m^*(56) = 5$ without determining the entire set $\mathcal{P}(56, 5)$, and we show that $m^*(72) = 6$ without determining $\mathcal{P}(72, 6)$. As mentioned above, we show that $m^*(64) = 6$ and briefly describe a computation which shows that $|\mathcal{P}(64, 6)| = 3$. In this case all the polynomials are symmetric and had already been determined in [Bo].

2. High order vanishing at 1
implies vanishing at certain roots of unity

Thoughout the paper, we will let 2^k denote the largest power of 2 dividing N and will assume that $P(1) = 0$ so that N must be even. We write $\Phi_q(x)$ for the qth cyclotomic polynomial, i.e., the minimal polynomial over $\mathbb{Q}$ of the primitive qth roots of unity. Since $P(x) \equiv (x^N - 1)/(x - 1) \pmod 2$, the complete factorization of P over $\mathbb{F}_2$ is known (see [LN]). In particular, if $2^k \| N$, then the product of the linear divisors of $P \pmod 2$ is $(x + 1)^{2^k - 1}$. Also, if p is a prime divisor of N, then $\Phi_p(x) = (x^p - 1)/(x - 1)$ divides $P \pmod 2$, although this will not in general be an irreducible factor (see [LN, pp. 63–66]). Another obvious fact that we use without comment below is that $|P(x)| \leq N$ if $|x| = 1$ by the triangle inequality.

We begin with some results that depend on slight extensions of the ideas of [Bo].

Lemma 1. *If $P \in \mathcal{P}(N, m)$ and if $N < 2^m$, then $P(-1) = 0$. Furthermore, if $m < 2^k - 1$ and if $N < 2^{m+1}$, then $P(-1) = 0$.*

Proof. Write $P(x) = (x - 1)^m Q(x)$. If $Q(-1) \neq 0$, then $|Q(-1)| \geq 1$ and we have $N \geq |P(-1)| = |(-2)^m Q(-1)| \geq 2^m$, contrary to the assumption $N < 2^m$. Hence $Q(-1) = 0$ and so $P(-1) = 0$.

Now consider the case $m < 2^k - 1$. As discussed above, $P(x) \pmod 2$ is divisible by $(x + 1)^{2^k - 1}$ and since $P(x) \equiv (x + 1)^m Q(x)$ it follows that $Q(x) \pmod 2$ must be divisible by $x + 1$. That is $Q(-1)$ is an even integer. Hence $P(-1) = (-2)^m Q(-1)$ is divisible by 2^{m+1}. However, $|P(-1)| \leq N$ so if $N < 2^{m+1}$, we must have $P(-1) = 0$. $\qquad\square$

Corollary 1. *If $P \in \mathcal{P}(N, m)$ and if $N < 2^m$, then $m \leq 2^k - 2$.*

Proof. From Lemma 1, $P(x) = (x - 1)^m (x + 1) R(x)$ for some polynomial $R(x) \in \mathbb{Z}[x]$. Hence $P(x) \pmod 2$ is divisible by $(x + 1)^{m+1}$. But the product of all linear factors of $P(x) \pmod 2$ is $(x + 1)^{2^k - 1}$ and hence $m + 1 \leq 2^k - 1$. $\qquad\square$

Remark 1. In particular, if $\mathcal{P}(N,7)$ is nonempty and $N < 128$, then N must be divisible by 16. This rules out $N = 56, 72$, and 88 as candidates for $m = 7$. Using the lower bounds established in [Bo], we now have $5 \leq m^*(N) \leq 6$ for $N = 56$ and 88 and $m^*(72) = 6$. We will show by a computation described below that $m^*(56) = 5$.

We observed in [Bo] that knowing the factorization of $P(x)$ over $\mathbb{F}_2$ shows that if $\Phi_p(x)$ divides $P(x)$, then p divides $P(x)$. The following is a partial converse of this.

Lemma 2. *If $P \in \mathcal{P}(N,m)$, if p is an odd prime divisor of N, and if $N^{p-1} < 2^{p-1}p^m$, then $\Phi_p(x)$ divides P.*

Proof. Since p divides N, it follows that $\Phi_p(x)$ divides $(x^N - 1)/(x - 1) \equiv P(x) \pmod{2}$; hence if ζ_p is any root of $\Phi_p(x)$, the number $P(\zeta_p) \in 2\mathbb{Z}(\zeta_p)$. Thus, $\mathrm{Norm}P(\zeta_p) = \prod_{j=1}^{p-1} P(\zeta_p{}^j)$ is an integer divisible by 2^{p-1}. Writing $P(x) = (x - 1)^m Q(x)$, we see that $\mathrm{Norm}P(\zeta_p)$ is divisible by $\mathrm{Norm}(\zeta_p - 1)^m = p^m$. Thus $\mathrm{Norm}P(\zeta_p)$ is divisible by $2^{p-1}p^m$. But

$$|\mathrm{Norm}P(\zeta_p)| = \prod_{j=1}^{p-1} |P(\zeta_p{}^j)| \leq N^{p-1} < 2^{p-1}p^m$$

by assumption, so we have $\mathrm{Norm}P(\zeta_p) = 0$, i.e., that $\Phi_p(x)$ divides $P(x)$. $\square$

Remark 2. In particular, if $N = 48$ and $m = 6$, we have $48^2 = 2304 < 2^2 3^6 = 2916$, so if $P \in \mathcal{P}(48,6)$, then $x^2 + x + 1$ divides P and hence $x^3 - 1$ divides P. The more precise discussion of $P(\zeta_3)$ in the next section will enable us to show that if $P \in \mathcal{P}(48,5)$, then $x^3 - 1$ divides P.

3. Values of P at roots of unity

In this section, assuming $P \in \mathcal{P}(N,m)$, we see what we can say about the possibilities for $P(\zeta_p)$ when p is a prime and ζ_p is a primitive pth root of unity. We will thus be working in the ring $\mathbb{Z}[\zeta_p]$. This is a familiar ring which occurs in the study of Fermat's Last Theorem [E], but here we do not need or use any deep facts about $\mathbb{Z}[\zeta_p]$. All we will need is the fact that every element of $\mathbb{Z}[\zeta_p]$, in particular $P(\zeta_p)$, can be represented in a unique way as a sum

$$(4) \qquad P(\zeta_p) = B_1 + B_2\zeta_p + \cdots + B_{p-1}\zeta_p{}^{p-2},$$

where the B_j are integers. This follows from the fact that the minimal polynomial of ζ_p, $\Phi_p(x) = x^{p-1} + \cdots + 1$, has degree $p - 1$.

Another natural, and also unique, representation of $P(\zeta_p)$ for $P \in \mathcal{P}(N,1)$ is as a sum

$$(5) \qquad P(\zeta_p) = A_1 + A_2\zeta_p + \cdots + A_p\zeta_p{}^{p-1},$$

where A_j are integers with $\sum_{j=1}^{p} A_j = 0$. To see how this comes about, notice that we can write any polynomial $P(x)$ in the form

$$(6) \qquad P(x) = \sum_{j=1}^{p} P_j(x^p)x^{j-1}.$$

Here $P_j(x) = \sum_{n=1}^{N_j} a_{j+(n-1)p} x^{n-1}$, where N_j is either $\lfloor N/p \rfloor$ or $\lceil N/p \rceil$. The N_j satisfy $N_1 \geq N_2 \geq \cdots \geq N_p$ and $\sum_{j=1}^p N_j = N$. Now using $\zeta_p{}^p = 1$ in (6) gives (5) with $A_j = P_j(1)$. Substituting $x = 1$ in (6) gives $0 = P(1) = \sum_{j=1}^p A_j$.

Using

$$(7) \qquad\qquad \zeta_p{}^{p-1} = -1 - \zeta_p - \cdots - \zeta_p{}^{p-2},$$

we see from (4) and (5) that

$$(8) \qquad\qquad B_j = A_j - A_p \quad \text{for } j = 1, \ldots, p-1,$$

so that

$$(9) \qquad\qquad \sum_{j=1}^{p-1} B_j = -pA_p.$$

Thus we can easily convert between the representations (4) and (5).

The reason that we need the representation (4) is that $P(\zeta_p) = p^r \beta$, for some $\beta \in \mathbb{Z}[\zeta_p]$, is equivalent to p^r dividing B_j for each j. It is important to realize that this is not equivalent to p^r dividing A_j for each j.

The following fact is well known but we give a simple proof for completeness.

Lemma 3. *Let $m \geq 0$ be an integer, p an odd prime, and let $r = \lfloor m/(p-1) \rfloor$. Then $(\zeta_p - 1)^m$ is divisible by p^r in $\mathbb{Z}[\zeta_p]$. That is, $(\zeta_p - 1)^m$ can be written in the form $p^r \beta$, where $\beta \in \mathbb{Z}[\zeta_p]$.*

Proof. We need only show that $(\zeta_p - 1)^{p-1}$ is divisible by p since if $m = r(p-1) + s$ we can write $(\zeta_p - 1)^m = ((\zeta_p - 1)^{p-1})^r (\zeta_p - 1)^s$ to show that $(\zeta_p - 1)^m$ is divisible by p^r. Using the binomial theorem and (7), we have

$$(10) \qquad (\zeta_p - 1)^{p-1} = \sum_{j=0}^{p-1} \binom{p-1}{j} (-1)^j \zeta_p{}^j = \sum_{j=0}^{p-2} \left((-1)^j \binom{p-1}{j} - 1 \right) \zeta_p{}^j.$$

Now check that each coefficient in the right member of (10) is divisible by p. $\qquad \square$

Example 1. Let $N = 48$, $m = 6$, and $p = 5$. Then the lengths $N_1, \ldots, N_5$ of $P_1(x), \ldots, P_5(x)$ in (6) are $10, 10, 10, 9, 9$, respectively. Since $A_j = P_j(1)$, we thus have $|A_j| \leq L(P_j)$ for $j = 1, \ldots, 5$ and $A_j \equiv N_j \pmod{2}$ so that A_j is even for $j = 1, 2, 3$ and odd for $j = 4, 5$. From (8), we thus have that B_j is odd and $|B_j| \leq 19$ for $j = 1, 2, 3$ and that B_4 is even and satisfies $|B_4| \leq 18$. Lemma 3 shows that $(\zeta_5 - 1)^m$ is divisible by 5 and hence $P(\zeta_5)$ is divisible by 5. Thus each B_j is divisible by 5 and hence $B_j \in \{\pm 5, \pm 15\}$ for $j = 1, 2, 3$ and $B_4 \in \{0, \pm 10\}$.

We also have that $\text{Norm} P(\zeta_5)$ is divisible by $\text{Norm}(\zeta_5 - 1)^m = 5^6$. Checking the 3×4^3 possibilities for $\sum_{j=1}^4 B_j \zeta_5{}^{j-1}$, we find that there are only 3 choices for $\pm P(\zeta_5)$, namely

$$\beta_1 = -10 + 10\zeta_5{}^2 - 5\zeta_5^3 + 5\zeta_5^4,$$

$$\beta_2 = 10 - 10\zeta_5 + 10\zeta_5{}^2 - 5\zeta_5{}^3 - 5\zeta_5{}^4,$$

$$\beta_3 = 10\zeta_5 - 5\zeta_5{}^3 - 5\zeta_5{}^4.$$

We have $\text{Norm}\beta_1 = 5^7$ and $\text{Norm}\beta_k = 5^6$, for $k = 2, 3$.

Since all coefficients of $P_j(x)$ are in $\{-1, 1\}$, in order to have $P_j(1) = A_j$, we must have $K_j = (N_j - A_j)/2$ coefficients equal to -1 and $N_j - K_j = (N_j + A_j)/2$ coefficients equal to $+1$. The size of the subset of $\mathcal{P}(N, 1)$ satisfying

$$\pm P(\zeta_p) = \sum_{j=1}^{p} A_j {\zeta_p}^{j-1}$$

is thus

(11)
$$\prod_{j=1}^{p} \binom{N_j}{K_j}.$$

(The restriction that P be monic is compensated for by the ambiguous $\pm$ sign except in the case $P(\zeta_p) = 0$ when (11) can be multiplied by $\frac{1}{2}$.)

Thus, for $\pm P(\zeta_p) = \beta_1$, for example, we have $(K_1, \ldots, K_5) = (10, 5, 0, 7, 2)$. From (11), the size of the set of $P \in \mathcal{P}(48, 1)$ with $\pm P(\zeta_5) = \beta_1$ is $\binom{10}{5}\binom{9}{2}^2 = 326592$. (In this case, $P(\zeta_5) = -\beta_1$ is impossible for P monic since this would require that all coefficients of $P_3(x)$ be -1, but $a_{48} = 1$ is the leading coefficient of P_3.) This set contains $\mathcal{P}(48, 7)$ since β_1 is the only possible value of $P(\zeta_5)$ with $\text{Norm} P(\zeta_5)$ divisible by 5^7. The search of this set by the methods of [Bo] for $P(x)$ divisible by $(x - 1)^7$ requires only a few seconds and shows that $|\mathcal{P}(48, 7)| = 0$. Furthermore, there are no $P(x)$ in this set divisible by $(x - 1)^6$ or $(x - 1)^5$.

For β_2, we have $(K_1, \ldots, K_5) = (0, 10, 0, 7, 7)$ so the subset of $\mathcal{P}(48, 1)$ with $\pm P(\zeta_5) = \beta_2$ is of size $\binom{9}{2}^2 = 1296$ which similarly can be searched in a few seconds for $P(x)$ divisible by $(x - 1)^6$. As one might expect, there are no such P. Nor are there any such $P(x)$ divisible by $(x - 1)^5$.

For $\pm P(\zeta_5) = \beta_3$, we have $(K_1, \ldots, K_5) = (5, 0, 5, 7, 7)$, so the size of the set to be searched is $\binom{10}{5}^2\binom{9}{2}^2 = 8.230 \times 10^7$. The search of this set for $P(x)$ divisible by $(x - 1)^6$ took 10 minutes. The only such polynomial is the one described in [Bo]. There are no other polynomials of this form divisible by $(x - 1)^5$.

Extending the above to $m = 5$ requires only the determination of those $\beta = \sum_{j=1}^{p} A_j {\zeta_p}^{j-1}$ satisfying the conditions of the first paragraph of this example and having norm divisible by 5^5. Up to sign, there are thirteen such β, of which we have already listed three. These are easily described: there are three $(A_1, \ldots, A_5)$ of the form $(10, 10, -10, -5, -5)$, there are six of the form $(-10, 0, 10, -5, 5)$, there are three of the form $(0, 0, 10, -5, -5)$, where in each case the first three entries can be permuted arbitrarily. Finally, there is $(0, 0, 0, 5, -5)$. The number of possibilities in the latter case is $\binom{10}{5}^3\binom{9}{2}^2 = 2.074 \times 10^{10}$ and the search of this set requires 39 hours of computation.

The final result is that there are 97 elements of $\mathcal{P}(48, 5)$ with $\pm P(\zeta_5) = 5{\zeta_5}^3 - 5{\zeta_5}^4$. There are 2 elements of $\mathcal{P}(48, 5)$ for each of $(A_1, \ldots, A_5) = (0, 0, 10, -5, -5)$ and $(10, 0, 0, -5, -5)$ and 1 for $(0, 10, 0, -5, -5)$ (namely the unique element of $\mathcal{P}(48, 6)$ as already described).

Example 2. $N = 48$, $m \geq 4$, and $p = 3$. Using the above technique, write $N = 48 = N_1 + N_2 + N_3$, where $N_j = 16$ for all j. Thus, we see that all A_j are even and satisfy $|A_j| \leq 16$ and hence B_j is even and $|B_j| \leq 32$ for $j = 1, 2$. Also $|B_1 - B_2| = |A_1 - A_2| \leq 32$. Since $m \geq 4$, Lemma 3 implies that 3^2 divides B_j for $j = 1, 2$ and hence we must have $B_j \in \{0, \pm 18\}$. So there are exactly four possibilities up to sign, namely $(B_1, B_2) = (0, 0), (0, 18), (18, 0)$ and $(18, 18)$

corresponding to $(A_1, A_2, A_3) = (0,0,0), (-6,12,-6), (12,-6,-6), (6,6,-12)$. The norms in the latter three cases are all 4×3^4.

This shows that if $m \geq 5$, then we must be in the first case, i.e., $P(\zeta_3) = 0$, which improves the result obtained from Lemma 2, which required $m \geq 6$. If we want to enumerate $\mathcal{P}(48, 4)$, then the enumeration for the latter three cases would require a search of size $3\binom{16}{5}^2\binom{16}{2} = 6.868 \times 10^9$ or less than one day's computation.

The size of the subset of $\mathcal{P}(48, 1)$ with $P(\zeta_3) = 0$ is $\frac{1}{2}\binom{16}{8}^3 = 1.066 \times 10^{12}$, where the factor $\frac{1}{2}$ is inserted since we can insist that P be monic. This search would require about 15 weeks of computation, which is a considerable improvement over the 5 years required to search all of $\mathcal{P}(48, 1)$ as in [Bo]. However, as a method for determining $\mathcal{P}(48, 6)$, it is considerably more than the 10 minutes required by using $p = 5$ as in Example 1. As we see in the next section, a little linear algebra can be used to reduce the search by a factor of about $1/15$.

Example 3. $N = 48$, $m \geq 6$, $p = 7$. Here $N_j = 7$ for $j = 1, \ldots, 6$ and $N_7 = 6$. Thus all B_j are odd and $|B_j| \leq 13$. By Lemma 3, if $m \geq 6$, $7|B_j$ and hence all $B_j = \pm 7$. All these 2^6 choices of β will have $7^6|\text{Norm}\beta$. If we restrict to $m \geq 7$, it turns out that $7^7|\text{Norm}\beta$ requires that $\sum_{j=1}^{6} B_j = 0$, i.e., that $A_j = B_j$ for $j = 1, \ldots, 6$ and $A_7 = 0$. Thus 3 of the A_j for $j \leq 6$ are -1 and 3 are $+1$. Since $L(P_j) = 7 = |A_j|$ for $j \leq 6$, the P_j for $j \leq 6$ are completely determined by the signs of the A_j. And since $A_7 = 0$, we have $P_7(1) = 0$. Thus

$$P(x) = \frac{x^{49} - 1}{x^7 - 1}F(x) + x^6 P_7(x^7),$$

where $F(x) = (A_1 + A_2 x + \cdots + A_6 x^5)/7$ and $\pm P_7(x)$ are in $\mathcal{P}(6, 1)$. An easy search of the 200 possibilities for F and P_7 determines that there are four such $P(x)$ which are divisible by $(x-1)^3$ but none divisible by any higher power of $x - 1$ so again $\mathcal{P}(48, 7)$ is empty.

Example 4. $N = 40$, $m = 4$, $p = 3$. Recall that in [Bo], we determined that $|\mathcal{P}(40, 4)| = 2207$ and that $|\mathcal{P}(40, 5)| = 1$ by a search of the $\frac{1}{2}\binom{40}{20} = 6.892 \times 10^{10}$ elements of $\mathcal{P}(40, 1)$. This computation took slightly over one week and was needed to show that $|\mathcal{P}(40, 6)| = 0$. Using the new method with $N = 40$, $m = 4$ and $p = 3$, we write $40 = 14 + 13 + 13$ so that A_1 is even with $|A_1| \leq 14$ and A_j is odd with $|A_j| \leq 13$ for $j = 2, 3$. Thus B_1 is odd with $|B_1| \leq 27$, B_2 is even with $|B_2| \leq 26$, and $|B_1 - B_2| \leq 27$. Since $m = 4$, we have $3^2|B_j$ by Lemma 3 and hence we find that $\pm P(\zeta_3) = 9 + 18\zeta_3 = 9\zeta_3 - 9\zeta_3^2$, with norm 3^5 or else $\pm P(\zeta_3) = 9 = 6 - 3\zeta_3 - 6\zeta_3^2$, with norm 3^4. This shows that $\mathcal{P}(40, 6)$ is empty without any further computation.

To determine $\mathcal{P}(40, 5)$, we need only consider the first possibility. In this case $(K_1, K_2, K_3) = (7, 2, 11)$, giving a total of $\binom{14}{7}\binom{13}{2}^2 = 2.088 \times 10^7$ polynomials. This requires only three minutes of computation and yields the 61 polynomials of $\mathcal{P}(40, 4)$ with $\pm P(\zeta_3) = 9\zeta_3 - 9\zeta_3^2$, one of which is the unique element of $\mathcal{P}(40, 5)$. To determine the remaining elements of $\mathcal{P}(40, 4)$, we consider the second possibility, for which $(K_1, K_2, K_3) = (10, 5, 5)$, i.e., a total of $\binom{14}{10}\binom{13}{5}^2 = 1.658 \times 10^9$ polynomials. This computation takes three hours and yields the remaining 2146 polynomials of $\mathcal{P}(40, 4)$.

Example 5. $N = 64$, $m = 6$, $p = 3$. Writing $64 = 22 + 21 + 21$ and proceeding as above, we see that if $P \in \mathcal{P}(64, 6)$, then $\pm P(\zeta_3) = 27 = 18 - 9\zeta_3 - 9\zeta_3^2$ which has

norm 3^6. This shows that $\mathcal{P}(64, 7)$ is empty and, since Byrnes' example $B_6(x)$ has $m = 6$, we have $m^*(64) = 6$ without any further computation. We know from the computations of [Bo] that there are three symmetric polynomials in $\mathcal{P}(64, 6)$.

A complete determination of $\mathcal{P}(64, 6)$ using just the information from $p = 3$ would require a search of $\binom{22}{2}\binom{21}{6}^2 = 6.802 \times 10^{11}$ polynomials or about 2 months of computation, which is certainly feasible (especially if a faster machine is used). However, it is possible to speed up this search by using information from other primes. Our methods show, for example, that if $P \in \mathcal{P}(64, 6)$, then $\pm P(\zeta_5) = 5 - 5\zeta_5 - 5\zeta_5{}^2 + 5\zeta_5{}^3$. The prime 7 can also be used. There are 26 possible values for $\pm P(\zeta_7)$. Of these, 25 of these can be eliminated by a direct search requiring about 15 hours of computation. This leaves only the possibility $\pm P(\zeta_7) = 7$. For the prime 2, we have $P(-1) = 0$ from Lemma 1. The information from the primes $2, 3, 5$, and 7 can be combined by using an extension of the linear algebra method described in the next section. A computation based on these ideas required three additional hours to determine that $|\mathcal{P}(64, 6)| = 3$, the three polynomials being the three symmetric polynomials determined in [Bo].

Example 6. $N = 80$, $m = 6$, $p = 3$. Here $80 = 27 + 27 + 26$, and we find that if $P \in \mathcal{P}(80, 7)$, then $\pm P(\zeta_3) = 27 - 27\zeta_3$, which has norm 3^7. However, in this case all coefficients of $P_0(x)$ are equal, to $+1$, say, and all coefficients of $P_1(x)$ are equal, say to -1. Thus there are only $\binom{26}{13}$ possibilities to check and a direct enumeration shows $\mathcal{P}(80, 7)$ is empty. (It is also possible to combine the information from the primes $p = 3$ and $p = 7$ to show that $\mathcal{P}(80, 7)$ is empty without an extensive computation, as was pointed out to me by Ron Ferguson.) Since we can construct elements of $\mathcal{P}(80, 6)$ from the unique element of $\mathcal{P}(40, 5)$, we have $m^*(80) = 6$. We know from the computations of [Bo] that there are exactly 50 symmetric polynomials in $\mathcal{P}(80, 6)$, but it does not seem feasible to compute the entire set $\mathcal{P}(80, 6)$, even using the information from the primes $p = 3, 5$, and 7.

Remark 3. Combining the results of Examples 1, 5, and 6 with Remark 1, we have $m^*(N) \leq 6$ for all $N < 96$ and hence we have shown that

$$N^*(7) = 96.$$

As already remarked, we know that $|\mathcal{P}(96, 7)| \geq 2$ so $m^*(96) \geq 7$. By using the prime $p = 5$, we can prove that if $P \in \mathcal{P}(96, 8)$, then $P(\zeta_5) = \pm 25$ which has norm 5^8. Thus $\mathcal{P}(96, 9)$ is empty and hence we have $7 \leq m^*(96) \leq 8$. To completely enumerate $\mathcal{P}(96, 8)$ using the information that $\pm P(\zeta_5) = 25 = 20 - 5\zeta_5 - 5\zeta_5{}^2 - 5\zeta_5{}^3 - 5\zeta_5{}^4$ would require the examination of $\binom{20}{0}\binom{19}{7}^4 = 6.446 \times 10^{18}$ polynomials, which is not currently feasible.

Example 7. $N = 56$, $m = 6$, $p = 3$. We now know that $m^*(48) = m^*(64) = 6$. In [Bo] we showed that $5 \leq m^*(56) \leq 7$ and in Remark 1 above that in fact $m^*(56) \leq 6$. Using $p = 3$, we have $56 = 19 + 19 + 18$ and can show that if $P \in \mathcal{P}(56, 6)$, then $\pm P(\zeta_3) = 9 + 9\zeta_3 - 18\zeta_3{}^2$. Thus to determine all of $\mathcal{P}(56, 6)$ requires an examination of only $\binom{19}{5}^2\binom{18}{0} = 1.352 \times 10^8$ polynomials. It required 38 minutes of computation to verify that $\mathcal{P}(56, 6)$ is empty, so $m^*(56) = 5$.

Remark 4. We now briefly consider the possibilities for $N^*(8)$. We know from Lemma 1 that this will require N to be a multiple of 16. We have just shown that $N^*(7) = 96$. From the known elements of $\mathcal{P}(96, 7)$ we can construct a number

of elements of $\mathcal{P}(192, 8)$, so we need only consider multiples of 16 in the range $96 \leq N \leq 192$. Using the above methods, choosing $p = 3$ or 5 to be the smallest nondivisor of N, we find the following bounds: $7 \leq m^*(96) \leq 8$, $6 \leq m^*(112) \leq 7$, $m^*(128) = 7$, $6 \leq m^*(144) \leq 10$, $7 \leq m^*(160) \leq 8$, $6 \leq m^*(176) \leq 8$, and $8 \leq m^*(192) \leq 9$. Thus the only possibilities for $N^*(8)$ are 96, 144, 160, 176, and 192. The most likely possibility seems to be 192, but $N = 144 = 2^4 \times 3^2$ is an intriguing possibility because of the large upper bound $m^*(144) \leq 10$ that our methods yield.

Example 8. $N = 144$, $m = 8$, $p = 5$. Writing $144 = 29 + 29 + 29 + 29 + 28$, we find that $P \in \mathcal{P}(144, 8)$ gives four possibilities for $\pm P(\zeta_5)$, namely $25(1 - \zeta_5 - \zeta_5{}^2 + \zeta_5{}^3)$ with norm 5^{10}, $25(1 - \zeta_5 + \zeta_5{}^2 - \zeta_5{}^3)$ or $25(1 + \zeta_5 - \zeta_5{}^2 - \zeta_5{}^3)$ with norm 5^9 and $5 + 5\zeta_5 + 5\zeta_5{}^2 + 5\zeta_5{}^3 - 20\zeta_5{}^4$ with norm 5^8. So even to rule out $m = 9$ or 10 using this information would require the examination of $3\binom{29}{2}^4\binom{28}{14} = 3.270 \times 10^{18}$ possibilities, which is not currently feasible. Using $p = 7$ leads to 72 possibilities for $\pm P(\zeta_7)$, one with norm 7^{11}, one with norm 7^{10}, 8 with norm 7^9, and 62 with norm exactly divisible by 7^8.

Example 9. In view of Byrnes' examples $B_k(x)$ with $N = 2^k$, it is worth seeing what the above methods yield in this case. Using $p = 3$, we find that $m^*(2^k) = k$ for $1 \leq k \leq 7$, that $k \leq m^*(2^k) \leq k + 1$ for $8 \leq k \leq 12$, and $13 \leq m^*(2^{13}) \leq 15$.

4. Computations

We now describe the improvements on the algorithm of [Bo] implied by the results of the previous sections. We will write $P(x) = \sum_{j=1}^{N} a(j)x^{j-1}$, and $P(1 + t) = \sum_{i=1}^{N} c(i)t^{i-1}$ with

$$(12) \qquad\qquad c(i) = \sum_{j=1}^{N} a(j)\binom{j-1}{i-1}.$$

Thus $P \in \mathcal{P}(N, m)$ if and only if $c(i) = 0$ for $i = 1, \ldots, m$.

In [Bo] we used the fact that if $P(1) = 0$, then N must be even and have $N/2$ coefficients equal to $+1$ and $N/2$ equal to -1. So P is specified by the subset of j for which $a(j) = -1$ and hence by an $N/2$-subset of the $(N-1)$-set $\{1, \ldots, N-1\}$ (because of the assumption $a(N) = 1$). Thus, for example, the set $\mathcal{P}(48, 1)$ contains $\frac{1}{2}\binom{48}{24} = 1.612 \times 10^{13}$ polynomials. Recall that in [Bo], we enumerated the set $\mathcal{P}(40, 1)$ which has $\frac{1}{2}\binom{40}{20} = 6.892 \times 10^{10}$ elements in about 1 week on a Sparc 10 workstation. Thus the enumeration of $\mathcal{P}(48, 1)$ would take roughly 234 weeks or about 4.5 years on the same machine.

By the method of the previous section, if $P \in \mathcal{P}(N, m)$ and $p \leq m + 1$, we can determine all possible $\beta \in \mathbb{Z}[\zeta_p]$ for which $\pm P(\zeta_p) = \beta$. Using the decomposition (6), we thus have to determine all $P \in \pm\mathcal{P}(N)$ for which $P_j(1) = A_j$, $j = 1, \ldots, p$. (The ambiguous sign simply means we do not restrict P to be monic). Thus, as already described, P_j must have $K_j = (N_j - A_j)/2$ coefficients equal to -1 and $N_j - K_j$ coefficients equal to $+1$, and so is completely specified by giving the K_j-subset of negative coefficients of the N_j-set of all coefficients of P_j.

As in [Bo] one can use the "revolving door" algorithm of Nijenhuis and Wilf [NW, p. 34] in exactly the same way as used in [Bo] to enumerate the above set. That algorithm provides an enumeration of the k-subsets of $\{1, \ldots, n\}$ in a circular list

in which each set differs from the previous set by the addition of one element "in" and the omission of an element "out". We simply need to set up the enumeration of each of the arrays $a(j + np)$, $j = 1, \ldots, p$ as a p-tuple of nested loops. Since the loops are circular, one can thus regard the whole system as an odometer, using "carry" flags to indicate the completion of each loop.

This gives an enumeration of $(a(1), \ldots, a(N))$ in which each vector differs from the previous one by the change of sign of some $a(\mathrm{in})$ from $+1$ to -1 and some other $a(\mathrm{out})$ from -1 to $+1$, so that the $c(i)$ can be updated by the rule

$$(13) \qquad\qquad c(i) \leftarrow c(i) - 2\binom{\mathrm{in} - 1}{i - 1} + 2\binom{\mathrm{out} - 1}{i - 1}$$

for $i = 1, \ldots, m$. The test for $(x - 1)^m$ to divide $P(x)$ is that $c(i) = 0$ for $i = 1, \ldots, m$. It is interesting that (13) does not depend on N and hence the computation time depends almost entirely on the size of the set to be searched and not explicitly on the size of N.

A linear algebra trick. There is a simple method for reducing the size of the search space by using some basic linear algebra. Select any m of the components of $(a(1), \ldots, a(N))$, say $a(i_1), \ldots, a(i_m)$, and solve the equations $c(i) = 0$ for the $a(i_j)$. It is easily seen that the rank of the coefficient matrix is m (by considering its interpretation in terms of a polynomial interpolation problem). And hence one obtains a matrix equation

$$(14) \qquad\qquad (a(i_1), \ldots, a(i_m)) = (a(1), \ldots, a(N))'A,$$

where the $'$ means to set the entries $a(i_j)$, $j = 1, \ldots, m$ to 0. The matrix A will have rational entries with a common denominator d, say, and hence we can write (6) as

$$(15) \qquad\qquad (b(1), \ldots, b(m)) = (a(1), \ldots, a(N))'B,$$

where $b(j) = da(i_j)$. If we enumerate the vectors $(a(1), \ldots, a(N))'$ by a revolving door algorithm, then the $b(j)$ can be updated by in a manner analogous to (13), i.e.,

$$(16) \qquad\qquad b(i) \leftarrow b(i) - 2B(i, \mathrm{in}) + 2B(i, \mathrm{out}).$$

The test for $(x - 1)^m$ to divide $P(x)$ is now that $|b(i)| = d$ for $i = 1, \ldots, m$. Since there are now only $N - m$ variables $a(j)$, we seem to have gained a factor of $1/2^m$.

However, there is a slight complication. Since we have eliminated m of the $a(i)$ from consideration, we now no longer know exactly how many remaining $a(j+np)$ in the jth congruence class modulo p are -1, at least if $\{i_1, \ldots, i_m\}$ intersects the jth congruence class. The solution is to have $\{i_1, \ldots, i_m\}$ intersect as few congruence classes as possible. If $\{i_1, \ldots, i_m\}$ has k elements in the jth congruence class, we enumerate all possible subsets of the $N_j - k$ remaining elements using the Gray code ordering [NW, p. 18]. Recall that this is an ordering of all subsets of $\{1, \ldots, n\}$ in a circular list in which each subset differs from the preceding subset by one element. This requires an easy modification of (16) for those congruence classes affected.

For example, consider $N = 48$, $m = 5$, $p = 3$, where $N_j = 16$ and $K_j = 8$ for each j, and here we can assume that P is monic so $a(48) = 1$. A straighforward enumeration as in Example 2 would have taken about 15 weeks. Let us choose $i_j = 3j$, $j = 1, \ldots, 5$. Then we enumerate the 2^{10} remaining subsets of $\{18, 24, \ldots, 45\}$ by the Gray code algorithm and the $\binom{16}{8} = 12870$ 8-subsets of each of $\{1, 4, \ldots, 46\}$

and $\{2, 5, \ldots, 47\}$, by the revolving door algorithm. Thus we need to enumerate a total of $2^{10}\binom{16}{8}^2 = 1.696 \times 10^{11}$ polynomials i.e., about 2.5 weeks of computation. (In fact, the saving is somewhat larger than this since the Gray code enumeration is faster than the revolving door enumeration.) The value of d is $3^5 = 243$ so the entries of B in (16) can be represented as single precision integers.

If we had wanted to simply enumerate $\mathcal{P}(48, 6)$ by this method, we would have taken $m = 6$ and so the time would be about half of this. Of course, the enumeration of $\mathcal{P}(48, 6)$ using the prime $p = 5$ as in Example 1 took only 10 minutes and hence was considerably more efficient.

The set $\mathcal{P}(48, 5)$**.** Using the methods of Examples 1 and 2, we have verified by two independent computations that $|\mathcal{P}(48, 5)| = 102$. Here are some more details about the polynomials in this set. The only symmetric polynomial in the set is the unique element of $\mathcal{P}(48, 6)$. There are in addition 41 antisymmetric polynomials in $\mathcal{P}(48, 5)$. All these were found in [Bo]. The remaining 60 polynomials come in pairs $(P, \pm P^*)$, where $P^*(x) = x^{47}P(1/x)$ is the reciprocal of P.

The factorization of the various polynomials is of interest. Lemmas 1 and 2 and Example 2 guarantee that each P found will be divisible by $\Phi_1^5\Phi_2\Phi_3$. In fact, all P have the additional factor $\Phi_4(x) = x^2 + 1$. The most common factorization, which occured for 32 of the 102 polynomials was

$$P = \Phi_1^5\Phi_2\Phi_3\Phi_4 Q_{37},$$

where Q_{37} denotes an irreducible noncyclotomic polynomial of degree 37 (different for different P, of course). These are necessarily not symmetric or antisymmetric since the only irreducible such polynomials of odd degree are $\Phi_1(x) = x - 1$ and $\Phi_2(x) = x + 1$. In addition, two of the antisymmetric polynomials factored as

$$P = \Phi_1^5\Phi_2^2\Phi_3\Phi_4 Q_{36}.$$

The most highly composite P found was one of the antisymmetric P, which factored as

$$P_{48} = \Phi_1^5\Phi_2^2\Phi_3^3\Phi_4^2\Phi_6^2\Phi_8\Phi_{12}^2\Phi_{24} Q_6,$$

where $Q_6(x) = x^6 + x^5 + 2x^4 + 3x^3 + 2x^2 + x + 1$. In fact $P_{12} = (x-1)^3\Phi_3 Q_6$ is the unique element of $\mathcal{P}(12, 3)$, $P_{24} = (x^{12} - 1)P_{12} \in \mathcal{P}(24, 4)$ and $P_{48} = (x^{24} - 1)P_{24}$, accounting for the highly composite structure of P_{48}.

As we indicated in [Bo], the extremal $P \in \mathcal{P}(48, 6)$ factors as $\Phi_1^6\Phi_2^3\Phi_3\Phi_4\Phi_6\Phi_8 Q_{28}$, where the first half of the coefficients of Q_{28} are

$$1, 4, 9, 16, 24, 32, 41, 50, 59, 68, 76, 82, 87, 90, 91.$$

5. Spectral-null codes

After the first version of this paper had been submitted for publication and circulated as a preprint, we were informed by R. Roth that there are a number of papers in the engineering literature on "spectral-null codes". These are sets of polynomials with coefficients in ± 1 that have a high order zero at $x = 1$. In that terminology, our set $\mathcal{P}(N, k)$ is the kth order spectral-null code of length N. The conjecture of Byrnes was also formulated at about the same time by Roth, Siegel and Vardy in [RSV]. The paper of Roth [R] and its references will provide an entry into this literature.

In a master's thesis, Skachek [S] has also enumerated $\mathcal{P}(48, k)$ for $k = 2, 5$ and 6 and showed that $\mathcal{P}(48, 7)$ is empty. He computed $\mathcal{P}(56, 5)$ and showed that $\mathcal{P}(64, 7)$ is empty but did not compute the set $\mathcal{P}(64, 6)$. His methods have some relation to those used here in that congruences modulo various primes are derived for the coefficients. These are derived without the use of $\mathbb{Z}[\zeta_p]$ and are not quite as strong as those we derive from Lemma 3.

In a recent paper, Freiman and Litsyn [FL] prove an asymptotic formula for $\mathcal{P}(N, k)$.

Finally, we should mention that Borwein and Mossinghoff [BM] have recently adapted the methods of this paper to treat the case of polynomials with coefficients in $\{-1, 0, 1\}$.

I would like to thank Ron Ferguson for his very careful reading of the manuscript.

References

[BM] P. Borwein and M. Mossinghoff, *Polynomials with height* 1 *and prescribed vanishing at* 1, Experiment. Math. **9** (2000), 425–433. CMP 2001:04

[Bo] D.W. Boyd, *On a problem of Byrnes concerning polynomials with restricted coefficients*, Math. Comp. **66** (1997), 1697–1703. MR **98a:**11033

[By] 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 and J.F. Byrnes, eds.), Kluwer Academic Publishers, Dordrecht, 1990, pp. 677–678.

[E] H.M. Edwards, *Fermat's Last Theorem. A genetic introduction to algebraic number theory*, Springer-Verlag, New York, 1977. MR **83b:**12001a

[FL] G. Freiman and S. Litsyn, *Asymptotically exact bounds on the size of high-order spectral-null codes*, IEEE Trans. Inform. Theory **45** (1999), 1798–1807. MR **2000k:**94060

[LN] R. Lidl and H. Niederreiter, *Finite Fields*, Addison-Wesley, Reading, 1983. MR **86c:**11106

[NW] A. Nijenhuis, and H.S. Wilf, *Combinatorial Algorithms*, Academic Press, Orlando, 1978. MR **80a:**68076

[RSV] R.M. Roth, P.H. Siegel, and A. Vardy, *High-order spectral-null codes: Constructions and bounds*, IEEE Trans. Inform. Theory **35** (1989), 463–472.

[R] R.M. Roth, *Spectral-null codes and null spaces of Hadamard submatrices*, Designs, Codes and Cryptography **9** (1996), 177–191. MR **98e:**94034

[S] V. Skachek, *Coding for Spectral-Null Constraints*, Research Thesis, Master of Science in Computer Science, Technion, Israel Institute of Technology, November 1997 (Hebrew).

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

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