MATHEMATICS OF COMPUTATION
Volume 75, Number 255, July 2006, Pages 1541–1552
S 0025-5718(06)01848-5
Article electronically published on May 1, 2006

LITTLEWOOD POLYNOMIALS WITH HIGH ORDER ZEROS

DANIEL BEREND AND SHAHAR GOLAN

Abstract. Let $N^*(m)$ be the minimal length of a polynomial with ± 1 coefficients divisible by $(x-1)^m$. Byrnes noted that $N^*(m) \leq 2^m$ for each m, and asked whether in fact $N^*(m) = 2^m$. Boyd showed that $N^*(m) = 2^m$ for all $m \leq 5$, but $N^*(6) = 48$. He further showed that $N^*(7) = 96$, and that $N^*(8)$ is one of the 5 numbers $96, 144, 160, 176$, or 192. Here we prove that $N^*(8) = 144$. Similarly, let $m^*(N)$ be the maximal power of $(x-1)$ dividing some polynomial of degree $N-1$ with ± 1 coefficients. Boyd was able to find $m^*(N)$ for $N < 88$. In this paper we determine $m^*(N)$ for $N < 168$.

1. Introduction

For a positive integer m, consider the polynomial

$$B_m(x) = \prod_{j=0}^{m-1} \left(x^{2^j} - 1\right).$$

Obviously, $B_m(x)$ is of degree $2^m - 1$, all its coefficients are ± 1 and it is divisible by $(x-1)^m$. Byrnes [4] asked whether $B_m(x)$ is the polynomial of minimal degree enjoying these properties. He mentioned that it would be interesting to know even just whether the minimal degree of such a polynomial increases exponentially or sub-exponentially as a function of m. The problem comes up in the design of antenna arrays and notch filters [5], in coding theory in connection with so-called *spectral-null codes* [10], [11], and it is also related to the *Prouhet-Thue-Morse sequence* [1]. The problem has been investigated by Boyd [2], [3]. Denote by $\mathcal{P}(N)$ the set of all monic *Littlewood polynomials* of degree $N-1$, i.e., polynomials all of whose coefficients are in $\{-1, 1\}$, and by $\mathcal{P}(N, m)$ the subset consisting of those polynomials divisible by $(x-1)^m$ (or by some higher power of $(x-1)$). For a fixed m, let $N^*(m)$ be the smallest N for which $\mathcal{P}(N, m)$ is nonempty, and for a fixed N let $m^*(N)$ be the largest m such that $\mathcal{P}(N, m)$ is nonempty. On the theoretical side, Boyd proved that $N^*(m) \geq e^{\sqrt{m}(1+o(1))}$. Moreover, for $m^*(N)$ to be large, N has to be divisible by a large power of 2. Also, if N fails to be divisible by some small prime, then it has to be exponentially large (as a function of m) for $\mathcal{P}(N, m)$ to be nonempty.

Boyd's approach is based on an ingenious exploitation of the fact that, if $P(x) \in \mathcal{P}(N, m)$, then, in particular, for any algebraic integer ζ, the algebraic integer $P(\zeta)$ is divisible by $(\zeta - 1)^m$. In general, this would be of little help, as $P(\zeta)$ may take

Received by the editor May 5, 2005 and, in revised form, June 30, 2005.
2000 *Mathematics Subject Classification.* Primary 11B83, 12D10; Secondary 94B05, 11Y99.
Key words and phrases. Littlewood polynomials, spectral-null code, antenna array.

any of 2^N possible values. However, if $\zeta = \zeta_p$ is a root of unity of low prime order p, then $P(\zeta_p)$ is limited to one of a relatively small number of values.

Boyd was able to use his method to calculate $m^*(N)$ for all $N < 88$. In particular, he showed that Byrnes's conjecture is true for $m \leq 5$, but fails for $m = 6$. He proved that $N^*(6) = 48$ by constructing a polynomial of degree 47 with ± 1 coefficients and divisible by $(x-1)^6$. To this end, he used heavy computer computations. We have $|\mathcal{P}(48)| = 2^{47}$. To be divisible by $x - 1$, namely to belong to $\mathcal{P}(48, 1)$, a polynomial must have the same number of $+1$ and -1 coefficients. We are thus left with a search space of size $\binom{47}{23}$. This space may be considered as the set of all subsets of size 23 of a set of size 47. Boyd would go over this set using the "revolving door" algorithm (cf. [9]), which allows a fast search as each subset in the sequence is obtained from its predecessor by a minimal change—removing a single element and joining another instead. Actually, due to computing power limitations, he searched only the set of symmetric polynomials in [2] (i.e., those satisfying $P(x) = x^{47}P(1/x)$), but further improvements of his method enabled him to reduce the size of the space to be searched to a feasible size in [3]. The number $N = 88$ was the smallest for which he was unable to calculate $m^*(N)$, and he left open the question whether $m^*(88) = 5$ or $m^*(88) = 6$.

In this paper we show that Boyd's approach can be improved both theoretically and computationally to strengthen his results. On the theoretical side, we are able to exploit the full power provided by the information arising from the fact that $P(\zeta_p)$ is divisible by $(\zeta_p - 1)^m$ to get better constraints on the values of the polynomial's coefficients. In addition, we manage to get some information from the fact that $P(\zeta_{p^k})$ is divisible by $(\zeta_{p^k} - 1)^m$ for prime powers p^k. On the computational side, we design a systematic method for combining the information obtained from different ζ_p's to further shorten the search. The search itself is performed by the same method as in [3], although it seems that our machine runs about four times faster than Boyd's. Thus whereas he could go over about 10^{10} polynomials per day, we can go over about $4 \cdot 10^{10}$. (In fact, all of our results could have been achieved even on a slower machine, since only for $N = 160$ does the search require almost a day. For $N = 144$ it took about two hours.) Using these improvements, we extend the range of N's with known $m^*(N)$ from $N < 88$ to $N < 168$. In particular, we are able to deal with two of the more interesting (i.e., divisible by a high power of 2 and by 3) numbers, $N = 96$ and $N = 144$, and show that $m^*(96) = 7$ and $m^*(144) = 8$.

We note that most of our results, even those which necessitated an extensive search, may be easily verified; once a polynomial is given, it is easy to check that it is divisible by some power of $(x - 1)$. The negative results are usually obtained by hand. Only for $N = 160$ is the reader required to believe our computations.

In Section 2 we present the main results. Section 3 contains a few simple results on cyclotomic fields. In Section 4 we demonstrate the power of our results by finding the values of $m^*(48)$ and $m^*(96)$ without the aid of a computer. The proofs of the main results are given in Section 5.

To prove that $m^*(N)$ is bounded below by some value, we usually have to find a polynomial of degree $N - 1$ divisible by an appropriate power of $x - 1$. Such polynomials, accompanying all the results of the paper, may be found in [6].

We would like to express our gratitude to J.-P. Allouche, who drew our attention to the problem discussed here, and to Boyd's work on the subject.

2. The main results

Our first result provides the value of $m^*(N)$ for every N with $m^*(N) \leq 5$. All parts of the theorem, except for the last two, can be inferred pretty easily from Boyd's results [2], [3].

Theorem 2.1. *We have:*

1. $m^*(N) = 0$ *if and only if* N *is odd.*
2. $m^*(N) = 1$ *if and only if* $2||N$.
3. $m^*(N) = 2$ *if and only if* $N = 4$.
4. $m^*(N) = 3$ *if and only if either* $N = 8$ *or both* $2^2||N$ *and* $N \geq 12$.
5. $m^*(N) = 4$ *if and only if* $N = 16, 24$.
6. $m^*(N) = 5$ *if and only if* $N = 32, 40, 56$.
7. $m^*(N) \geq 6$ *if and only if* $N = 48$ *or both* $2^3 \mid N$ *and* $N \geq 64$.

In the next theorem we provide the value of $m^*(N)$ for several N's which are not covered by (parts 1–6 of) Theorem 2.1. As mentioned earlier, out of these, the value of $m^*(N)$ was found by Boyd for every $N < 88$ and for $N = 128$. Some of the other values were not dealt with by Boyd, and for others he obtained only lower and upper bounds. For example, he showed that $7 \leq m^*(96) \leq 8$, $7 \leq m^*(144) \leq 10$ and $8 \leq m^*(256) \leq 9$.

Theorem 2.2.

1. *For* $N = 48, 64, 72, 80, 88, 104, 120, 136, 152$ *we have* $m^*(N) = 6$.
2. *For* $N = 96, 112, 128, 160$ *we have* $m^*(N) = 7$.
3. *For* $N = 144, 256$ *we have* $m^*(N) = 8$.

From Theorems 2.1 and 2.2 we immediately obtain

Theorem 2.3. $N^*(8) = 144$.

In the next proposition we provide lower bounds for $m^*(N_1+N_2)$ and $m^*(N_1N_2)$ in terms of $m^*(N_1)$ and $m^*(N_2)$. This result was insinuated in Boyd's article, and we provide its proof for completeness. Note that the proof is constructive. Namely, given polynomials $P_1 \in \mathcal{P}(N_1, m_1)$, $P_2 \in \mathcal{P}(N_2, m_2)$, we construct explicitly polynomials in $\mathcal{P}(N_1 + N_2)$ and $\mathcal{P}(N_1N_2)$ with zeros of the prescribed order at 1.

Proposition 2.4. *For any* N_1, N_2 *we have*

1. $m^*(N_1 + N_2) \geq \min(m^*(N_1), m^*(N_2))$.
2. $m^*(N_1N_2) \geq m^*(N_1) + m^*(N_2)$.

3. Auxiliary results on cyclotomic extensions

As mentioned earlier, Boyd's method is based on the fact that, if $(x-1)^m \mid P(x)$, then in particular $(\zeta_p - 1)^m \mid P(\zeta_p)$, where $\zeta_p = e^{2ki\pi/p}$. In order to reduce the search space to such polynomials, he needed to characterize the numbers, which are divisible by $(\zeta_p - 1)^m$. Boyd used the fact that, if $(\zeta_p - 1)^m \mid \beta$, then $\|\beta\|$ is divisible by p^m. We develop an exact criterion for divisibility by high powers of $(\zeta_p - 1)$, which allows us to reduce, substantially in some cases, the search space. Additionally, in Proposition 3.1 we accomplish this for $(\zeta_{p^k} - 1)$. Proposition 3.4 gives a strengthened version of Proposition 3.1 for the case where $k = 1$. Proposition 3.5 discusses the case $p^k = 2$, which simply means $\zeta_{p^k} = -1$.

Throughout this section, β will denote an element of $\mathbf{Z}[\zeta_{p^k}]$ with a (nonunique) representation of the form $\beta = A_0 + A_1\zeta_{p^k} + A_2\zeta_{p^k}^2 + \cdots + A_{p^k-1}\zeta_{p^k}^{p^k-1}$, with rational

integers A_j. Recall that $(\zeta_{p^k}-1)^{\varphi(p^k)}/p$ is a unit in $\mathbf{Z}[\zeta_{p^k}]$ (cf. [12]), i.e., a number in $\mathbf{Z}[\zeta_{p^k}]$ is divisible by $(\zeta_{p^k}-1)^{\varphi(p^k)}$ if and only if it is divisible by p. In particular, $(\zeta_{p^k}-1)$ divides a rational integer if and only if p divides this integer.

Proposition 3.1. *β is divisible by $(\zeta_{p^k}-1)^{l\varphi(p^k)+r}$, where $l\geq 0$ and $1\leq r<\varphi(p^k)$, if and only if:*

1. *For each $j\in\{0,1,\ldots,p^{k-1}\}$, the numbers $A_j, A_{j+p^{k-1}},\ldots,A_{j+(p-1)p^{k-1}}$ are congruent modulo p^l.*
2. *β/p^l is an algebraic integer. Moreover writing $\beta/p^l=A'_0+A'_1\zeta_{p^k}+A'_2\zeta_{p^k}^2+\cdots+A'_{p^k-1}\zeta_{p^k}^{p^k-1}$ for appropriate integers $A'_0,A'_1,\ldots,A'_{p^k-1}$, we have*

$$\binom{j}{j}A'_j+\binom{j+1}{j}A'_{j+1}+\cdots+\binom{p^k-1}{j}A'_{p^k-1}\equiv 0 \pmod p,\quad 0\leq j<r.$$

The proposition immediately follows from the following two lemmas.

Lemma 3.2. *β is divisible by $(\zeta_{p^k}-1)^r$, where $r<\varphi(p^k)$, if and only if*

$$\binom{j}{j}A_j+\binom{j+1}{j}A_{j+1}+\cdots+\binom{p^k-1}{j}A_{p^k-1}\equiv 0 \pmod p,\quad 0\leq j<r.$$

Proof. Write

$$\begin{aligned}\beta &= A_0+A_1((\zeta_{p^k}-1)+1)+A_2((\zeta_{p^k}-1)+1)^2+\cdots\\ &\quad +A_{p^k-1}((\zeta_{p^k}-1)+1)^{p^k-1}\\ &= \textstyle\sum_{j=0}^{p^k-1}\left(\binom{j}{j}A_j+\binom{j+1}{j}A_{j+1}+\cdots+\binom{p^k-1}{j}A_{p^k-1}\right)(\zeta_{p^k}-1)^j.\end{aligned}\tag{3.1}$$

We prove the lemma by induction. If $(\zeta_{p^k}-1)\mid\beta$, then by (3.1) we have $(\zeta_{p^k}-1)\mid\binom{0}{0}A_0+\binom{1}{0}A_1+\cdots+\binom{p^k-1}{0}A_{p^k-1}$, and therefore $p\mid\sum_{j=0}^{p^k-1}\binom{j}{0}A_j$.

Suppose the lemma holds for $r-1$ instead of r, and let $(\zeta_{p^k}-1)^r\mid\beta$. By the induction hypothesis,

$$\binom{j}{j}A_j+\binom{j+1}{j}A_{j+1}+\cdots+\binom{p^k-1}{j}A_{p^k-1}\equiv 0 \pmod p,\quad j<r-1.$$

The sum on the left-hand side is the coefficient of $(\zeta_{p^k}-1)^j, 0\leq j<r-1$, in (3.1). The coefficient of $(\zeta_{p^k}-1)^{r-1}$ is $\binom{r-1}{r-1}A_{r-1}+\binom{r}{r-1}A_r+\cdots+\binom{p^k-1}{-1}A_{p^k-1}$, and it must be divisible by $(\zeta_{p^k}-1)$, which means it must be divisible by p. □

Lemma 3.3. *β is divisible by $(\zeta_{p^k}-1)^{l\varphi(p^k)}$ if and only if for each $0\leq j<p^{k-1}$, the numbers A_j,$A_{j+p^{k-1}}$, $A_{j+2p^{k-1}},\ldots,A_{j+(p-1)p^{k-1}}$ are congruent modulo p^l.*

Proof. Use the equality $\zeta_{p^k}^{\varphi(p^k)}=-1-\zeta_{p^k}^{p^{k-1}}-\cdots-\zeta_{p^k}^{(p-2)p^{k-1}}$ to write β as a linear combination of the $\zeta_{p^k}^j$'s, $0\leq j\leq\varphi(p^k)-1$:

$$\begin{aligned}\beta = \quad & (A_0-A_{\varphi(p^k)})+(A_1-A_{1+\varphi(p^k)})\zeta_{p^k}+(A_2-A_{2+\varphi(p^k)})\zeta_{p^k}^2+\cdots\\ & +(A_{\varphi(p^k)-1}-A_{p^k-1})\zeta_{p^k}^{\varphi(p^k)-1}.\end{aligned}$$

We know that β is divisible by p^l. A number in $Z[\zeta_{p^k}]$ is divisible by $(\zeta_{p^k}-1)^{l\varphi(p^k)}$ if and only if all coefficients in its representation according to the basis $\{\zeta_{p^k}^j\}_{j=0}^{\varphi(p^k)-1}$ are divisible by p^l. This means that $A_j\equiv A_{j+p^{k-1}} \pmod{p^l}$, for $j\leq\varphi(p^k)-1$. □

For the next proposition we assume that $k = 1$. From Lemma 3.2 we easily get that, if $\beta \in (\zeta_p - 1)\mathbf{Z}[\zeta_p]$, then β has a unique representation of the form

$$\beta = A_0 + A_1\zeta_p + A_2\zeta_p^2 + \cdots + A_{p-1}\zeta_p^{p-1}, \quad \sum_{j=0}^{p-1} A_j = 0. \tag{3.2}$$

Proposition 3.4. *Let $\beta \in (\zeta_p - 1)\mathbf{Z}[\zeta_p]$. Then β is divisible by $(\zeta_p - 1)^{l(p-1)+r}$, where $l \geq 0$ and $1 \leq r < p - 1$, if and only if in the representation* (3.2)*:*

1. *Each A_j is divisible by p^l.*
2. *Denoting $A'_j = A_j/p^l$ for each j, we have the system of congruences*

$$\binom{j}{j}A'_j + \binom{j+1}{j}A'_{j+1} + \cdots + \binom{p-1}{j}A'_{p-1} \equiv 0 \pmod{p}, \quad 0 \leq j < r.$$

Proof. We know that β is divisible by p^l. Put $\beta' = \beta/p^l$. Write $\beta = B'_0 + B'_1\zeta_p + B'_2\zeta_p^2 + \cdots + B'_{p-1}\zeta_p^{p-1}$, where $\sum_{j=0}^{p-1} B'_j = 0$. Now β' is divisible by $(\zeta_p - 1)^r$. Since $r < p - 1$, Lemma 3.2 gives

$$\binom{j}{j}B'_j + \binom{j+1}{j}B'_{j+1} + \cdots + \binom{p-1}{j}B'_{p-1} \equiv 0 \pmod{p} \quad 0 \leq j < r.$$

β has the representation $p^l\beta' = p^lB'_0 + p^lB'_1\zeta_p + p^lB'_2\zeta_p^2 + \cdots + p^lB'_{p-1}\zeta_p^{p-1}$, which is the unique representation of β satisfying $\sum_{j=0}^{p-1} p^lB'_j = 0$. This means that $A_j = p^lB'_j$ and therefore $A'_j = B'_j$ for $0 \leq j \leq p - 1$. □

The next proposition will give a constraint on polynomials in $\mathcal{P}(N, m)$, where N is divisible by a low power of 2.

Proposition 3.5. *If $P \in \mathcal{P}(N, m)$, where $2^k||N$ and $m > 2^k - 2$, then $|P(-1)| \geq 2^m$.*

First we prove a lemma that will help us in the proof.

Lemma 3.6. *If $P \in \mathcal{P}(N, m)$ and $|P(-1)| < 2^m$, then $P(-1) = 0$.*

Proof. Write $P(x) = (x - 1)^mQ(x)$. We have $|P(-1)| = |(-2)^mQ(-1)| < 2^m$, and $Q(-1)$ is an integer. Hence $Q(-1) = 0$, and so $P(-1) = 0$. □

Proof of Proposition 3.5. Assume, to the contrary, that $|P(-1)| < 2^m$. By Lemma 3.6, $P(x) = (x - 1)^m(x + 1)R(x)$ for some polynomial $R(x) \in \mathbb{Z}[x]$. Hence $P(x)$ is divisible by $(x + 1)^{m+1}$ modulo 2. Recall that $P(x) \equiv (x^N - 1)/(x - 1) \pmod 2$. Hence the complete factorization of P over $\mathbb{F}_2$ is known (see [7]). In particular, if $2^k||N$, then the product of all linear factors of $P(x)$ over $\mathbb{F}_2$ is $(x + 1)^{2^k-1}$. This implies that $m+1 \leq 2^k-1$. This is contrary to the assumption that $m > 2^k-2$. □

4. Examples: $N = 48$ and $N = 96$

In this section we illustrate the strength of the results in Sections 2 and 3 by evaluating $m^*(48)$ and $m^*(96)$ (almost) by hand. Boyd needed to check about 10^8 polynomials in order to enumerate $\mathcal{P}(48, 6)$, and was unable to determine $m^*(96)$. Here we manage to reduce the search space for $\mathcal{P}(48, 6)$ to about a hundred possible polynomials. We determine $m^*(96)$ by using our results, without checking a single polynomial.

We use the results of Section 3 in the following way: Let $P \in \mathcal{P}(N)$. Let A be the set of indices of the $+1$ coefficients, and B the corresponding set for the -1's. For a prime power p^k and $0 \le j \le p^k - 1$, denote by $d_{p^k,j}$ the difference between the number of elements, which are congruent to j modulo p^k in A, and the corresponding number in B:

$$d_{p^k,j} = \mid A \cap (p^k\mathbf{Z} + j) \mid - \mid B \cap (p^k\mathbf{Z} + j) \mid .$$

Obviously, $P(\zeta_{p^k}) = d_{p^k,0} + d_{p^k,1}\zeta_{p^k} + d_{p^k,2}\zeta_{p^k}^2 + \cdots + d_{p^k,p^k-1}\zeta_{p^k}^{p^k-1}$, and $\sum_{j=0}^{p^k-1} d_{p^k,j} = 0$ if $P \in \mathcal{P}(N,1)$. If $P \in \mathcal{P}(N,m)$, then $(\zeta_{p^k} - 1)^m$ divides $P(\zeta_{p^k})$. In this case we can deduce from Section 3 some constraints on the values of the $d_{p^k,j}$'s.

Example 4.1. Let $N = 48$. We would like to enumerate $\mathcal{P}(48, 6)$. There are 16 elements in $(3\mathbf{Z}+j) \cap [0, 47]$, and thus $\mid d_{3,j} \mid \le 16$. By Proposition 3.4, all $d_{3,j}$'s are congruent modulo 27, and their sum is 0. The only option is $d_{3,0} = d_{3,1} = d_{3,2} = 0$. For $p = 5$, the sizes of the sets $(5\mathbf{Z} + j) \cap [0, 47]$, $j = 0, 1, 2, 3, 4$, are $10, 10, 10, 9, 9$, respectively. By Proposition 3.4, $d_{5,j} = 0, \pm 10$ for $j = 0, 1, 2$ and $d_{5,j} = \pm 5$ for $j = 3, 4$. A quick enumeration shows that, up to sign, all options have at least one $d_{5,j}$ equal to 10, which means that a whole residue class modulo 5 is contained in A. Using $p = 7$, we find two main options up to sign: either $d_{7,6} = 6$ and all other $d_{7,j}$'s are -1, or $d_{7,6} = 0$, three of the other $d_{7,j}$'s are -7, and the rest are $+7$. However, since each residue class modulo 7 intersects every residue class modulo 5, and since at least one residue class modulo 5 is contained in A, no $d_{7,j}$ may be -7. Thus the only possibility for the $d_{5,j}$'s is $(0, 10, 0, -5, -5)$, and for the $d_{7,j}$'s is $(-1, -1, -1, -1, -1, -1, 6)$. Hence all fourteen elements of $((5\mathbf{Z} + 1) \cap [0, 47]) \cup ((7\mathbf{Z} + 6) \cap [0, 47])$ belong to A. From here we continue with $p^k = 9$. We know that $d_{9,j} + d_{9,j+3} + d_{9,j+6} = d_{3,j} = 0$ for $j = 0, 1, 2$, as the residue class $(3\mathbf{Z} + j) = (9\mathbf{Z} + j) \cup (9\mathbf{Z} + j + 3) \cup (9\mathbf{Z} + j + 6)$. In addition, by Proposition 3.4, $d_{9,j}, d_{9,j+3}, d_{9,j+6}$ are congruent modulo 3. These severe constraints, combined with the information gathered using 5 and 7, leaves only ten options for the numbers $d_{9,j}$, $0 \le j \le 8$. The equality $P(\zeta_3) = d_{3,0} + d_{3,1}\zeta_3 + d_{3,2}\zeta_3 = 0$ also implies that the polynomial P is divisible by $x^2 + x + 1$. Now $(\zeta_9 - 1)^2 \mid (\zeta_9^2 + \zeta_9 + 1)$, so that $(\zeta_9 - 1)^8 \mid P(\zeta_9)$. Out of the ten options for the $d_{9,j}$'s, only for the two options $\pm(2, 2, 2, -1, -1, -1, -1, -1, -1)$ is $\sum_{j=0}^{8} d_{9,j}\zeta_9^j$ divisible by $(\zeta_9 - 1)^8$. Using the same method for 4, we find that, up to sign, the only possible options for the $d_{4,j}$'s are $(0, 0, 0, 0), (-4, 4, 4, -4)$. These constraints cause our search space to shrink to only about a hundred polynomials. The only polynomial that is found is the unique member of $\mathcal{P}(48, 6)$, which does not belong to $\mathcal{P}(48, 7)$, so that $m^*(48) = 6$.

Example 4.2. Let $N = 96$. From the previous example, and by Proposition 2.4, we get that $m^*(96) \ge 7$. Suppose we have a polynomial yielding $m = 8$. For $p = 5$, the sizes of the sets $(5\mathbf{Z}+j) \cap [0, 95]$, $j = 0, 1, 2, 3, 4$, are $20, 19, 19, 19, 19$, respectively. By Proposition 3.4, each $d_{5,j}$ is divisible by 5, and the $d_{5,j}$'s are congruent modulo 25. The only option, up to sign, is $(d_{5,0}, d_{5,1}, d_{5,2}, d_{5,3}, d_{5,4}) = (20, -5, -5, -5, -5)$. Namely, A contains all 20 numbers in the range $[0, 95]$ divisible by 5, and 7 out of the 19 numbers in each of the other 4 residue classes modulo 5. To continue, we consider $p = 7$. By Proposition 3.4, we see that $d_{7,j} = 0, \pm 14$ for $0 \le j \le 4$ and $d_{7,j} = \pm 7$ for $j = 5, 6$. However, since each residue class modulo 7 intersects $5\mathbf{Z} \cap [0, 95]$, which contains only elements of A, no $d_{7,j}$ may be -14. The only possible value for $(d_{7,0}, d_{7,1}, \ldots, d_{7,6})$, after taking this constraint and Proposition

3.4 into consideration, is $(0,0,14,0,0,-7,-7)$. In other words, all 14 elements of $(7\mathbf{Z}+2)\cap[0,95]$ in our range belong to A (where 2 of these, 30 and 65, were already known to be there), while out of the 13 elements of each of $(7\mathbf{Z}+5)\cap[0,95]$ and $(7\mathbf{Z}+6)\cap[0,95]$, only the 3 elements belonging to $5\mathbf{Z}\cap[0,95]$ lie in A and the other 10 lie in B. Altogether, by now we know 52 coefficients, of which 32 belong to A and 20 to B. Now take $p=11$. Note that by Proposition 3.4, if $m^*(96)=8$, then the values of $d_{11,j}$ for $j=8,9,10$ determine uniquely the values of all other $d_{11,j}$'s. As $d_{11,8}, d_{11,9}, d_{11,10}$ are all even and lie between -8 and 8 to begin with, and we have already found 4 elements in $(11\mathbf{Z}+j)\cap[0,95]$ for $j=8,9,10$, we have only 125 options for the $d_{11,j}$'s. For none of these is $\sum_{j=0}^{11} d_{11,j}\zeta_{11}^j$ divisible by $(\zeta_{11}-1)^8$, and hence $\mathcal{P}(96,8)=\emptyset$. Thus $m^*(96)=7$.

5. Proofs of the main results

Proof of Proposition 2.4. In each part we present a polynomial divisible by the required power of $(x-1)$. Let $P_1(x)\in\mathcal{P}(N_1,m_1)$, $P_2(x)\in\mathcal{P}(N_2,m_2)$.

1. Set $m=\min(m_1,m_2)$. Then the polynomial $P_1(x)+x^{N_1}P_2(x)$ is of degree N_1+N_2-1, all its coefficients are ±1, and it is divisible by $(x-1)^m$. Thus $P_1(x)+x^{N_1}P_2(x)\in\mathcal{P}(N_1+N_2,m)$.
2. The polynomial $P_2(x^{N_1})$ is divisible by $(x^{N_1}-1)^{m_2}$, and hence the polynomial $P_1(x)P_2(x^{N_1})$ is of degree N_1N_2-1, all its coefficients are ±1, and it is divisible by $(x-1)^{m_1}(x^{N_1}-1)^{m_2}$, and therefore by $(x-1)^{m_1+m_2}$. Thus $P_1(x)P_2(x^{N_1})\in\mathcal{P}(N_1N_2,m_1+m_2)$. □

For later reference, we record in Table 1 some of the values of $m^*(N)$ found by Boyd.

In Table 2 we record lower and upper bounds for $m^*(N)$ for several values of N, as found by Boyd. (The ordering follows Theorem 2.2.)

Proof of Theorem 2.1. In each of parts 1–6 of the theorem, it will suffice to prove only that $m^*(N)$ assumes the required value for the N's in those parts. The fact that these are the only N's with this value of m^* will then follow once we are done with the other parts of the theorem.

1. Since N is odd, so is $P(1)$, which means that $(x-1)$ does not divide P.
2. By Proposition 2.4 we get (since $m^*(2)=1$) that $m^*(N)\geq 1$. In [2] it is proved that, if $4\nmid N$, then $\mathcal{P}(N,2)$ is empty.
3. See Table 1.

Table 1. Values of $m^*(N)$ according to [2], [3]

N	2	4	8	12	16	24	32	40	56	48	64	72	80	128
$m^*(N)$	1	2	3	3	4	4	5	5	5	6	6	6	6	7

Table 2. Bounds for $m^*(N)$ according to [2], [3]

N	88	104	120	112	136	152	168	96	160	144	256
$m^*(N)\geq$	5	5	5	6	6	6	6	7	7	7	8
$m^*(N)\leq$	6	6	6	7	7	7	7	8	8	10	9

4. By Table 1 we have $m^*(N) = 3$ for $N = 8, 12$. By Proposition 2.4, we have $m^*(12+8j) \geq 3$ for $j > 0$. In [2] it is proved that, if $8 \nmid N$, then $\mathcal{P}(N, 4)$ is empty.
5. See Table 1.
6. See Table 1.
7. If $N = 48, 64, 72, 80, 88, 96, 104$, then by Table 1 and Theorem 2.2 we have $m^*(N) \geq 6$. By Proposition 2.4, this implies $m^*(N) \geq 6$ for any N satisfying the condition of this part. On the other hand, if $2^3 \nmid N$, then $m^*(N) \leq 3$ by [2], while if $2^3 \mid N$, and $N \neq 48$ and $N < 64$, then $m^*(N) \leq 5$ by the preceding parts. □

Proof of Theorem 2.2. The values $N = 48, 64, 72, 80, 128$ were treated by Boyd, $N = 96$ was investigated in Section 4, and we continue with the others.

1.a) $N = 88$.

By Table 2, $m^*(88) \leq 6$. Suppose we have a polynomial yielding $m = 6$. By Proposition 3.4, all $d_{3,j}$'s are divisible by 9 and congruent modulo 27. As $|d_{3,0}| \leq 30$ and $|d_{3,1}|, |d_{3,2}| \leq 29$, the only possibilities (up to sign) are $(d_{3,0}, d_{3,1}, d_{3,2}) = (0, 27, -27)$ and $(d_{3,0}, d_{3,1}, d_{3,2}) = (18, -9, -9)$. It can be shown that the first option does not lead to any polynomial with $m = 6$, but this is of no consequence. The second option leaves us with too many possibilities, and we shall enumerate only the symmetric polynomials. We know that 24 out of the 30 elements of $3\mathbf{Z} \cap [0, 87]$ belong to A and the other 6 to B. We take all $\binom{15}{12}$ options for a symmetric splitting of $3\mathbf{Z} \cap [0, 87]$. In order to divide the other two classes, we will use $p = 5$. By Proposition 3.4 and the symmetry, up to sign we have only the options $(d_{5,0}, d_{5,1}, d_{5,2}, d_{5,3}, d_{5,4}) = (0, 10, 0, -5, -5), (10, -10, 10, -5, -5)$, and $(10, 10, 10, -15, -15)$. For each splitting of $3\mathbf{Z} \cap [0, 87]$, we go over all possibilities of dividing the rest of the elements according to the 6 different possibilities according to the prime 5. After checking about $1.5 \cdot 10^7$ possibilities, we find all symmetric polynomials, 101 in all. For example, the following polynomial is a member of $\mathcal{P}(88, 6)$:

$$\begin{aligned}
&1 - x - x^2 + x^3 + x^4 - x^5 + x^6 - x^7 - x^8 + x^9 - x^{10} + x^{11} + x^{12} - x^{13} - x^{14} \\
&+ x^{15} + x^{16} - x^{17} - x^{18} - x^{19} + x^{20} + x^{21} - x^{22} - x^{23} + x^{24} + x^{25} + x^{26} \\
&+ x^{27} - x^{28} - x^{29} + x^{30} - x^{31} - x^{32} + x^{33} + x^{34} + x^{35} + x^{36} - x^{37} - x^{38} \\
&- x^{39} + x^{40} + x^{41} - x^{42} - x^{43} - x^{44} - x^{45} + x^{46} + x^{47} - x^{48} - x^{49} - x^{50} \\
&+ x^{51} + x^{52} + x^{53} + x^{54} - x^{55} - x^{56} + x^{57} - x^{58} - x^{59} + x^{60} + x^{61} + x^{62} \\
&+ x^{63} - x^{64} - x^{65} + x^{66} + x^{67} - x^{68} - x^{69} - x^{70} + x^{71} + x^{72} - x^{73} - x^{74} \\
&+ x^{75} + x^{76} - x^{77} + x^{78} - x^{79} - x^{80} + x^{81} - x^{82} + x^{83} + x^{84} - x^{85} - x^{86} + x^{87}.
\end{aligned}$$

Thus, $m^*(88) = 6$.

1.b) $N = 104$.

By Table 2, $m^*(104) \leq 6$. Suppose we have a polynomial yielding $m = 6$. We shall examine only the symmetric polynomials. By Lemma 3.3 and the symmetry, we see that, up to sign, $(d_{3,0}, d_{3,1}, d_{3,2}) = (9, 9, -18)$. We know that 8 out of the 34 elements of $(3\mathbf{Z}+2) \cap [0, 103]$ belong to A and the other 26 to B. We take all $\binom{17}{4}$ options for a symmetric splitting of $(3\mathbf{Z}+2) \cap [0, 103]$. In order to divide the other two classes, we will use $p = 5$. After considering Proposition 3.4 and the symmetry, up to

sign the only the possible options are $(d_{5,0}, d_{5,1}, d_{5,2}, d_{5,3}, d_{5,4}) = (-15,15,15,-15,0)$, $(-5,15,15,-5,-20)$, $(5,-5,-5,5,0)$, $(5,5,5,5,-20)$, $(15,-5,-5,15,-20)$. For each splitting of $(3\mathbf{Z}+2)\cap[0,103]$, we may go over all possibilities of dividing the rest of the elements according to the 10 different possibilities according to the prime 5. After checking the $\approx 10^8$ symmetric polynomials with $(d_{5,0}, d_{5,1}, d_{5,2}, d_{5,3}, d_{5,4}) = (5,5,5,5,-20)$, we already find that 74 of them belong to $\mathcal{P}(104,6)$. For example, the following polynomial is a member of $\mathcal{P}(104,6)$:

$$\begin{aligned}
&1 - x + x^2 + x^3 - x^4 - x^5 + x^6 + x^7 - x^8 - x^9 - x^{10} - x^{11} - x^{12} + x^{13} - x^{14} \\
&\quad + x^{15} + x^{16} - x^{17} + x^{18} - x^{19} + x^{20} - x^{21} + x^{22} + x^{23} - x^{24} + x^{25} + x^{26} \\
&\quad + x^{27} + x^{28} - x^{29} - x^{30} + x^{31} - x^{32} + x^{33} - x^{34} - x^{35} + x^{36} + x^{37} - x^{38} \\
&\quad - x^{39} + x^{40} - x^{41} + x^{42} + x^{43} - x^{44} - x^{45} + x^{46} - x^{47} + x^{48} - x^{49} - x^{50} \\
&\quad + x^{51} + x^{52} - x^{53} - x^{54} + x^{55} - x^{56} + x^{57} - x^{58} - x^{59} + x^{60} + x^{61} - x^{62} \\
&\quad + x^{63} - x^{64} - x^{65} + x^{66} + x^{67} - x^{68} - x^{69} + x^{70} - x^{71} + x^{72} - x^{73} - x^{74} \\
&\quad + x^{75} + x^{76} + x^{77} + x^{78} - x^{79} + x^{80} + x^{81} - x^{82} + x^{83} - x^{84} + x^{85} - x^{86} \\
&\quad + x^{87} + x^{88} - x^{89} + x^{90} - x^{91} - x^{92} - x^{93} - x^{94} - x^{95} + x^{96} + x^{97} - x^{98} \\
&\quad - x^{99} + x^{100} + x^{101} - x^{102} + x^{103}.
\end{aligned}$$

Thus $m^*(104) = 6$.

1.c) $N = 120$.

By Table 2, $m^*(120) \le 6$. By Table 1 and Proposition 2.4, we have $m^*(120) = m^*(48+72) \ge \min(6,6) = 6$.

1.d) $N = 136$.

By Table 2, $m^*(136) \ge 6$. By Proposition 3.5, we get that, if $P \in \mathcal{P}(136,7)$, then $|P(-1)| \ge 128$. By Lemma 3.3, the only option, up to sign, for $(d_{2,0}, d_{2,1})$ is $(64,-64)$. This means that 66 out of 68 elements of $2\mathbf{Z}\cap[0,135]$ belong to A and the other 2 to B, whereas for $(2\mathbf{Z}+1)\cap[0,135]$ the situation is the opposite. Using $p=3$ we see that the only option for $(d_{3,0}, d_{3,1}, d_{3,2})$ is $(0,27,-27)$, which means that exactly 9 out of the 45 elements of $(3\mathbf{Z}+2)\cap[0,135]$ belong to A. Now $2\mathbf{Z}\cap(3\mathbf{Z}+2)\cap[0,135]$ contains 23 elements, which means that at least 21 of them belong to A. This leads to a contradiction, and therefore $m^*(136) = 6$.

1.e) $N = 152$.

By Table 2, $m^*(152) \ge 6$. By Proposition 3.5, we get that, if $P \in \mathcal{P}(152,7)$, then $|P(-1)| \ge 128$. By Lemma 3.3, the only option, up to sign, for $(d_{2,0}, d_{2,1})$ is $(64,-64)$. This means that 70 out of 76 elements of $2\mathbf{Z}\cap[0,151]$ belong to A and the other 6 to B, whereas for $(2\mathbf{Z}+1)\cap[0,151]$ the situation is the opposite. Using $p=3$ we see that the only option for $(d_{3,0}, d_{3,1}, d_{3,2})$ is $(-27,27,0)$, which means that exactly 12 out of the 51 elements of $3\mathbf{Z}\cap[0,151]$ belong to A. Now $2\mathbf{Z}\cap3\mathbf{Z}\cap[0,151]$ contains 25 elements, which means that at least 19 of them belong to A. This leads to a contradiction, and therefore $m^*(152) = 6$.

2.a) $N = 112$.

By Table 2, $m^*(112) \le 7$. Suppose we have a polynomial yielding $m = 7$. We shall examine only the antisymmetric polynomials. By Lemma 3.4 we see that, up to sign, $(d_{3,0}, d_{3,1}, d_{3,2}) = (0,-27,27)$. We know that 32 out of the 37 elements of $(3\mathbf{Z}+2)\cap[0,111]$ belong to A and the other 5 to B, whereas for $(3\mathbf{Z}+1)\cap[0,111]$ the situation is the opposite. We take all $\binom{32}{5}$ options of splitting $(3\mathbf{Z}+2)\cap[0,111]$

and $(3\mathbf{Z}+1)\cap[0,111]$ (in an antisymmetric manner). In order to divide $3\mathbf{Z}\cap[0,111]$, we will use $p=5$. By Proposition 3.4 and the antisymmetry, up to sign we have only the option $(d_{5,0},d_{5,1},d_{5,2},d_{5,3},d_{5,4})=(5,-5,10,0,-10)$. For each splitting of $(3\mathbf{Z}+2)\cap[0,111]$ and $(3\mathbf{Z}+1)\cap[0,111]$, we go over all possibilities of dividing the rest of the elements according to the 2 different possibilities according to the prime 5. After checking about $3\cdot 10^8$ possibilities, we find only one antisymmetric polynomial belonging to $\mathcal{P}(112,7)$:

$$\begin{aligned}1 &- x + x^2 - x^3 - x^4 + x^5 - x^6 + x^7 + x^8 - x^9 - x^{10} + x^{11} + x^{12} - x^{13} - x^{14}\\ &+ x^{15} - x^{16} + x^{17} - x^{18} - x^{19} + x^{20} + x^{21} - x^{22} + x^{23} + x^{24} - x^{25} + x^{26}\\ &+ x^{27} - x^{28} - x^{29} + x^{30} - x^{31} + x^{32} - x^{33} - x^{34} + x^{35} + x^{36} - x^{37} + x^{38}\\ &+ x^{39} - x^{40} + x^{41} - x^{42} - x^{43} - x^{44} + x^{45} - x^{46} + x^{47} + x^{48} - x^{49} + x^{50}\\ &- x^{51} - x^{52} - x^{53} - x^{54} - x^{55} + x^{56} + x^{57} + x^{58} + x^{59} + x^{60} - x^{61} + x^{62}\\ &- x^{63} - x^{64} + x^{65} - x^{66} + x^{67} + x^{68} + x^{69} - x^{70} + x^{71} - x^{72} - x^{73} + x^{74}\\ &- x^{75} - x^{76} + x^{77} + x^{78} - x^{79} + x^{80} - x^{81} + x^{82} + x^{83} - x^{84} - x^{85} + x^{86}\\ &- x^{87} - x^{88} + x^{89} - x^{90} - x^{91} + x^{92} + x^{93} - x^{94} + x^{95} - x^{96} + x^{97} + x^{98}\\ &- x^{99} - x^{100} + x^{101} + x^{102} - x^{103} - x^{104} + x^{105} - x^{106} + x^{107} + x^{108} - x^{109}\\ &+ x^{110} - x^{111}.\end{aligned}$$

Thus, $m^*(112)=7$.

2.b) $N=160$.

By Table 2, $m^*(160)\geq 7$. Suppose we have a polynomial yielding $m\geq 8$. By Proposition 3.4, we easily see that, up to sign, $d_{3,0}=54$. In other words, all 54 elements of $3\mathbf{Z}\cap[0,160]$ are in A. To continue we use $p=7$ and $p=11$. There are 11 different sets of values for $d_{7,j}$, where in each set we have that at least 3 of the $d_{7,j}$'s are -7 (which means that 8 elements from the corresponding residue classes belong to A). As we know 8 of the elements in $(7\mathbf{Z}+j)\cap[0,160]\cap A$ for $j=0,2,3,5,6$, and 7 elements in $(7\mathbf{Z}+j)\cap[0,160]\cap A$ for $j=1,4$, we have at most 256 options to determine all of the classes with 8 elements. For each such choice we complete the division using 11. There are 13 different values for $d_{11,j}$. After checking about $2\cdot 10^{10}$ possibilities, we find that $\mathcal{P}(160,8)$ is empty, which means that $m^*(160)=7$.

3.a) $N=144$.

Suppose we have a polynomial yielding $m\geq 9$. By Proposition 3.4, we easily see that $d_{5,j}=\pm 25$ for $j=0,1,2,3$ (two of them being $+25$ and the other two -25). In other words, two of these residue classes have 27 out of 29 elements in A and the other two elements in B, and the other two classes are the opposite. Now the intersection of any residue class modulo 5 with any residue class modulo 7 contains at least 4 elements in our range. It follows that each of the residue classes modulo 7 contains at least 4 elements from each of the sets A and B. This rules out $d_{7,j}=\pm 21$ for $j=0,1,2,3$ and $d_{7,j}=\pm 14$ for $j=4,5,6$, which leaves no feasible solution. Thus $m^*(144)\leq 8$.

Suppose we have a polynomial yielding $m=8$ for $N=144$. By Proposition 3.4, either $(d_{5,0},d_{5,1},\ldots,d_{5,4})=(5,5,5,5,-20)$ or $d_{5,j}=\pm 25$ for $j=0,1,2,3$. We tried only the first of these. It means that A contains only 4 elements from $(5\mathbf{Z}+4)\cap[0,143]$. Using $p=7$ we focus only on symmetric solutions, and get only 6

possible values for the $d_{7,j}$'s. These possibilities are $\pm(-21,7,7,-21,14,0,14)$, $\pm(-7,-7,-7,-7,14,0,14)$ and $\pm(-7,7,7,-7,0,0,0)$. The first option and its complement are easily checked and do not yield any polynomial in $\mathcal{P}(144,8)$. For the second we bring $p=11$ into play. There are 142 possible values for the $d_{11,j}$'s, most of which are very easily checked after taking into account the constraints for $(5\mathbf{Z}+4)\cap[0,143]$, $(7\mathbf{Z}+4,5,6)\cap[0,143]$. After checking about $4\cdot 10^9$ options, we find that there are exactly 3 symmetric polynomials with $(d_{7,0},d_{7,1},\dots,d_{7,6}) = (-7,-7,-7,-7,14,0,14)$ in $\mathcal{P}(144,8)$. For example, the following polynomial is a member of $\mathcal{P}(144,8)$:

$$\begin{aligned}
&1 - x + x^2 - x^3 + x^4 - x^5 - x^6 + x^7 - x^8 + x^9 + x^{10} - x^{11} - x^{12} - x^{13} + x^{14} \\
&- x^{15} + x^{16} + x^{17} - x^{18} + x^{19} - x^{20} + x^{21} - x^{22} + x^{23} + x^{24} - x^{25} + x^{26} \\
&- x^{27} + x^{28} + x^{29} + x^{30} + x^{31} - x^{32} - x^{33} - x^{34} - x^{35} - x^{36} + x^{37} - x^{38} \\
&+ x^{39} - x^{40} - x^{41} + x^{42} + x^{43} - x^{44} + x^{45} - x^{46} + x^{47} - x^{48} + x^{49} + x^{50} \\
&+ x^{51} - x^{52} - x^{53} + x^{54} - x^{55} - x^{56} - x^{57} + x^{58} + x^{59} - x^{60} - x^{61} - x^{62} \\
&+ x^{63} + x^{64} + x^{65} - x^{66} - x^{67} + x^{68} + x^{69} - x^{70} + x^{71} + x^{72} - x^{73} + x^{74} \\
&+ x^{75} - x^{76} - x^{77} + x^{78} + x^{79} + x^{80} - x^{81} - x^{82} - x^{83} + x^{84} + x^{85} - x^{86} \\
&- x^{87} - x^{88} + x^{89} - x^{90} - x^{91} + x^{92} + x^{93} + x^{94} - x^{95} + x^{96} - x^{97} + x^{98} \\
&- x^{99} + x^{100} + x^{101} - x^{102} - x^{103} + x^{104} - x^{105} + x^{106} - x^{107} - x^{108} \\
&- x^{109} - x^{110} - x^{111} + x^{112} + x^{113} + x^{114} + x^{115} - x^{116} + x^{117} - x^{118} \\
&+ x^{119} + x^{120} - x^{121} + x^{122} - x^{123} + x^{124} - x^{125} + x^{126} + x^{127} - x^{128} \\
&+ x^{129} - x^{130} - x^{131} - x^{132} + x^{133} + x^{134} - x^{135} + x^{136} - x^{137} - x^{138} \\
&+ x^{139} - x^{140} + x^{141} - x^{142} + x^{143}.
\end{aligned}$$

Thus $m^*(144)=8$.

3.b) $N=256$.

By Table 2, $m^*(256)\geq 8$. Suppose we have a polynomial yielding $m=9$. By Proposition 3.4, we easily see that $d_{3,j}=\pm 81$ for $j=1,2$ (one of them being $+81$ and the other -81). In other words, one of these residue classes has 83 out of 85 elements in A and the other 2 in B, and for the other class we have the opposite situation. Now the intersection of any residue class modulo 3 with any residue class modulo 5 contains at least 17 elements in our range. It follows that each of the residue classes modulo 5 contains at least 15 elements from each of the sets A and B. This rules out $d_{5,j}=\pm 25$ for $j=1,2,3,4$, which leaves no feasible solution. Thus $m^*(256)=8$. □

References

[1] J.-P. Allouche and J. Shallit, *The ubiquitous Prouhet-Thue-Morse sequence*, Sequences and their applications, Proceedings of SETA'98 (C. Ding, T. Helleseth & H. Niederreiter, eds.), Spinger-Verlag, 1999, pp. 1–16. MR1843077 (2002e:11025)

[2] D.W. Boyd, *On a problem of Byrnes concerning polynomials with restricted coefficients*, Math. Comp. **66** (1997), 1697–1703. MR1433263 (98a:11033)

[3] D.W. Boyd, *On a problem of Byrnes concerning polynomials with restricted coefficients, II*, Math. Comp. **71** (2002), 1205–1217. MR1898751 (2003d:11035)

[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. MR1081341 (91g:42001)
[5] J.S. Byrnes and D.J. Newman, *Null steering employing polynomials with restricted coefficients*, IEEE Trans. Antennas and Propagation **36** (1988), 301–303.
[6] S. Golan, `http://www.cs.bgu.ac.il/~golansha/polynomials.`
[7] R. Lidl and H. Niederreiter, *Finite Fields*, Addison-Wesley, Reading, 1983. MR0746963 (86c:11106)
[8] V. Skachek, T. Etzion, and R.M. Roth, *Efficient encoding algorithm for third-order spectral-null codes*, IEEE Trans. Inform. Theory **44** (1998), 846–851. MR1607751 (98k:94017)
[9] A. Nijenhuis and H.S. Wilf, *Combinatorial Algorithms*, Academic Press, Orlando, 1978. MR0510047 (80a:68076)
[10] 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.
[11] R.M. Roth, *Spectral-null codes and null spaces of Hadamard submatrices*, Designs, Codes and Cryptography **9** (1996), 177–191. MR1409444 (98e:94034)
[12] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer, New York (1982). MR0718674 (85g:11001)

Department of Computer Science, Ben-Gurion University of the Negev, POB 653, Beer-Sheva 84105 Israel
E-mail address: `berend@cs.bgu.ac.il`

Department of Computer Science, Ben-Gurion University of the Negev, POB 653, Beer-Sheva 84105 Israel
E-mail address: `golansha@cs.bgu.ac.il`