MATHEMATICS OF COMPUTATION
Volume 77, Number 263, July 2008, Pages 1695–1712
S 0025-5718(08)02072-3
Article electronically published on January 29, 2008

EQUAL MOMENTS DIVISION OF A SET

SHAHAR GOLAN

ABSTRACT. Let $N_q^*(m)$ be the minimal positive integer N, for which there exists a splitting of the set $[0, N-1]$ into q subsets, $S_0, S_1, \ldots, S_{q-1}$, whose first m moments are equal. Similarly, let $m_q^*(N)$ be the maximal positive integer m, such that there exists a splitting of $[0, N-1]$ into q subsets whose first m moments are equal. For $q = 2$, these functions were investigated by several authors, and the values of $N_2^*(m)$ and $m_2^*(N)$ have been found for $m \leq 8$ and $N \leq 167$, respectively. In this paper, we deal with the problem for any prime q. We demonstrate our methods by finding $m_3^*(N)$ for any $N < 90$ and $N_3^*(m)$ for $m \leq 6$.

1. Introduction

For $k \in \mathbb{N}$, let ζ_k be a primitive root of unity of order k. Let $\mathcal{P}_q(N)$ denote the set of polynomials of degree $N-1$ with all coefficients in $\{1, \zeta_q, \ldots, \zeta_q^{q-1}\}$. (It will become clear later that N is a more natural parameter than $\deg P$.) Let $\mathcal{P}_q(N, m)$ denote the subset of $\mathcal{P}_q(N)$, consisting of polynomials divisible by $(x-1)^m$ (or by some higher power of $x-1$).

The set $\mathcal{P}_q(N, m)$ has been extensively studied for $q = 2$. It comes up in the design of antenna arrays and notch filters [6], in coding theory in connection with so-called *spectral-null codes*, [12], and is also related to the *Prouhet-Thue-Morse sequence* [1]. In [13] and [8], asymptotics are obtained for its size. An algorithm for enumerating $\mathcal{P}_2(N, 3)$ is described in [7]. A method of encoding data by words in $\mathcal{P}_2(N, 3)$ is defined in [11].

It turns out that the polynomials in $\mathcal{P}_2(N, m)$ have the following property. Given $P \in \mathcal{P}_2(N, m)$, let S_0 be the subset of $\{0, 1, \ldots, N-1\}$, consisting of those k's for which x^k appears in P with a "+" sign, and S_1 the set of those for which it appears with a "-" sign. Then the first m moments of S_0 are equal to those of S_1, i.e.,

$$\sum_{j \in S_0} j^k = \sum_{j \in S_1} j^k, \qquad k = 0, \ldots, m-1. \tag{1.1}$$

In fact, if $S_0 \cup S_1 = \{0, 1, \ldots, N-1\}$ and $S_0 \cap S_1 = \emptyset$, then the equalities in (1.1) imply that

$$P = \sum_{j \in S_0} x^k - \sum_{j \in S_1} x^k \in \mathcal{P}_2(N, m).$$

We shall show (see Proposition 2.1 *infra*) that a similar equivalence exists for any prime q. This means that the problem of finding a polynomial in $\mathcal{P}_q(N, m)$ is

Received by the editor March 19, 2007 and, in revised form, May 23, 2007.
2000 *Mathematics Subject Classification.* Primary 11B83, 12D10; Secondary 94B05, 11Y99.
Key words and phrases. Littlewood polynomials, spectral-null code, antenna array.

equivalent to the problem of splitting the set $\{0, 1, \ldots, N-1\}$ into q subsets, S_0, S_1, …, S_{q-1}, whose first m moments are equal, i.e.,

$$\sum_{j \in S_i} j^k = \sum_{j \in S_{i'}} j^k, \qquad k = 0, \ldots, m-1, \quad 0 \leq i < i' \leq q-1.$$

For a fixed m, let $N_q^*(m)$ be the smallest N for which $\mathcal{P}_q(N,m)$ is non-empty, and for a fixed N let $m_q^*(N)$ be the largest m such that $\mathcal{P}_q(N,m)$ is non-empty. This paper examines the question of finding $m_q^*(N)$ and $N_q^*(m)$ for several values of N and m.

For $q = 2$, the problem has been investigated by Boyd [3], [4]. On the theoretical side, Boyd proved that $N_2^*(m) \geq e^{\sqrt{m}(1+o(1))}$. Moreover, for $m_2^*(N)$ to be large, N has to be divisible by a large power of 2. Boyd was able to calculate $m_2^*(N)$ for all $N < 88$. In particular, he proved that $N^*(6) = 48$, thus disproving a conjecture of Byrnes [5], whereby $N_2^*(m) = 2^m$ for every m. Additionally, he showed that $N_2^*(7) = 96$, but was unable to determine whether $m^*(96)$ is 7 or 8. Boyd's approach is based on an ingenious exploitation of the fact that, if $P(x) \in \mathcal{P}_2(N,m)$, 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 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.

In [2] Berend and the author improved Boyd's approach both theoretically and computationally, which helped in strengthening his results. On the theoretical side, we were able to exploit the full power provided by the information arising from the divisibility of $P(\zeta_p)$ by $(\zeta_p - 1)^m$ to get better constraints on the values of the polynomial's coefficients. On the computational side, we combined the information obtained from different primes to further shorten the search. Using these improvements, we were able extend the range of N's with known $m^*(N)$ from $N < 88$ to $N < 168$. In particular, we were able show that $m^*(96) = 7$ and $m^*(144) = 8$ (so that $N^*(8) = 144$).

As mentioned above, in this paper we deal with the problem for any prime q, and generalize the results achieved in [3], [4] and [2]. We demonstrate our methods by finding $m_3^*(N)$ for any $N < 90$ and $N_3^*(m)$ for $m \leq 6$. We also determine $m_3^*(N)$ for any N with $m_3^*(N) < 5$.

In Section 2 we present the main results. Section 3 contains a few auxiliary results on equal moments divisions of a set. In Section 4 we derive some simple results on cyclotomic fields, on which we base our methods. The proofs of the main results are given in Section 5. In Section 6 we describe the methods and heuristics that were used for scanning the search range.

To prove that $m_3^*(N)$ 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 [9].

Acknowledgments. I would like to express my deep gratitude to Daniel Berend, for his careful reading and for his (many) helpful comments. I would also like to thank the anonymous reviewer of this paper for his detailed and helpful comments.

2. The main results

We start with the equivalence of the two problems discussed in the previous section.

Proposition 2.1. *Let q be a prime, and m a positive integer. Let S_i, $0 \le i \le q-1$, be finite multisets of non-negative integers. Then*

$$\sum_{j \in S_i} j^k = \sum_{j \in S_{i'}} j^k, \qquad k = 0, \dots, m-1, \quad 0 \le i < i' \le q-1, \tag{2.1}$$

if and only if

$$(x-1)^m \mid \sum_{i=0}^{q-1} \zeta_q^i \sum_{j \in S_i} x^j. \tag{2.2}$$

Remark. The implication (2.1) ⇒ (2.2) holds for every q, prime or not. In fact, going over the proof of Proposition 2.1, we can see that, in this direction, the primality of q is not used. However, the implication (2.2) ⇒ (2.1) is false for every composite q. Indeed, if $q = dl$, let $S_{di} = \{i\}$, $0 \le i < l$, and$S_j = \emptyset$, for $0 \le j < dl$ with $d \nmid j$. Then the right-hand side of (2.2) is

$$\sum_{i=0}^{l-1} \zeta_l^i x^i = \frac{x^l - 1}{\zeta_l x - 1}, \tag{2.3}$$

which is divisible by $x-1$, yet the 0-th moment of S_0 (i.e., its size, which is 1) differs from that of S_1 (which is 0).

The following results, from Theorem 2.2 up to Corollary 2.6 are simple generalizations of their analogues in the case $q = 2$, proved by Boyd [3], but due to their importance we state them explicitly (with proofs, except for Theorem 2.4).

Theorem 2.2. *If $\mathcal{P}_q(N, m)$ is non-empty and $q^k \parallel N$, then $m \le q^k - 1$.*

Corollary 2.3. *If $\mathcal{P}_q(N, m)$ is non-empty and $m \ge q^k$, then $q^{k+1} \mid N$.*

Theorem 2.4. *If $\mathcal{P}_q(N, m)$ is non-empty, then $N \ge \exp(\sqrt{m}(1 + o(1)))$.*

The proof of this theorem is very similar to the one given in [3] (based on Theorem 3.6 *infra*), and will be omitted.

In the next proposition we provide lower bounds for $m_q^*(2N)$, $m_q^*(N_1 + N_2)$ and $m_q^*(N_1 N_2)$ in terms of $m_q^*(N)$, $m_q^*(N_1)$ and $m_q^*(N_2)$. Note that the proof is constructive. Namely, given polynomials $P_1 \in \mathcal{P}_q(N, m)$, $P_2 \in \mathcal{P}_q(N_1, m_1)$, and $P_3 \in \mathcal{P}_q(N_2, m_2)$, we explicitly construct polynomials in $\mathcal{P}_q(2N)$, $\mathcal{P}_q(N_1 + N_2)$ and $\mathcal{P}_q(N_1 N_2)$ with zeros of the prescribed order at 1.

Proposition 2.5. *For any N, N_1, N_2 we have:*

1. *If $m_q^*(N)$ is odd, then $m_q^*(2N) \ge m_q^*(N) + 1$.*
2. *$m_q^*(N_1 + N_2) \ge \min(m_q^*(N_1), m_q^*(N_2))$.*
3. *$m_q^*(N_1 N_2) \ge m_q^*(N_1) + m_q^*(N_2)$.*

Corollary 2.6.

$$N_q^*(m) \le \begin{cases} (2q)^{m/2}, & m \equiv 0 \pmod{2}, \\ 2^{(m-1)/2} q^{(m+1)/2}, & m \equiv 1 \pmod{2}. \end{cases}$$

The rest of the section deals with the case $q = 3$. The next result provides the value of $m_3^*(N)$ for every N with $m^*(N) < 5$.

Theorem 2.7.

1. *$m_3^*(N) = 0$ if and only if $3 \nmid N$.*
2. *$m_3^*(N) = 1$ if and only if $N = 3$.*
3. *$m_3^*(N) = 2$ if and only if either $N = 9$ or both $3 \parallel N$ and $N \geq 6$.*
4. *$m_3^*(N) = 3$ if and only if $N \in \{18, 27\}$.*
5. *$m_3^*(N) = 4$ if and only if $N \in \{36, 45, 54, 63\}$.*
6. *$m_3^*(N) \geq 5$ if and only if $3^2 \mid N$ and $N \geq 72$.*

In the next theorem we provide the value of $m_3^*(N)$ for several N's which are not covered by Theorem 2.7, and lower bounds for several others.

Theorem 2.8.

1. *For $N \in \{72, 81, 99, 117\}$ we have $m_3^*(N) = 5$.*
2. *For $N \in \{90, 108, 126\}$ we have $m_3^*(N) \geq 6$.*

From Theorems 2.7 and 2.8 we immediately obtain

Theorem 2.9. *Table 1 gives the values of $N_3^*(m)$ for $m \leq 6$.*

m	1	2	3	4	5	6
$N_3^*(m)$	3	6	18	36	72	90

TABLE 1. Values of $N_3^*(m)$ for $1 \leq m \leq 6$

3. AUXILIARY RESULTS ON EQUAL MOMENTS DIVISIONS

Lemma 3.1. *Let q be a prime, and S_i, $0 \leq i \leq q-1$, be finite multi-sets of integers. Then, for any non-negative integer m,*

$$(x-1)^m \mid \sum_{i=0}^{q-1} \zeta_q^i \sum_{j \in S_i} x^j \tag{3.1}$$

if and only if

$$\sum_{i=0}^{q-1} \zeta_q^i \sum_{j \in S_i} j^k = 0, \qquad k = 0, 1, \ldots, m-1. \tag{3.2}$$

Note that, if S_i contains negative elements, the polynomials on the right hand-side of (3.1) belong to $\mathbb{Z}[x, \frac{1}{x}]$.

Proof. We use induction on m. For $m = 0$, the lemma is trivial. Suppose the lemma holds for some m, and assume that

$$(x-1)^{m+1} \mid P(x) = \sum_{i=0}^{q-1} \zeta_q^i \sum_{j \in S_i} x^j$$

and

$$(x-1)^{m+2} \nmid \sum_{i=0}^{q-1} \zeta_q^i \sum_{j \in S_i} x^j.$$

By the induction hypothesis

$$\sum_{i=0}^{q-1} \zeta_q^i \sum_{j \in S_i} j^k = 0, \qquad k = 0, 1, \ldots, m-1.$$

Now

$$P^{(m)}(x) = \sum_{i=0}^{q-1} \zeta_q^i \sum_{j \in S_i} j(j-1) \cdot \ldots \cdot (j-m+1) x^{j-m}. \tag{3.3}$$

Since $(x-1)^{m+1} \mid P(x)$, we have $(x-1) \mid P^{(m)}(x)$, so that $P^{(m)}(1) = 0$, and by (3.3)

$$\sum_{i=0}^{q-1} \zeta_q^i \sum_{j \in S_i} j(j-1) \cdot \ldots \cdot (j-m+1) = 0. \tag{3.4}$$

For fixed m, the expression $j(j-1) \cdot \ldots \cdot (j-m+1)$, considered as a polynomial in j, is a linear combination of the polynomials $j^k,\ k = 1, \ldots, m$. By the induction hypothesis we get

$$\sum_{i=0}^{q-1} \zeta_q^i \sum_{j \in S_i} j^k = 0, \qquad k = 0, \ldots, m-1. \tag{3.5}$$

Subtracting from the left-hand side of (3.4) appropriate multiples of the left-hand side of (3.5) for $k = 1, \ldots, m-1$, we obtain:

$$\sum_{i=0}^{q-1} \zeta_q^i \sum_{j \in S_i} j^m = 0.$$

Similarly

$$\sum_{i=0}^{q-1} \zeta_q^i \sum_{j \in S_i} j^{m+1} \neq 0.$$

□

Corollary 3.2. *Let S_i, $0 \le i \le q-1$, be finite multi-sets of integers, where $q \ge 2$. Given any non-negative integer m, and any integer c, the system of equalities*

$$\sum_{i=0}^{q-1} \zeta_q^i \sum_{j \in S_i} j^k = 0, \qquad k = 0, 1, \ldots, m-1,$$

and

$$\sum_{i=0}^{q-1} \zeta_q^i \sum_{j \in S_i} (j+c)^k = 0, \qquad k = 0, 1, \ldots, m-1,\ c \in \mathbb{Z},$$

are equivalent.

Proof. Let $P(x) = \sum_{i=0}^{q-1} \zeta_q^i \sum_{j\in S_i} x^j$. By Lemma 3.1 we have, $\sum_{i=0}^{q-1} \zeta_q^i \sum_{j\in S_i} j^k = 0$ for $k = 0, 1, \dots, m-1$, if and only if $(x-1)^m \mid P(x)$. Now $(x-1)^m \mid P(x)$ if and only if $(x-1)^m \mid x^c P(x) = \sum_{i=0}^{q-1} \zeta_q^i \sum_{j\in S_i} x^{j+c}$. Using Lemma 3.1 again we get that this is equivalent to $\sum_{i=0}^{q-1} \zeta_q^i \sum_{j\in S_i} (j+c)^k = 0$ for $k = 0, 1, \dots, m-1$. □

A polynomial P of degree $N-1$ is *symmetric* if $P(x) = x^{N-1}P(\frac{1}{x})$. (Such polynomials are sometimes called *reciprocal* or *palindromic.*)

Corollary 3.3. *If $P(x) \in \mathcal{P}_q(N, m)$, with m odd, is a symmetric polynomial, then $P(x) \in \mathcal{P}_q(N, m+1)$.*

Proof. Let $P(x) = \sum_{i=0}^{q-1} \zeta_q^i \sum_{j\in S_i} x^j$ for appropriate sets S_i, $0 \le i \le q-1$. By Lemma 3.1 we have $\sum_{i=0}^{q-1} \zeta_q^i \sum_{j\in S_i} j^k = 0$ for $k = 0, 1, \dots, m-1$. Since P is symmetric, S_i contains a number t if and only if it contains $N-1-t$. This implies that, if k is a positive odd integer, then $\sum_{j\in S_i} (2j - N + 1)^k = 0$ for each i. In particular, this holds for $k = m$. Thus, for the sets $S_i' = \{2j - N + 1 : j \in S_i\}$ we obtain $\sum_{i=0}^{q-1} \zeta_q^i \sum_{j\in S_i'} j^m = 0$. Hence from Corollary 3.2 we get $\sum_{i=0}^{q-1} \zeta_q^i \sum_{j\in S_i} (2j)^m = 2^m \sum_{i=0}^{q-1} \zeta_q^i \sum_{j\in S_i} j^m = 0$. Using Lemma 3.1 again we obtain $P(x) \in \mathcal{P}_q(N, m+1)$. □

Lemma 3.4. *If $P \in \mathcal{P}_q(N)$ and $Q \in \mathcal{P}_q(M)$, where $Q \mid P$, then $M \mid N$.*

Put $A_d(x) = 1 + x + \ldots + x^{d-1} = (x^d - 1)/(x-1)$. Clearly, if $P \in \mathcal{P}_q(N)$, then $P \equiv A_N \pmod{\zeta_q - 1}$. We agree that $A_0(x) = 0$.

Proof. Suppose $N = kM + r$, with $0 \le r < M$. One easily verifies that

$$A_N(x) = x^r A_k(x^M) A_M(x) + A_r(x). \tag{3.6}$$

Since $P(x) \equiv A_N(x) \pmod{\zeta_q - 1}$ and $Q(x) \equiv A_M(x) \pmod{\zeta_q - 1}$, this implies

$$A_N(x) \equiv Q_0(x) A_M(x) \pmod{\zeta_q - 1} \tag{3.7}$$

for some polynomial Q_0 over $\mathbb{Z}[\zeta_q]$. This means that $A_M \mid A_r \pmod{\zeta_q - 1}$. This can be true only if $r = 0$. Thus $M \mid N$. □

Corollary 3.5. *Let $P \in \mathcal{P}_q(N)$. If $P(\zeta_p) = 0$ for some prime $p \ne q$, then $p \mid N$.*

Proof. The minimal polynomial of ζ_p over $\mathbb{Z}[\zeta_q]$ is $A_p(x)$, which is in $\mathcal{P}_q(p)$. The condition $P(\zeta_p) = 0$ is therefore equivalent to $A_p(x) \mid P(x)$, which by Lemma 3.4 requires that $p \mid N$. □

Theorem 3.6. *If $\mathcal{P}_q(N, m)$ is non-empty and $p \ne q$ is a prime not dividing N, then $N \ge (p^{1/(p-1)})^m$.*

Proof. If $P \in \mathcal{P}_q(N, m)$, then $P(x) = (x-1)^m Q(x)$ for some $Q \in \mathbb{Z}[\zeta_q][x]$. By Corollary 3.5, we have $P(\zeta_p) \ne 0$. Computing the norm of $P(\zeta_p)$ over $\mathbb{Z}[\zeta_q]$, and using the equality $\prod_{j=1}^{p-1}(1 - \zeta_p^j) = A_p(1) = p$, we obtain

$$0 \ne \prod_{j=1}^{p-1} P(\zeta_p^j) = \pm p^m \prod_{j=1}^{p-1} Q(\zeta_p^j) = \pm p^m Q_1(\zeta_q)$$

for some $Q_1 \in \mathbb{Z}[x]$. Computing the norm of $p^m Q_1(\zeta_q)$ over $\mathbb{Z}$ we get:

$$\prod_{k=1}^{q-1} p^m Q_1(\zeta_q^j) = p^{(q-1)m} \prod_{k=1}^{q-1} Q_1(\zeta_q^j).$$

The estimates $|P(\zeta_p^j)| \leq N$ and $|\prod Q_1(\zeta_q^j)| \geq 1$ give

$$\begin{aligned} N^{(p-1)(q-1)} &= \mathrm{Norm}_{\mathbb{Z}[\zeta_{pq}]/\mathbb{Z}}(N) \geq |\mathrm{Norm}_{\mathbb{Z}[\zeta_{pq}]/\mathbb{Z}}(P(\zeta_p))| \\ &= |p^{(q-1)m} \prod_{k=1}^{q-1} Q_1(\zeta_q^j)| \geq p^{(q-1)m}, \end{aligned} \tag{3.8}$$

which completes the proof. □

4. 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 p is a prime. Throughout this section, we shall always assume that $p \neq q$. For any n, denote $\mathbb{O}_n = \mathbb{Z}[\zeta_n]$. In [2], we developed an exact criterion for divisibility by high powers of $(\zeta_p - 1)$ in the ring $\mathbb{O}_p$ (and, more generally, for divisibility by high powers of $(\zeta_{p^k} - 1)$ in the ring $\mathbb{O}_{p^k}$). This allowed us to reduce, substantially in most cases, the search space. Here we expand this criterion to a criterion for divisibility in $\mathbb{O}_{p^k q}$. In Proposition 4.2 we accomplish it for $(\zeta_{p^k} - 1)$. Proposition 4.5 strengthens Proposition 4.2 for the case where $k = 1$. These two propositions, and the lemmas used in their proofs, are completely analogous to their counterparts in the case $q = 2$ [2], except that the numbers A_j appearing there are now algebraic integers, and not rational integers. To make the paper self-contained we include the proofs.

Recall that $(\zeta_{p^k} - 1)^{\varphi(p^k)}/p$ is a unit in $\mathbb{O}_{p^k q}$ (cf. [14]), i.e., a number in $\mathbb{O}_{p^k q}$ is divisible by $(\zeta_{p^k} - 1)^{\varphi(p^k)}$ if and only if it is divisible by p.

Lemma 4.1. *A number in $\mathbb{O}_q$ is divisible by $\zeta_{p^k} - 1$ if and only if it is divisible by p. In other words $(\zeta_{p^k} - 1)\mathbb{O}_{p^k q} \cap \mathbb{O}_q = p\mathbb{O}_q$.*

For simplicity of notation we will prove the lemma for the case $k = 1$. The proof for $k > 1$ is very similar.

Proof. The inclusion $(\zeta_p - 1)\mathbb{O}_{pq} \cap \mathbb{O}_q \supseteq p\mathbb{O}_q$ is trivial. Since $p \neq q$, the prime p does not ramify in $\mathbb{O}_q$. That is, $p\mathbb{O}_q = \mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_k$ for some distinct prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_k \subseteq \mathbb{O}_q$. The inertia degree $f(\mathfrak{p}_i/p)$ is $(q-1)/k$ for every i. In $\mathbb{O}_p$ we have $(p) = (1 - \zeta_p)^{p-1}$. Next consider the factorization $(1 - \zeta_p) = \mathfrak{P}_1\mathfrak{P}_2 \ldots \mathfrak{P}_l$ in the ring $\mathbb{O}_{pq}$ into a product of (not necessarily distinct) prime ideals $\mathfrak{P}_i \subseteq \mathbb{O}_{pq}$. Hence in $\mathbb{O}_{pq}$ we have $(p) = (\mathfrak{P}_1\mathfrak{P}_2 \ldots \mathfrak{P}_l)^{p-1}$. As $\gcd(\mathfrak{p}_i, \mathfrak{p}_j) = (1)$ for $i \neq j$, the number l of ideals in the factorization of $(1 - \zeta_p)$ in $\mathbb{O}_{pq}$ is at least k; in fact, otherwise we would have distinct ideals $\mathfrak{p}_i$ divisible by the same ideal $\mathfrak{P}_j$. Without loss of generality, assume $\mathfrak{P}_i \mid \mathfrak{p}_i,\ 1 \leq i \leq k$. Then

$$\varphi(pq)/(p-1) = q - 1 = \sum_{i=1}^{l} f(\mathfrak{P}_i/p) \geq \sum_{i=1}^{k} f(\mathfrak{P}_i/p) \geq \sum_{i=1}^{k} f(\mathfrak{p}_i/p) = q - 1.$$

In particular, $l = k$. Now

$$(\zeta_p - 1)\mathbb{O}_{pq} \cap \mathbb{O}_q = \mathfrak{P}_1\mathfrak{P}_2 \ldots \mathfrak{P}_k \cap \mathbb{O}_q = \bigcap_{i=1}^{k} \mathfrak{P}_i \cap \mathbb{O}_q = \bigcap_{i=1}^{k} \mathfrak{p}_i = p\mathbb{O}_q. \qquad \square$$

Throughout this section, β will denote an element of $\mathbb{O}_{p^k q}$ with a (non-unique) representation of the form

$$\beta = A_0 + A_1\zeta_{p^k} + A_2\zeta_{p^k}^2 + \ldots + A_{p^k-1}\zeta_{p^k}^{p^k-1}, \qquad A_j \in \mathbb{Z}[\zeta_q], \quad 0 \le j < p^k.$$

Proposition 4.2. *A number $\beta \in \mathbb{O}_{p^k q}$ is divisible by $(\zeta_{p^k} - 1)^{l\varphi(p^k)+r}$, where $l \ge 0$ and $1 \le r < \varphi(p^k)$, if and only if both of the following conditions are satisfied:*

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 $\beta/p^l = A'_0 + A'_1\zeta_{p^k} + A'_2\zeta_{p^k}^2 + \ldots + A'_{p^k-1}\zeta_{p^k}^{p^k-1}$ for appropriate integers $A'_0, A'_1, \ldots, A'_{p^k-1}$, we have:

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

The proposition immediately follows from the following two lemmas.

Lemma 4.3. *A number $\beta \in \mathbb{O}_{p^k q}$ is divisible by $(\zeta_{p^k} - 1)^r$, where $r < \varphi(p^k)$, if and only if*

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

Proof. Write:

$$\begin{aligned}\beta &= A_0 + A_1((\zeta_{p^k} - 1) + 1) + \ldots + A_{p^k-1}((\zeta_{p^k} - 1) + 1)^{p^k-1} \\ &= \textstyle\sum_{j=0}^{p^k-1} \left(\binom{j}{j}A_j + \binom{j+1}{j}A_{j+1} + \ldots + \binom{p^k-1}{j}A_{p^k-1}\right)(\zeta_{p^k} - 1)^j.\end{aligned} \tag{4.1}$$

We prove the lemma by induction on r. For $r = 1$, since $(\zeta_{p^k} - 1) \mid \beta$, by (4.1) we have $(\zeta_{p^k} - 1) \mid \binom{0}{0}A_0 + \binom{1}{0}A_1 + \ldots + \binom{p^k-1}{0}A_{p^k-1}$, and therefore $p \mid \sum_{j=0}^{p^k-1} \binom{j}{0}A_j$ by Lemma 4.1.

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

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

The sum on the left-hand side is the coefficient of $(\zeta_{p^k} - 1)^j, 0 \le j < r - 1$, in (4.1). The coefficient of $(\zeta_{p^k} - 1)^{r-1}$ is $\binom{r-1}{r-1}A_{r-1} + \binom{r}{r-1}A_r + \ldots + \binom{p^k-1}{-1}A_{p^k-1}$ and it must be divisible by $(\zeta_{p^k} - 1)$, which means it must be divisible by p by Lemma 4.1. $\square$

Lemma 4.4. *A number $\beta \in \mathbb{O}_{p^k q}$ is divisible by $(\zeta_{p^k} - 1)^{l\varphi(p^k)}$ if and only if, for each $0 \le j < p^{k-1}$, 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 $\zeta_{p^k}^{\varphi(p^k)} = -1 - \zeta_{p^k}^{p^{k-1}} - \ldots - \zeta_{p^k}^{(p-2)p^{k-1}}$ to express β as a linear combination of the $\zeta_{p^k}^j$'s, $0 \le j \le \varphi(p^k) - 1$:

$$\beta = \sum_{i=0}^{p^{k-1}-1} \sum_{j=0}^{p-2} \zeta_{p^k}^{jp^{k-1}+i} \left(A_{jp^{k-1}+i} - A_{\varphi(p^k)+i} \right).$$

Since $(\zeta_{p^k} - 1)^{l\varphi(p^k)} \mid \beta$ and $(\zeta_{p^k} - 1)^{\varphi(p^k)}/p$ is a unit in $\mathbb{O}_{p^k q}$, we have $p^l \mid \beta$. A number in $\mathbb{O}_{p^k q}$ is divisible by p^l 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. Hence for each i and j we have $A_{jp^{k-1}+i} \equiv A_{\varphi(p^k)+i} \bmod p^l$, and therefore $A_i \equiv A_{i+p^{k-1}} \bmod p^l$ for $0 \le i < \varphi(p^k)$. □

For the next proposition we assume that $k = 1$. From Lemma 4.3 we easily get that, if $\beta \in (\zeta_p - 1)\mathbb{O}_{pq}$, then β has a unique representation of the form

$$\beta = A_0 + A_1\zeta_p + A_2\zeta_p^2 + \ldots + A_{p-1}\zeta_p^{p-1}, \quad \sum_{j=0}^{p-1} A_j = 0. \tag{4.2}$$

Proposition 4.5. *Let $\beta \in (\zeta_p - 1)\mathbb{O}_{pq}$, Then β is divisible by $(\zeta_p - 1)^{l(p-1)+r}$, where $l \ge 0$ and $1 \le r < p - 1$ or both $r = 1$ and $p = 2$, if and only if in the representation* (4.2) *both of the following conditions are satisfied:*

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:*

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

Proof. We know that β is divisible by p^l. Put $\beta' = \beta/p^l$. Write $\beta = B'_0 + B'_1\zeta_p + B'_2\zeta_p^2 + \ldots + B'_{p-1}\zeta_p^{p-1}$, where $\sum_{j=0}^{p-1} B'_j = 0$. Now β' is divisible by $(\zeta_p - 1)^r$. In case $p \ne 2$, Lemma 4.3 gives

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

If $p = 2$ and $r = 1$, since β' is divisible by 2 we get $B'_0 + B'_1 \equiv 0 \pmod 2$. Hence in either case $\beta = p^l\beta' = p^lB'_0 + p^lB'_1\zeta_p + p^lB'_2\zeta_p^2 + \ldots + p^lB'_{p-1}\zeta_p^{p-1}$, 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 $0 \le j \le p - 1$. □

5. Proofs of the main results

Proof of Proposition 2.1. From Lemma 3.1 we get that

$$(x-1)^m \mid \sum_{i=0}^{q-1} \zeta_q^i \sum_{j \in S_i} x^j$$

if and only if

$$\sum_{i=0}^{q-1} \left(\sum_{j \in S_i} j^k \right) \zeta_q^i = 0, \qquad k = 0, 1, \ldots, m-1. \tag{5.1}$$

Since the minimal polynomial of ζ_q is $1+x+\ldots+x^{q-1}$, this happens if and only if

$$\sum_{j\in S_i} j^k = \sum_{j\in S_{i'}} j^k, \qquad k=0,\ldots,m-1. \tag{5.2}$$ □

Proof of Theorem 2.2. Write $N=q^kM$ with $q\nmid M$. Suppose $P\in\mathcal{P}_q(N,m)$. Then, writing $t=x-1$, the Taylor expansion of P at 1 is of the form

$$P(1+t)=c_mt^m+c_{m+1}t^{m+1}+\ldots. \tag{5.3}$$

On the other hand, modulo ζ_q-1 we have

$$\begin{aligned} P(1+t) &\equiv A_N(1+t)=t^{-1}((1+t)^N-1)\\ &=t^{-1}((1+t)^{q^kM}-1)\equiv t^{-1}((1+t^{q^k})^M-1)\\ &\equiv Mt^{q^k-1}+\binom{M}{2}t^{2q^k-1}+\binom{M}{3}t^{3q^k-1}+\ldots. \end{aligned} \tag{5.4}$$

Comparing (5.3) and (5.4), we see that $m\le q^k-1$. □

Proof of Proposition 2.5. In each part we present a polynomial divisible by the required power of $(x-1)$. Let $P(x)\in\mathcal{P}_q(N,m)$ with m odd, $P_1(x)\in\mathcal{P}_q(N_1,m_1)$, and $P_2(x)\in\mathcal{P}_q(N_2,m_2)$.

1. The polynomial $P(x)+x^{2N-1}P(1/x)$ is clearly symmetric, and it is easily seen to belong to $\mathcal{P}_q(2N,m)$. By Corollary 3.3, it belongs to $\mathcal{P}_q(2N,m+1)$.
2. 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 from $\{1,\zeta_q,\ldots,\zeta_q^{q-1}\}$, and it is divisible by $(x-1)^m$. Thus $P_1(x)+x^{N_1}P_2(x)\in\mathcal{P}_q(N_1+N_2,m)$.
3. 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 from $\{1,\zeta_q,\ldots,\zeta_q^{q-1}\}$, 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 $P_1(x)P_2(x^{N_1})\in\mathcal{P}_q(N_1N_2,m_1+m_2)$. □

Now we turn to the proofs of Theorems 2.7 and 2.8, which determine the value of $m_3^*(N)$ for various N's. In the course of the proofs, we use the results of Section 4 in the following way: Let $P\in\mathcal{P}_q(N,m)$ for a certain $m>0$. Let S_0 be the set of indices of the $\zeta_q^0=1$ coefficients in the polynomial, S_1 the corresponding set for the ζ_q^1's, and so on. For a prime power p^k, $0\le i\le q-1$ and $0\le j\le p^k-1$, denote by $d_{i,p^k,j}$ the number of elements of S_i, congruent to j modulo p^k, namely $d_{i,p^k,j}=|S_i\cap(p^k\mathbb{Z}+j)|$. Put

$$\mathbf{d}_{p^k,j}=(d_{0,p^k,j},d_{1,p^k,j},\ldots,d_{q-1,p^k,j}).$$

It is easy to see that

$$P(\zeta_{p^k})=A_{p^k,0}+A_{p^k,1}\zeta_{p^k}+A_{p^k,2}\zeta_{p^k}^2+\ldots+A_{p^k,p^k-1}\zeta_{p^k}^{p^k-1} \tag{5.5}$$

with

$$A_{p^k,j}=d_{0,p^k,j}+d_{1,p^k,j}\zeta_q+\ldots+d_{q-1,p^k,j}\zeta_q^{q-1}. \tag{5.6}$$

Since $m>0$, we have $\sum_{j=0}^{p^k-1}A_{p^k,j}=0$. The results of Section 4 give strict conditions on the $A_{p^k,j}$'s, and thus restrictions on the $\mathbf{d}_{p^k,j}$'s.

For the next proofs we will denote the members of $\mathcal{P}_3(N)$ by writing the S_i's explicitly. For example, the polynomial $1+\zeta_3x+\zeta_3^2x^2$ will be denoted by $\{0\}\{1\}\{2\}$.

Proof of Theorem 2.7. In each of parts 1-6 of the theorem, it will suffice to prove only that $m_3^*(N)$ 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_3^* will then follow once we are done with the other parts of the theorem.

1. Since N is not divisible by 3, neither is $P(1)$, which means that $(x-1)$ does not divide P.
2. The polynomial $1+\zeta_3 x+\zeta_3^2 x^2$ is divisible by $x-1$. Obviously, no quadratic polynomial with ζ_3^j coefficients is divisible by $(x-1)^2$.
3. By Proposition 2.5 we have $m_3^*(6) \geq 2$, $m_3^*(9) \geq 2$, and therefore Proposition 2.5 implies $m_3^*(N) \geq 2$ for every $N \geq 6$ with $3 \mid N$. A short search shows that $m_3^*(9) = 2$. By Theorem 2.2, if $9 \nmid N$, then $\mathcal{P}_3(N,3)$ is empty.
4. By Proposition 2.5 we have $m_3^*(18) \geq 3$, $m_3^*(27) \geq 3$. A short search shows that $m_3^*(18) = m_3^*(27) = 3$.
5. We treat each of the numbers separately:

   a. $N = 36$.
   By Proposition 2.5, we have $m_3^*(36) \geq 4$. Using Proposition 4.5 with $p = 5$, we see that no polynomial $P \in \mathcal{P}_3(36)$ satisfies $(\zeta_5 - 1)^5 \mid P(\zeta_5)$. Indeed, such a polynomial would have $A_{5,1}$ divisible by 5, meaning that all $d_{i,5,0}$'s are congruent modulo 5. Since $d_{0,5,1} + d_{1,5,1} + d_{2,5,1} = |(5\mathbb{Z}+1) \cap [0,35]| = 7$, there is no possible value for $A_{5,1}$. This means that $m_3^*(36) = 4$.

   b. $N = 45$.
   Suppose we have a polynomial yielding $m = 4$. By Proposition 4.5 with $p = 2$, we get that the $A_{2,j}$'s must be divisible by 8. This means that $(d_{0,2,0} - d_{2,2,0})$, $(d_{1,2,0} - d_{2,2,0})$, $(d_{0,2,1} - d_{2,2,1})$, and $(d_{1,2,1} - d_{2,2,1})$ are all divisible by 8. Additionally, from the definition of $d_{i,p^k,j}$ we obtain $d_{0,2,0} + d_{1,2,0} + d_{2,2,0} = 23$ and $d_{0,2,1} + d_{1,2,1} + d_{2,2,1} = 22$ (since there are 23 even elements in $[0,44]$ and 22 odd elements in this range). The only option for the $\mathbf{d}_{2,j}$'s is $(\mathbf{d}_{2,0}, \mathbf{d}_{2,1}) = ((13,5,5),(2,10,10))$. After scanning the range of possible polynomials for a few seconds, we already get more than 10 members of $\mathcal{P}_3(45,4)$, for example:
   $\{4,5,6,7,8,18,22,24,26,28,30,32,36,40,44\}$,
   $\{0,3,10,11,13,17,19,20,21,29,31,37,38,39,42\}$,
   $\{1,2,9,12,14,15,16,23,25,27,33,34,35,41,43\}$.
   Since the only option for $A_{2,0}$, dictated by the value of $\mathbf{d}_{2,0}$, is not divisible by 16, we have $m_3^*(45) = 4$.

   c. $N = 54$.
   By Proposition 2.5, we have $m_3^*(54) \geq 4$. Suppose we have a polynomial yielding $m = 5$. Using Proposition 4.5 with $p = 5$, we obtain 9 options, up to symmetry, for the $\mathbf{d}_{5,j}$'s. After searching $\approx 5 \cdot 10^9$ options, we find no polynomial divisible by $(x-1)^5$. This means that $m_3^*(54) = 4$.

   d. $N = 63$.
   Suppose we have a polynomial yielding $m = 4$. By Proposition 4.5, we get that up to symmetry, the $\mathbf{d}_{2,j}$'s are equal to $((0,16,16),(21,5,5))$ or $((8,8,16),(13,13,5))$. Using the first option we get that S_0 does not contain any even elements. We continue by using Proposition 4.5 with $p = 5$. One of the options for the $\mathbf{d}_{5,j}$'s is $((3,5,5)$, $(3,5,5)$, $(3,5,5)$,

$(6,3,3)$, $(6,3,3))$. After scanning the range of possible polynomials for a few seconds, we already get a few members of $\mathcal{P}_3(63,4)$, for example:
$\{3,5,7,9,11,13,19,23,27,29,31,33,35,39,43,49,51,53,55,57,59\}$,
$\{2,4,8,10,12,14,18,24,25,26,28,36,41,42,45,46,47,50,52,60,61\}$,
$\{0,1,6,15,16,17,20,21,22,30,32,34,37,38,40,44,48,54,56,58,62\}$.
Suppose we have a polynomial yielding $m = 5$. Using Proposition 4.5 with $p = 5$, we get that the only option for the $\mathbf{d}_{2,j}$'s is $(\mathbf{d}_{2,0}, \mathbf{d}_{2,1}) = ((0,16,16),(21,5,5))$. After searching $\binom{32}{0}\binom{31}{21} \approx 4 \cdot 10^7$ options, we find that there is no polynomial divisible by $(x-1)^5$. This means that $m_3^*(63) = 4$.

6. If $N = 72, 81, 90, 99, 108, 117, 126$, then by Theorem 2.8 we have $m_3^*(N) \geq 5$. Proposition 2.5 gives $m_3^*(135) = m_3^*(45 \cdot 3) \geq m_3^*(45) + m_3^*(3) = 5$. Again, by Proposition 2.5, this implies $m_3^*(N) \geq 5$ for any N satisfying the condition of this part. On the other hand, if $9 \nmid N$, then $m_3^*(N) \leq 2$ by Theorem 2.2, while if $9 \mid N$ and $N < 72$, then $m_3^*(N) \leq 5$ by the preceding parts. □

Given a division of $[0, N-1]$ into subsets $S_0, \ldots, S_{q-1}$, the *reflection* of S_i, denoted by $r(S_i)$, is the set $\{j : N - j - 1 \in S_i\}$. A subset S_i is *symmetric* if $S_i = r(S_i)$. A subset-couple (S_{i_1}, S_{i_2}) is *anti-symmetric* if $S_{i_2} = r(S_{i_1})$. Note that a polynomial in $\mathcal{P}_q(N,m)$ is symmetric if and only if all the subsets S_i are symmetric. A polynomial in $\mathcal{P}_2(N,m)$ is *anti-symmetric* if the pair (S_0, S_1) is anti-symmetric. For odd q, a polynomial in $\mathcal{P}_q(N,m)$ is *anti-symmetric* if S_0 is symmetric and (S_{2i-1}, S_{2i}) is anti-symmetric for $1 \leq i \leq \frac{q-1}{2}$.

Proof of Theorem 2.8. 1.a) $N = 72$.

Suppose we have a polynomial yielding $m = 5$.We shall examine only anti-symmetric polynomials. By Proposition 4.5, all $A_{5,j}$'s are divisible by 5. Now the classes $|(5\mathbb{Z} + j) \cap [0,71]|$ have 15 members for $j = 0, 1$ and 14 members for $j = 2,3,4$. This means that, up to symmetry, the $\mathbf{d}_{5,j}$'s have for $j = 0,1$ three possible values: $(5,5,5)$, $(10,5,0)$ or $(15,0,0)$. For $j = 2,3,4$ we get, up to symmetry, $\mathbf{d}_{5,j} = (8,3,3)$. We checked the option $(\mathbf{d}_{5,0}, \mathbf{d}_{5,1}, \mathbf{d}_{5,2}, \mathbf{d}_{5,3}, \mathbf{d}_{5,4}) = ((5,5,5),(5,5,5),(3,3,8),(8,3,3),(3,8,3))$. (It can be shown that the other options do not lead to any anti-symmetric polynomial with $m = 5$, but this is of no consequence.) We scanned all $\binom{15}{5}\binom{14}{3}\binom{7}{4} \approx 4 \cdot 10^7$ options for determining S_0 (in a symmetric manner). We found only one option for S_0 whose first five moments match the corresponding target values. For this option we try to determine S_1. After going over about $3 \cdot 10^5$ possibilities, we found 4 polynomials. For example, the following polynomial is a member of $\mathcal{P}_3(72,5)$:
$\{3,4,5,8,13,18,19,20,26,30,34,35,36,37,41,45,51,52,53,58,63,66,67,68\}$,
$\{0,7,9,10,11,14,16,21,27,28,29,38,39,40,46,47,48,49,54,56,59,65,69,70\}$,
$\{1,2,6,12,15,17,22,23,24,25,31,32,33,42,43,44,50,55,57,60,61,62,64,71\}$.

Suppose we have a polynomial yielding $m = 6$. The only option for the $\mathbf{d}_{5,j}$'s is $(\mathbf{d}_{5,0}, \mathbf{d}_{5,1}, \mathbf{d}_{5,2}, \mathbf{d}_{5,3}, \mathbf{d}_{5,4}) = ((0,5,10),(10,5,0),(8,3,3),(3,8,3),(3,3,8))$. Combining this information with that obtained with $p = 2$ we are left with $\approx 10^{11}$ possibilities, none of which belongs to $\mathcal{P}_3(72,6)$. Thus $m_3^*(72) = 5$.

1.b) $N = 81$.

Suppose we have a polynomial yielding $m = 5$. By Proposition 4.5, all $A_{2,j}$'s are divisible by 16. As $|2\mathbb{Z} \cap [0,80]| = 41$ and $|(2\mathbb{Z}+1) \cap [0,80]| = 40$, the only possibility (up to symmetry) is $(\mathbf{d}_{2,0}, \mathbf{d}_{2,1}) = ((3,19,19),(24,8,8))$. We take all $\binom{41}{3}$ options for choosing 3 members of S_0 from $2\mathbb{Z} \cap [0,80]$. In order to divide $(2\mathbb{Z}+1) \cap [0,80]$, we will use $p = 5$. Employing Proposition 4.5 we find 264 options for $(\mathbf{d}_{5,0}, \mathbf{d}_{5,1}, \mathbf{d}_{5,2}, \mathbf{d}_{5,3}, \mathbf{d}_{5,4})$. For each splitting of $2\mathbb{Z} \cap [0,80]$, we go over all possibilities of choosing the rest of the elements of S_0 according to the various possibilities obtained using $p = 5$. For every such division we check if the first 5 moments have the target values for S_0. For every division satisfying the constraint, we go over the possibilities of choosing the elements of S_1. We take all $\binom{16}{8}$ options for a splitting of the remaining elements of $2\mathbb{Z} \cap [0,80]$. For each such splitting, we go over all possibilities of dividing the rest of the elements according to the various possibilities obtained with $p = 5$. After checking about $3 \cdot 10^{12}$ possibilities, we find all polynomials in $\mathcal{P}_3(81,5)$. For example, the following polynomial is a member of $\mathcal{P}_3(81,5)$:

$$\begin{aligned}
&\{3,5,7,9,11,15,16,23,24,29,31,33,41,43,45,\\
&\qquad\qquad 48,49,51,53,55,59,61,69,71,73,77,79\},\\
&\{1,2,4,14,17,18,21,22,25,26,28,30,37,38,42,46,\\
&\qquad\qquad 50,56,57,58,62,63,66,68,75,76,78\},\\
&\{0,6,8,10,12,13,19,20,27,32,34,35,36,39,40,44,47,\\
&\qquad\qquad 52,54,60,64,65,67,70,72,74,80\}.
\end{aligned}$$

Using Proposition 4.5 with $p = 2$, we see that there is no polynomial yielding $m = 6$. (Alternatively, as we found all members of $\mathcal{P}_3(81,5)$, we could check if any of them satisfies the additional condition.) Thus $m_3^*(81) = 5$.

1.c) $N = 99$.

Suppose we have a polynomial yielding $m = 5$. We shall examine only the anti-symmetric polynomials. By Proposition 4.5, all $A_{2,j}$'s are divisible by 16. The only possibility (up to symmetry) is $(\mathbf{d}_{2,0}, \mathbf{d}_{2,1}) = ((6,22,22),(27,11,11))$. We use Proposition 4.5 with $p = 5$ and get 46 options, corresponding to anti-symmetric polynomials, for the $\mathbf{d}_{5,j}$'s. We checked the option $(\mathbf{d}_{5,0}, \mathbf{d}_{5,1}, \mathbf{d}_{5,2}, \mathbf{d}_{5,3}, \mathbf{d}_{5,4}) = ((5,10,5),(5,5,10),(5,10,5),(5,5,10),(13,3,3))$. After checking about 10^{11} possibilities, we find 55158 polynomials. For example, the following polynomial is a member of $\mathcal{P}_3(99,5)$:

$$\begin{aligned}
&\{1,5,6,10,15,17,18,19,23,25,33,35,41,43,45,47,49,\\
&\qquad\qquad 51,53,55,57,63,65,73,75,79,80,81,83,88,92,93,97\},\\
&\{2,4,8,9,12,16,20,22,24,28,30,32,36,38,42,50,52,\\
&\qquad\qquad 54,58,59,61,64,67,69,71,72,77,84,85,87,91,95,98\},\\
&\{0,3,7,11,13,14,21,26,27,29,31,34,37,39,40,44,46,\\
&\qquad\qquad 48,56,60,62,66,68,70,74,76,78,82,86,89,90,94,96\}.
\end{aligned}$$

Using Proposition 4.5 with $p = 2$, we see that there is no polynomial yielding $m = 6$. Thus $m_3^*(99) = 5$.

1.d) $N = 117$.

Suppose we have a polynomial yielding $m = 5$. We shall examine only anti-symmetric polynomials. By Proposition 4.5, all $A_{2,j}$'s are divisible by 16. The only possibility (up to symmetry) is $(\mathbf{d}_{2,0}, \mathbf{d}_{2,1}) = ((9,25,25),(30,14,14))$. We use Proposition 4.5 with $p = 5$ and get 46 options corresponding to anti-symmetric polynomials, for the $\mathbf{d}_{5,j}$'s. We checked the option $(\mathbf{d}_{5,0}, \mathbf{d}_{5,1}, \mathbf{d}_{5,2}, \mathbf{d}_{5,3}, \mathbf{d}_{5,4}) = ((8,8,8), (8,8,8), (6,6,11), (11,11,1), (6,6,11))$. Going over about 10^6 possibilities, we find the following member of $\mathcal{P}_3(117,5)$:

$$\{0,3,5,13,15,19,20,23,25,27,29,30,35,40,43,47,49,53,57,58,$$
$$59,63,67,69,73,76,81,86,87,89,91,93,96,97,101,103,111,113,116\},$$
$$\{1,4,7,9,14,16,17,21,24,32,34,36,37,39,42,44,50,52,54,56,61,$$
$$65,68,70,71,75,78,83,85,88,90,94,98,104,105,106,108,110,114\},$$
$$\{2,6,8,10,11,12,18,22,26,28,31,33,38,41,45,46,48,51,55,60,$$
$$62,64,66,72,74,77,79,80,82,84,92,95,99,100,102,107,109,112,115\}.$$

Using Proposition 4.5 with $p = 2$,we see that there is no polynomial yielding $m = 6$. Thus $m_3^*(117) = 5$.

2.a) $N = 90$.

Suppose we have a polynomial yielding $m = 6$. We shall examine only symmetric polynomials. Using Proposition 4.5 with $p = 7$ we get 7 options, corresponding to symmetric polynomials, for the $\mathbf{d}_{7,j}$'s. We checked the option $(\mathbf{d}_{7,0}, \dots, \mathbf{d}_{7,6}) = ((7,4,2), (0,4,9), (7,4,2), (7,4,2), (0,4,9), (7,4,2), (2,6,4))$. Going over about $4 \cdot 10^7$ possibilities, we find 57 polynomials. For example, the following polynomial is a member of $\mathcal{P}_3(90,6)$:

$$\{3,5,7,9,12,14,16,17,28,31,35,38,40,41,44,$$
$$45,48,49,51,54,58,61,72,73,75,77,80,82,84,86\},$$
$$\{2,4,6,8,13,19,20,21,24,29,30,33,37,42,43,$$
$$46,47,52,56,59,60,65,68,69,70,76,81,83,85,87\},$$
$$\{0,1,10,11,15,18,22,23,25,26,27,32,34,36,39,$$
$$50,53,55,57,62,63,64,66,67,71,74,78,79,88,89\}.$$

2.b) $N = 108$.

Suppose we have a polynomial yielding $m = 6$. We shall examine only symmetric polynomials. Since 108 is divisible by 4, it is possible that all $d_{i,4,j}$'s are 9, i.e., all $A_{4,j}$'s are 0. Using Proposition 4.5 with $p = 5$ we get 3 options, corresponding to symmetric polynomials, for the $\mathbf{d}_{5,j}$'s. Going over about $5 \cdot 10^8$ possibilities, we find the following member of $\mathcal{P}_3(108,6)$:

$$\{1,2,3,13,16,20,21,23,26,31,32,33,34,36,39,40,41,53,$$
$$54,66,67,68,71,73,74,75,76,81,84,86,87,91,94,104,105,106\},$$
$$\{0,4,5,11,17,18,19,24,25,27,28,29,37,38,45,50,51,52,$$
$$55,56,57,62,69,70,78,79,80,82,83,88,89,90,96,102,103,107\},$$
$$\{6,7,8,9,10,12,14,15,22,30,35,42,43,44,46,47,48,49,$$
$$58,59,60,61,63,64,65,72,77,85,92,93,95,97,98,99,100,101\}.$$

2.c) $N = 126$.

Suppose we have a polynomial yielding $m{=}6$. We shall examine only symmetric polynomials. Using Proposition 4.5 with $p = 4$ we get 6 options (up to symmetry) corresponding to symmetric polynomials, for the $\mathbf{d}_{4,j}$'s. Using Proposition 4.5 again with $p{=}5$ we get 81 options, corresponding to symmetric polynomials, for the $\mathbf{d}_{5,j}$'s. We checked the option $(\mathbf{d}_{5,0}, \dots, \mathbf{d}_{5,4}) = ((2,12,12), (10,10,5), (10,5,10),$

$(10,5,10), (10,10,5))$ and $(\mathbf{d}_{4,0},\dots,\mathbf{d}_{4,3}) = ((4,12,16),(4,12,16),(17,9,5),(17,9,5))$. After checking about $6\cdot 10^7$ possibilities, we find the following member of $\mathcal{P}_3(126,6)$:

$$\begin{gathered}\{4,6,8,9,11,12,14,22,23,31,34,35,38,42,43,46,47,54,58,59,62,63,\\ 66,67,71,78,79,82,83,87,90,91,94,102,103,111,113,114,116,117,119,121\},\\ \{1,2,7,13,15,17,19,21,24,25,27,36,39,41,44,45,50,51,55,60,61,64,\\ 65,70,74,75,80,81,84,86,89,98,100,101,104,106,108,110,112,118,123,124\},\\ \{0,3,5,10,16,18,20,26,28,29,30,32,33,37,40,48,49,52,53,56,57,68,\\ 69,72,73,76,77,85,88,92,93,95,96,97,99,105,107,109,115,120,122,125\}.\end{gathered}$$

□

6. Methods and heuristics

In this section we describe the methods employed to find the possible values of $P(\zeta_{p^k})$ and the $d_{i,p^k,j}$'s, and to search for polynomials in $\mathcal{P}_q(N,m)$ (of course, here we actually ran the programs only for $q=3$). The algorithms were implemented in C++.

6.1. Finding possible divisions of residue classes modulo p^k.

Here we have 4 types of constraints:

1. Divisibility: $A_{p^k,j}$ is divisible by some power of p, denoted by p^l.

This means that $d_{i,p^k,j} - d_{q-1,p^k,j}$ is divisible by p^l, $0 \le i \le q-1$. In order to scan the possible values of $A_{p^k,j}$ efficiently, we first determine $d_{q-1,p^k,j}$. If

$$|(p^k\mathbb{Z}+j)\cap[0,N-1]| - qd_{q-1,p^k,j}$$

is not divisible by p^l, we increase $d_{q-1,p^k,j}$. Otherwise, we need to add multiples of p^l to the $d_{i,p^k,j}$'s. This problem is equivalent to finding all q-part compositions of $(|(p^k\mathbb{Z}+j)\cap[0,N-1]| - qd_{q-1,p^k,j})/p^l$. In [10, Ch. 5, p. 190] the problem of finding all k-part compositions of n is reduced to that of finding all $(k-1)$-subsets of a set of size $n+k-1$.

2. Congruence: $A_{p^k,j}$ is congruent to $A_{p^k,s}$ modulo p^l.

Assume that $A_{p^k,s}$ is pre-determined. The requirement is that $d_{i,p^k,j} - d_{q-1,p^k,j} - d_{i,p^k,s} + d_{q-1,p^k,s}$ is divisible by p^l. Similar to the situation for the preceding type of constraint, we determine $d_{q-1,p^k,j}$ and continue by finding the minimal values of the $d_{i,p^k,j}$'s and adding multiples of p^l using q-part compositions.

3. Subset size: The size of each S_i is N/q for $0 \le i \le q-1$.

The $A_{p^k,j}$'s with $j < p^k - \varphi(p^k)$ are totally determined by the other $A_{p^k,j}$'s. For $k=1$ this simply means that $d_{i,p,0} = N/q - \sum_{j=1}^{p-1} d_{i,p,j}$. For $k>1$ we first need to calculate the possible values for $A_{p^{k-1},j}$ by $A_{p^{k-1},j} = \sum_{i=0}^{p-1} A_{p^k,j+ip^{k-1}}$.

4. Sum: The system of congruences defined by the second parts of Propositions 4.2 and 4.5, is satisfied.

This system is triangular. We use this constraint only for $k=1$. The constraint implies that, after determining $A_{p,j}$ for all $j \ge r$, the rest of the $A_{p,j}$'s are determined modulo p^l. In particular, if $j<r$ and we set $\mathtt{sum}_{ipj} = \sum_{s=j+1}^{p-1}\binom{s}{j} d_{i,p,s}$, then we require $d_{i,p,j} - d_{q-1,p,j} + \mathtt{sum}_{ipj} - \mathtt{sum}_{q-1,p,j}$ to be divisible by p^l.

Let us now describe the procedure for finding the possible values of the $A_{p^k,j}$'s. The procedure is recursive. We begin by finding all possible values of A_{p^k,p^k-1}. For every such value, we find all possible values for A_{p^k,p^k-2}, and so on:

```
Routine determineA($p$, $k$, $j$)
    if $k = 1$:
        $l = \left\lfloor \frac{m}{p-1} \right\rfloor$, $r = m \pmod{p-1}$
        congruent $= p^l + 1$
        if $j = 0$, use Subset-size constraint
        if $1 \leq j < r$, use Sum constraint
        if $r = 0$ and $j < p-1$, use Congruence constraint
        else use Divisibility constraint
    else
        congruent $= p^{\left\lfloor \frac{m}{\varphi(p^k)} \right\rfloor}$
        if $j < p^k - \varphi(p^k)$, use Subset-size constraint
        if $p^k - \varphi(p^k) \leq j < \varphi(p^k)$ use Congruence constraint
        else there is no constraint on $A_j$
```

6.2. **Scanning the reduced search range.** After finding the constraints on the divisions of residue classes modulo p^k, we need to go over the set of polynomials adhering to these constraints. We use an iterative approach that incrementally builds S_0; for every instance of S_0 with the desired values of moments we construct S_1 in a similar manner, and so on. Note that, after S_0, S_1,…,S_{q-2} have been constructed, $S_{q-1} = [0, N-1] \setminus (\bigcup_{i=0}^{q-2} S_i)$ automatically has the desired moments. In every iteration, we choose one of the constraints, namely one of the $d_{i,p^k,j}$'s, and try to enlarge S_i so that it will have exactly $d_{i,p^k,j}$ members which are congruent to j modulo p^k. This is done by checking the current number of members in S_i, congruent to j modulo p^k, and the number of unassigned members (i.e., members for which it has not yet been determined if they belong to S_i). We go over all possibilities of enlarging S_i, using the "revolving door" algorithm (cf. [10]), 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.

The following procedure describes the method we use in our search. The arrays set, primePower and residue hold the plan for scanning the search range.

```
Routine main()
    for i=0..1
        inSet[$i$] $\leftarrow \emptyset$
        notInSet[$i$] $\leftarrow \emptyset$
    read arrays set, primePower, residue
    find(0)
    return
Routine find(location)
    if location $=$ planSize
        if set[planSize $- 1$] has the required moments
            print the $S_i$'s
        return
    if set[location] $\neq$ set[location $- 1$]
        if set[location] is not complete
            return
        else
            notInSet[1] $\leftarrow S_0$
    $i \leftarrow$ set[location]
    $p^k \leftarrow$ primePower[location]
    $j \leftarrow$ residue[location]
    read $d_{i,p^k,j}$ from file
    unassigned $\leftarrow [0, N-1] \setminus$ (inSet[$i$] $\cup$ notInSet[$i$])
    curNum $\leftarrow |S_i \cap (j + p^k\mathbb{Z})|$
    if curNum $> d_{i,p^k,j}$ or $d_{i,p^k,j} -$ curNum $>$ |unassigned|
        return
    for every choice of $d_{i,p^k,j} -$ curNum elements from unassigned do:
        Add to inSet[$i$] the set of chosen elements
        Add to notInSet[$i$] the set of rejected elements
        find(location $+ 1$)
        Remove from inSet[$i$] the set of chosen elements
        Remove from notInSet[$i$] the set of rejected elements
```

6.3. **Scanning only symmetric/anti-symmetric polynomials.** Given a positive integer N and an arbitrary fixed prime power p^k, an integer $j_1 \in [0, N-1]$ is a *reflection* of an integer j_2 in the range if$j_1 \equiv N - j_2 - 1 \pmod{p^k}$. Throughout this section, p^k will denote an arbitrary fixed prime power, and we shall omit the reference to it.

Scanning only symmetric/anti-symmetric polynomials, we obtain additional constraints on the $A_{p^k,j}$'s:

If S_i is symmetric and j_1 is a reflection of j_2, then $d_{i,p^k,j_1} = d_{i,p^k,j_2}$.

If S_i is symmetric and j is a reflection of itself, then $d_{i,p^k,j}$ must be even, unless N is odd and $j \equiv \frac{N-1}{2} \pmod{p^k}$. In the latter case, if $d_{i,p^k,j}$ is odd, then $\frac{N-1}{2} \in S_i$. (Hence, for a symmetric polynomial and$j \equiv \frac{N-1}{2} \pmod{p^k}$, exactly one of the $d_{i,p^k,j}$'s is odd.)

If (S_i, S_{i+1}) is anti-symmetric and j_1 is a reflection of j_2, then $d_{i,p^k,j_1} = d_{i+1,p^k,j_2}$.

When we scan only symmetric/anti-symmetric polynomials, we can reduce substantially the search range as follows:

If N is odd and $j \equiv \frac{N-1}{2} \pmod{p^k}$, we should adjoin $\frac{N-1}{2}$ to the unique symmetric set S_i with odd $d_{i,p^k,j}$.

If S_i is symmetric and j_1 is a reflection of j_2, where $j_1 \neq j_2$, then we select d_{i,p^k,j_1} elements from $((j_1 + p^k\mathbb{Z}) \cup (j_2 + p^k\mathbb{Z})) \cap [0, N/2 - 1]$ and obtain d_{i,p^k,j_1} additional elements by reflection.

If S_i is symmetric and j is a reflection of itself, then we select $d_{i,p^k,j}/2$ elements from $(j + p^k\mathbb{Z}) \cap [0, N/2 - 1]$ and obtain $d_{i,p^k,j}/2$ additional elements by reflection.

When looking for anti-symmetric solutions, after choosing the elements of S_0, S_1,. . . ,S_{q-3}, we choose those of S_{q-2} and S_{q-1} as follows. Suppose j_1 is a reflection of j_2, where $j_1 \neq j_2$. We select d_{1,p^k,j_1} elements from $(j_1 + p^k\mathbb{Z}) \cap [0, N-1]$ and obtain d_{1,p^k,j_2} additional elements by an anti-symmetric reflection. In particular, for $q = 3$ we operate this way right after choosing the elements of S_0.

Similarly, if j is a reflection of itself, then we choose the elements of $S_{q-2} \cap (j + p^k\mathbb{Z})$ by going over all subsets of $(j + p^k\mathbb{Z}) \cap [0, N/2 - 1]$, and obtain the additional elements by an anti-symmetric reflection.

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, 1–16. MR1843077 (2002e:11025)

[2] D. Berend and S. Golan, *Littlewood polynomials with high order zeros*, Math. Comp. **75**(2006), 1541–1552. MR2219044 (2007b:11028)

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

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

[5] 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.

[6] J.S. Byrnes and D.J. Newman, *Null steering employing polynomials with restricted coefficients*, IEEE Trans. Antennas and Propagation **36**(1988), 301–303.

[7] T.S. Chen and C.N. Yang, *An algorithm to enumerate codewords for third-order spectral-null codes*, Proceedings, 2004 IEEE International Symposium on Information Theory, p. 88.

[8] 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. MR1720633 (2000k:94060)

[9] S. Golan, **http://www.cs.bgu.ac.il/~golansha/polynomials.**

[10] E. M. Reingold, J. Nievergelt and N. Deo, *Combinatorial Algorithms*, Prentice-Hall, New Jersey, 1977. MR0471431 (57:11164)

[11] 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)

[12] R.M. Roth, *Spectral-null codes and null spaces of Hadamard submatrices*, Designs, Codes and Cryptography **9**(1996), 177–191. MR1409444 (98e:94034)

[13] 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.

[14] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer, New York, 1982. MR718674 (85g:11001)

Department of Computer Science, Ben-Gurion University of the Negev, POB 653, Beer-Sheva 84105 Israel

E-mail address: golansha@cs.bgu.ac.il