#A48 INTEGERS 10 (2010), 623-638

ON TERNARY INCLUSION-EXCLUSION POLYNOMIALS

Gennady Bachman
Department of Mathematical Sciences, University of Nevada, Las Vegas, Las Vegas, Nevada
bachman@unlv.nevada.edu

Received: 12/12/09, Accepted: 6/5/10, Published: 11/11/10

Abstract

Taking a combinatorial point of view on cyclotomic polynomials leads to a larger class of polynomials we shall call the inclusion-exclusion polynomials. This gives a more appropriate setting for certain types of questions about the coefficients of these polynomials. After establishing some basic properties of inclusion-exclusion polynomials we turn to a detailed study of the structure of ternary inclusion-exclusion polynomials. The latter subclass is exemplified by cyclotomic polynomials Φ_{pqr}, where $p < q < r$ are odd primes. Our main result is that the set of coefficients of Φ_{pqr} is simply a string of consecutive integers which depends only on the residue class of r modulo pq.

1. Introduction

A ternary cyclotomic polynomial is a cyclotomic polynomial Φ_t where t is a product of three distinct odd primes. More precisely,

$$\Phi_t(z) = \prod_{\substack{0<a<t \\ (a,t)=1}} \left(z - e^{2\pi i a/t}\right),$$

where $t = pqr$ and p, q, and r are distinct odd primes. Following the usual conventions we assume that p is the smallest of the three primes, let $a_m = a_m(t)$ denote the coefficients of Φ_t, and set

$$A(t) = \max_m |a_m(t)|.$$

There has been much progress recently in our understanding of coefficients of Φ_t and, especially, of the function $A(t)$. A long-standing conjecture of M. Beiter [4] asserted that the bound

$$A(t) = A(pqr) \leq \frac{p+1}{2} \tag{1}$$

holds for all t. But in a recent work of Y. Gallot and P. Moree [6] this conjecture was disproved in a rather dramatic fashion and a number of prescriptions of integers t for which (1) fails to hold were given. In particular, it was shown that if

$\epsilon > 0$ is fixed then for every sufficiently large prime p there exist q and r such that

$$A(t) > \Big(\frac{2}{3} - \epsilon\Big)p. \tag{2}$$

They conjectured that, in fact,

$$A(t) \leq \frac{2}{3}p. \tag{3}$$

Following this B. Lawrence [9] announced that he proved the validity of (3) for $p > 10^6$.

Another interesting question that was resolved recently is whether it is possible to arrange it so that

$$A(t) = 1, \tag{4}$$

even for arbitrary large p. We say that polynomial Φ_t is flat in this case. An old folklore conjecture asserts that there are flat cyclotomic polynomials of all orders – the order of Φ_n is the number of distinct odd prime divisors of n if n is not a power of 2 and is 1 otherwise. The case of ternary cyclotomic polynomials has now been settled in the affirmative and the validity of (4) was first established by this author in [3]. This result was later extended by T. Flanagan [5] who showed that (4) holds for a larger family of integers t. But the best known result in this direction is due to N. Kaplan [8] who showed that (4) holds for every t with $r \equiv \pm 1 \pmod{pq}$.

As part of his work on (4) Kaplan showed that the value of $A(t)$ is completely determined by the residue class of r modulo pq, where $r > q > p$. More precisely, he showed that if $s > q$ is another prime and if $r \equiv \pm s \pmod{pq}$ then

$$A(pqr) = A(pqs). \tag{5}$$

Moreover, he also obtained the following partial analogue of (5) for the set of coefficients $\mathcal{A}_t = \{a_m(t)\}$ of Φ_t. Set identities

$$\mathcal{A}_{pqr} = \begin{cases} \mathcal{A}_{pqs}, & \text{if } r \equiv s \pmod{pq}, \\ -\mathcal{A}_{pqs}, & \text{if } r \equiv -s \pmod{pq}, \end{cases} \tag{6}$$

are certainly valid if $r, s > pq$. The first of these identities was also proved by Flanagan [5]. Actually (6) is only implicit in [8]. It follows that each residue class r_0 modulo pq determines at most two different sets of coefficients $\mathcal{A}_{pqr}$ with $r \equiv r_0 \pmod{pq}$.

The residue class of r modulo pq imposes certain structure on Φ_t and its set of coefficients $\mathcal{A}_t$ and our object here is to further investigate this structure. The main result of this paper is that $\mathcal{A}_t$ is completely determined by the residue class

of r modulo pq, that is, that (6) holds for $r, s > q$. We are also interested in an analogue of (6) for the case when $r \equiv s \pmod{pq}$ but $s < q < r$. Kaplan's result on $r \equiv \pm 1 \pmod{pq}$ falls into this case and is seen to be a special case of this general principle (see Section 3). In pursuing this development we shall work in a more general setting of what we shall call inclusion-exclusion polynomials. Accordingly we begin with a brief discussion of this class of polynomials and their relation to cyclotomic polynomials; this is the subject of Section 2. We then concentrate on the ternary case (of the inclusion-exclusion polynomials) in Section 3.

2. Inclusion-Exclusion Polynomials

Let $\rho = \{ r_1, r_2, \ldots, r_s \}$ be a set of natural numbers satisfying $r_i > 1$ and $(r_i, r_j) = 1$ for $i \neq j$, and put

$$n_0 = \prod_i r_i, \quad n_i = \frac{n_0}{r_i}, \quad n_{ij} = \frac{n_0}{r_i r_j} \ [i \neq j], \quad \ldots \ .$$

For each such ρ we define a function Q_ρ by

$$Q_\rho(z) = \frac{(z^{n_0} - 1) \cdot \prod_{i<j} (z^{n_{ij}} - 1) \cdot \ldots}{\prod_i (z^{n_i} - 1) \cdot \prod_{i<j<k} (z^{n_{ijk}} - 1) \cdot \ldots}. \tag{7}$$

Our first observation is that Q_ρ is, in fact, a polynomial.

Theorem 1. *We have*

$$Q_\rho(z) = \prod_\omega (z - \omega), \tag{8}$$

where the product is taken over all the roots of unity ω satisfying the condition

$$\omega^{n_0} = 1 \quad \textit{but} \quad \omega^{n_i} \neq 1 \quad [1 \leq i \leq s].$$

Moreover, the degree of Q_ρ is given by

$$\varphi(\rho) = \prod_i (r_i - 1).$$

Proof. The claim follows by routine applications of the inclusion-exclusion principle and we omit the straight-forward details. □

We shall refer to polynomials Q_ρ as inclusion-exclusion polynomials, the term suggested by the construction (7). Our interest in this class of polynomials is motivated by the study of coefficients of cyclotomic polynomials, as will become

plain below. From the algebraic point of view the most interesting case is when parameters r_i are assumed to be distinct prime numbers. In this case $n_0 = \prod_i r_i$ is a canonical factorization of n_0 into primes, n_0 is a square-free integer, and the product in (8) is taken over all primitive n_0th roots of unity ω. In other words, in this case polynomial Q_ρ is better known as cyclotomic polynomial Φ_{n_0}. In general, as we show presently, Q_ρ is a certain product of cyclotomic polynomials.

Theorem 2. *Given ρ let*

$$D = D_\rho = \{\, d : d \mid n_0 \text{ and } (d, r_i) > 1 \text{ for all } i \,\}. \tag{9}$$

Then we have

$$Q_\rho(z) = \prod_{d \in D} \Phi_d(z). \tag{10}$$

Proof. Since both sides of (10) are monic polynomials with roots of multiplicity 1 it suffices to show that the roots are, in fact, the same. So consider any root ω of Q_ρ and let d be the smallest integer such that $\omega^d = 1$. Then ω is a root of Φ_d. Moreover, by Theorem 1, $d \in D$ since $d \mid n_0$ and $(d, r_i) > 1$.

In the opposite direction, fix $d \in D$ and let ω be any root of Φ_d. Then $\omega^{n_0} = 1$. Moreover, $(d, n_i) < d$ and we conclude that $\omega^{n_i} \neq 1$. Thus, by Theorem 1, ω is a root of Q_ρ. □

We now turn our attention to the question of coefficients of these polynomials. We begin with a few remarks of general nature on coefficients of inclusion-exclusion polynomials versus coefficients of cyclotomic polynomials. As is well known, to study coefficients of cyclotomic polynomials it suffices to consider only polynomials Φ_n with n square-free. We have seen that in this case $\Phi_n = Q_\rho$, where r_i are prime factors of n. It is thus natural to consider properties of coefficients of cyclotomic polynomials in the larger context of coefficients of inclusion-exclusion polynomials. In fact, the literature on this topic contains many results on cyclotomic polynomials that are actually theorems about inclusion-exclusion polynomials. This characterization certainly applies to every result which was obtained by an argument that (i) used identity (7) as a point of departure and (ii) did not crucially depend on parameters r_i to be prime but actually only required the condition $(r_i, r_j) = 1$, for $i \neq j$. For instance, most of the work on coefficients of cyclotomic polynomials of low order falls into this category. Even when it comes to open questions about coefficients of cyclotomic polynomials, it seems rather clear that some of them are truly questions about coefficients of inclusion-exclusion polynomials. Take, for instance, the question of whether there exist flat cyclotomic polynomials of arbitrary large order. It is quite evident that

this is a question about the structure of (7) and that the algebraic distinction of cyclotomic polynomials has no bearing on the matter.

Finally, we remark that the setting of inclusion-exclusion polynomials may offer not only a more appropriate context but it may actually furnish certain "practical" advantages over the setting of cyclotomic polynomials. This will become plain in the next section where we take up the case of ternary inclusion-exclusion polynomials (defined below).

We define the order of Q_ρ to be s, if $s = 1$ or if $r_i \geq 3$ for $1 \leq i \leq s$, and $s-1$ otherwise. This parameter corresponds to the order of cyclotomic polynomial and plays an important role. The situation is identical to the more familiar setting of cyclotomic polynomials and the best known examples of this are polynomials of orders 1 and 2. Indeed, if $s = 1$ and $\rho = \{\, p \,\}$ ($p \geq 2$; not necessarily prime), then

$$Q_{\{p\}}(z) = \frac{z^p - 1}{z - 1} = \sum_{n=0}^{p-1} z^n. \tag{11}$$

Similarly,

$$Q_{\{p,q\}}(z) = \frac{(z^{pq}-1)(z-1)}{(z^q-1)(z^p-1)} = (1-z^{pq})(1-z)\sum_{i=0}^{\infty} z^{iq} \sum_{j=0}^{\infty} z^{jp}$$

$$\equiv (1-z) \sum_{i,j \geq 0} z^{iq+jp} \pmod{z^{(p-1)(q-1)+1}},$$

by Theorem 1. It follows that if χ denotes the characteristic function of integers representable in the form $iq + jp$ with $i, j \geq 0$ then

$$Q_{\{p,q\}}(z) = \sum_{n=0}^{(p-1)(q-1)} \chi(n) z^n - \sum_{n=0}^{(p-1)(q-1)-1} \chi(n) z^{n+1}. \tag{12}$$

Thus, in the sense of (11) and (12), the structure of Q_ρ is determined by the order. In particular, polynomials of orders 1 and 2 are flat. (For a more detailed discussion of polynomials of order 2, phrased in terms of cyclotomic polynomials, see, for example, [10].)

The condition $r_i \geq 3$ in the definition of order of Q_ρ is explained by the identity (whose cyclotomic polynomials analogue is also well-known)

$$Q_{\{2,r_2,\ldots,r_s\}}(z) = Q_{\{r_2,\ldots,r_s\}}(-z) \quad [s \geq 2].$$

This follows readily from Theorem 1 and we omit the details (see, for example, [10]). This takes us to polynomials of order at least 3 where the situation is considerably more interesting. As we already mentioned in the introduction, even the

ternary case, that is Q_ρ of order 3, still presents interesting challenges. This case is the principal object of this paper and it will be taken up in the next section.

The fact that cyclotomic polynomials are reciprocal proved to be useful in the study of their coefficients. We conclude this section by observing that the same is true for inclusion-exclusion polynomials. Indeed, the identity

$$Q_\rho(z) = z^{\varphi(\rho)} Q_\rho(z^{-1})$$

follows readily from (7) and the fact that $\varphi(\rho)$ is the degree of Q_ρ. From this we infer that if

$$Q_\rho(z) = \sum_{m=0}^{\varphi(\rho)} a_m z^m \quad [a_m = a_m(\rho)],$$

then $a_m = a_{\varphi(\rho)-m}$.

3. The Ternary Case

We shall write Q_τ to denote a ternary inclusion-exclusion polynomial. For esthetic reasons we normally write $\tau = \{ p, q, r \}$ rather than $\tau = \{ r_1, r_2, r_3 \}$. Thus, contrary to the conventions of Section 1, we now assume only that parameters p, q, and r are ≥ 3 and relatively prime in pairs. At times, however, the use of notation $\tau = \{ r_1, r_2, r_3 \}$ will prove to be the better choice. Consequently, we consider the two forms to be interchangeable and shall freely use either one with our choice dictated by convenience. Adopting other conventions in the introduction we write, by Theorem 1,

$$Q_\tau(z) = \sum_{m=0}^{\varphi(\tau)} a_m z^m \quad [a_m = a_m(\tau)], \tag{13}$$

as well as

$$\mathcal{A}_\tau = \{ a_m(\tau) \} \quad \text{and} \quad A(\tau) = \max_m |a_m(\tau)|. \tag{14}$$

Moreover, set

$$A^+(\tau) = \max_m a_m(\tau) \quad \text{and} \quad A^-(\tau) = \min_m a_m(\tau).$$

Let us emphasize that we are not assuming any particular order for the parameters p, q, and r. The structural symmetry of Q_τ with respect to these parameters is a key aspect of the problem and it will play an important role in our development. Correspondingly, we shall explicitly state any additional assumptions on p, q, and r when it is appropriate.

Recall from the introduction that we are after the relationship between polynomials $Q_{\{p,q,r\}}$ and $Q_{\{p,q,s\}}$ with $r \equiv s \pmod{pq}$. This problem splits into two parts according to whether

$$r,\, s > \max(p,q) \quad \text{or} \quad r > \max(p,q) > s \geq 1,$$

say. The principal focus of this paper is the former condition and our main result is as follows.

Theorem 3. *Set of coefficients $\mathcal{A}_{\{p,q,r\}}$ is a string of consecutive integers and, for $r > \max(p,q)$, is completely determined by the residue class of r modulo pq. More precisely, we have*

$$\mathcal{A}_\tau = [\, A^-(\tau), A^+(\tau)\,] \cap \mathbb{Z} \tag{15}$$

and, for $r, s > \max(p,q)$,

$$\mathcal{A}_{\{p,q,r\}} = \begin{cases} \mathcal{A}_{\{p,q,s\}}, & \text{if } r \equiv s \pmod{pq}, \\ -\mathcal{A}_{\{p,q,s\}}, & \text{if } r \equiv -s \pmod{pq}. \end{cases} \tag{16}$$

As we pointed out in Section 2, much of what is known about cyclotomic polynomials of low order pertains to corresponding inclusion-exclusion polynomials. The work of Flanagan and Kaplan discussed in the introduction is a case in point. In particular, identity (16) was already known to hold under the assumption $r, s > pq$.

The remark in the preceding paragraph applies to all of our references in what follows. Thus, for the sake of simplicity, we shall henceforth ignore the distinction between cyclotomic and inclusion-exclusion polynomials, when appropriate.

We deduce (15) from Lemma 6 below. Both of these facts were discovered independently by Gallot and Moree [7]. It is worth noting that the approach in the works of [8] and [7] is rather different from ours.

We derive Theorem 3 by a sequence of lemmas some of which are of independent interest and shed additional light on the structure of Q_τ. As we remarked earlier, our development preserves symmetry in the parameters p, q, and r whenever it is appropriate. This, in particular, will be handy when considering the second alternative, namely

$$r \equiv \pm s \pmod{pq} \quad \text{and} \quad r > \max(p,q) > s \geq 1. \tag{17}$$

The situation in this case is more complicated and $A(p,q,r)$ need not equal $A(p,q,s)$ – in a slight abuse of notation we shall write $A(p,q,r)$ in place of $A(\{\, p,q,r\,\})$, and use the same conventions for the functions A^+ and A^-. Instead

we have the following result. Recall from Section 2 that polynomials of order less than 3 are flat, so that $A(p,q,2) = 1$. Moreover, it is convenient to extend the definition of A by setting $A(p,q,1) = 0$. With these conventions we state our result for (17).

Theorem 4. *If r and s satisfy* (17)*, then*

$$A(p,q,s) \le A(p,q,r) \le A(p,q,s) + 1. \tag{18}$$

The proof of Theorem 4 will require further development and will be carried out elsewhere. We shall limit ourselves here to a few brief remarks. Note that, by Theorem 3, we have

$$A(p,q,r) = A(p,q,pq \pm s),$$

under (17). In this light (18) is seen as a recursive estimate. Of course, using an absolute upper bound for $A(p,q,s)$ on the right of (18) yields the corresponding upper bound for $A(p,q,r)$. For instance, a simple and convenient estimate

$$A(p,q,r) = A(p,q,pq \pm s) \le s, \tag{19}$$

valid for all $s \ge 1$, is obtained on combining (18) with the bound (see [1])

$$A(p,q,s) \le s - \lceil s/4 \rceil .$$

Estimate (19) sacrifices precision for convenience and is certainly weaker than (18) for $s \ge 5$. On the other hand, (19) is sharp for $1 \le s \le 3$. We do not know if the equation $A(p,q,pq+4) = 4$ has any solutions. Note also that Kaplan's result on flat cyclotomic polynomials corresponds to (19) with $s = 1$.

When iteration of (18) is possible it leads to a very rapid reduction technique. For example, two applications of (18) give

$$A(p, pq+1, p^2q+p+q) \le A(p, pq+1, q) + 1 \le 2.$$

Our first step is to observe that, by (7), polynomial Q_τ has a representation

$$\begin{aligned} Q_\tau(z) &= \frac{(1-z^{pqr})(1-z^r)(1-z^q)(1-z^p)}{(1-z^{qr})(1-z^{rp})(1-z^{pq})(1-z)} \\ &\equiv (1-z^r)(1-z^q)(1+z+\cdots+z^{p-1}) \\ &\qquad \times \sum_{i=0}^{\infty} z^{iqr} \sum_{j=0}^{\infty} z^{jrp} \sum_{k=0}^{\infty} z^{kpq} \pmod{z^{pqr}}. \end{aligned} \tag{20}$$

Evidently, of key importance are integers n of the form

$$n = iqr + jrp + kpq, \quad i, j, k \geq 0, \tag{21}$$

and we let $\chi = \chi_\tau$ be the characteristic function of such integers, that is,

$$\chi(n) = \chi_\tau(n) = \begin{cases} 1, & \text{if } n \text{ has representation (21),} \\ 0, & \text{otherwise.} \end{cases} \tag{22}$$

Note that if $n < pqr$ then either representation (21) is not possible or it is unique. Therefore, by (13), (20) and (22), the identity

$$a_m = \sum_{m-p<n\leq m} \big(\chi(n) - \chi(n-q) - \chi(n-r) + \chi(n-q-r)\big) \tag{23}$$

holds for all $m < pqr$. Let us clarify the meaning of this statement. Recall that Q_τ is a polynomial of degree $\varphi(\tau)$. But in (23) we take $a_m = 0$ for $m < 0$ and for $\varphi(\tau) < m < pqr$ and then the identity remains valid in the range $m < pqr$. We shall find this extension useful for technical reasons.

In considering integers representable in the form (21) it is helpful to observe that every integer n has a unique representation in the form

$$n = x_n qr + y_n rp + z_n pq + \delta_n pqr, \tag{24}$$

with $0 \leq x_n < p$, $0 \leq y_n < q$, $0 \leq z_n < r$, and $\delta_n \in \mathbb{Z}$. It follows that n is representable in the form (21) if and only if $\delta_n \geq 0$. But if $n < pqr$, as we shall assume henceforth, then $\delta_n \leq 0$ and we obtain the characterization

$$\chi(n) = 1 \quad \text{if and only if} \quad \delta_n = 0 \quad [n < pqr]. \tag{25}$$

We shall deduce (15) from Lemma 5 below. Recall our convention of using $\{ p, q, r \}$ and $\{ r_1, r_2, r_3 \}$ interchangeably.

Lemma 5. *We have*

$$\big|\chi(n) - \sum_i \chi(n - r_i) + \sum_{i<j} \chi(n - r_i - r_j) - \chi(n - r_1 - r_2 - r_3)\big| \leq 1.$$

Proof. Let $\tau' = \{ \pm r_1, \pm r_2, \pm r_3 \}$ and for every pair of $u, v \in \tau'$ with $|u| \neq |v|$ set

$$\psi_{uv}(n) = \chi(n) - \chi(n-u) - \chi(n-v) + \chi(n-u-v). \tag{26}$$

Observe that if w is another element of τ' and $|u|$, $|v|$, and $|w|$ are all distinct then

$$\big|\chi(n)-\sum_i \chi(n-r_i)+\sum_{i<j}\chi(n-r_i-r_j)-\chi(n-\textstyle\sum_i r_i)\big| = \big|\psi_{uv}(n')-\psi_{uv}(n'-w)\big|,$$

where $n' = n+(u-|u|)/2+(v-|v|)/2+(w-|w|)/2$. Therefore to prove the lemma it suffices to show that the inequality

$$\psi_{uv}(n)-\psi_{uv}(n-w)\le 1 \tag{27}$$

holds for all n (in an appropriate range depending on parameters u, v, and w).

In [1, Lemma 2] it was shown that

$$|\psi_{uv}(n)|\le 1. \tag{28}$$

Actually, this estimate was given explicitly only for ψ_{qr}, with $q,r>p$, but the argument applies for every choice of u and v in τ'. The rest of this proof is essentially an extension of [1, Proof of Lemma 2] and, in particular, (28) will serve as a convenient reduction tool. In the first place, by (27) and (28), it suffices to show that there is no n for which

$$\psi_{uv}(n)=1 \quad\text{and}\quad \psi_{uv}(n-w)=-1. \tag{29}$$

To reach a contradiction let us assume that (29) holds for some n. Noting that, by (26), we have

$$\psi_{uv}(n)=\psi_{(-u)(-v)}(n-u-v),$$

shows that, in addition to $\psi_{uv}(n)=1$, there is no loss in generality in assuming that $\chi(n)=1$. Similarly, by (26) and symmetry, it follows that in addition to $\psi_{uv}(n-w)=-1$ we may assume that $\chi(n-w-u)=1$. It now follows from (28) with v replaced by w that we may also assume that $\chi(n-w)=1$, say. But then, since $\psi_{uv}(n-w)=-1$, we must also have $\chi(n-w-v)=1$ and $\chi(n-w-u-v)=0$. Finally, in view of $\psi_{uv}(n)=1$, we may further assume that $\chi(n-u)=0$, say. To summarize, to show that (29) is not possible it suffices to show that there is no n for which

$$\chi(n)=\chi(n-w)=\chi(n-w-u)=\chi(n-w-v)=1 \text{ and } \chi(n-u)=\chi(n-w-u-v)=0.$$

But this readily follows from (24) and (25) by chasing the coefficients in representations (24) of all the relevant integers (see [1, Proof of Lemma 2]). □

Lemma 6. *We have* $\big|a_m(\tau)-a_{m-1}(\tau)\big|\le 1$.

Proof. By (23) and (26), $a_m - a_{m-1} = \psi_{qr}(m) - \psi_{qr}(m-p)$, and the claim follows from Lemma 5. □

The following simple observation is rather useful. By (24) and (25), we have

$$\chi(n) = \chi(n-pq), \quad \text{unless } \delta_n = z_n = 0, \tag{30}$$

$$\chi(n) = 1 \text{ and } \chi(n-pq) = 0, \quad \text{if } \delta_n = z_n = 0, \tag{31}$$

as well as the analogues of (30) and (31) with pq and z_n replaced by qr and x_n or by rp and y_n, respectively.

Lemma 7. *Let R_m be the set of all integers appearing as an argument of χ in the summation* (23)*. Then we have*

$$a_m = a_{m-pq}, \quad \textit{unless there is } n \in R_m \textit{ with } \delta_n = z_n = 0, \tag{32}$$

as well as the analogues of (32) *with pq and z_n replaced by qr and x_n or by rp and y_n, respectively.*

Proof. This is an immediate consequence of (23) and (30). □

Lemma 8. *The estimate*

$$|a_m - a_{m-r_i r_j}| \le 2 \tag{33}$$

holds unconditionally for every pair of parameters $r_i \neq r_j$. Moreover, if $r \ge p+q$ then we have

$$|a_m - a_{m-pq}| \le 1. \tag{34}$$

Proof. Consider representation (23) with parameter p given by $p = \min(r_1, r_2, r_3)$. We shall now prove (33) with $r_i r_j = qr$, the remaining case follows in the same way. Put $I_n = (n-p, n] \cap \mathbb{Z}$, so that

$$R_m = I_m \cup I_{m-q} \cup I_{m-r} \cup I_{m-q-r}. \tag{35}$$

Note that $x_n = 0$ if and only if n is a multiple of p. But each of the four intervals on the right of (35) contains exactly one multiple of p, say $\alpha_i p$. Therefore, by (23), (30) and (31), we get

$$|a_m - a_{m-qr}| \le |\chi(\alpha_1 p) - \chi(\alpha_2 p) - \chi(\alpha_3 p) + \chi(\alpha_4 p)|,$$

and (33) follows.

To prove (34) we argue in the same way but take advantage of the condition $r \ge p+q$. By Lemma 7, we may assume that R_m contains multiples of r – these

are integers n with $z_n = 0$. But, in the present case, the range $I_m \cup I_{m-q}$ contains at most one such multiple, say αr. Therefore, by (23), (30) and (31), we have

$$|a_m - a_{m-pq}| = |\chi(\alpha r) - \chi(\alpha r - r)| \leq 1,$$

as claimed. □

Lemmas 3 and 4 have a number of interesting consequences. Observe that if we take r to be the largest of the three parameters then, by (32), it suffices to consider coefficients a_m with $m = \alpha r + \beta$ and $0 \leq \beta < \min(r, p + q)$. We will use this fact below. The parallel between (34) and Lemma 6 is immediate. Unlike Lemma 6, however, (34) has a hole in the form of the range $\max(p, q) < r < p + q$. Estimate (33) may be used to give a simple upper bound for coefficients of Q_τ as follows. Let $p < \min(q, r)$ and take $r_i r_j = qr$ in (33). One then readily verifies that iterating (33) yields the bound

$$|a_m| \leq 2 \lceil m/(qr) \rceil + 1. \tag{36}$$

Recall that we may assume that $m \leq \varphi(\tau)/2 < pqr/2$. Thus (36) suggests that coefficients of largest size are to occur near the middle of the range of the index m and gives a nontrivial bound for "small" m. Note also that replacing 2 by 1 on the right of (33) would have the same effect on the right of (36). But this would imply the bound $A(\tau) \leq \lceil p/2 \rceil + 1$, contradicting (2). It follows that, in general, (33) is sharp.

Another immediate consequence of (24) is that $\delta_n \geq 0$ if and only if $x_n qr + y_n rp \leq n$. Therefore, if

$$f(n) = f_{\tau,r}(n) = x_n q + y_n p, \tag{37}$$

then, by (25),

$$\chi(n) = 1 \quad \text{if and only if} \quad f(n) \leq \lfloor n/r \rfloor . \tag{38}$$

This observation, first made in [2], plays a key role in our analysis. Note that $f(n) \equiv nr^* \pmod{pq}$, where r^* is the multiplicative inverse of r modulo pq. Now let $[N]_{pq}$ denote the least nonnegative residue of N modulo pq and let $\mathcal{R}_{p,q}$ be the set of integers representable as a nonnegative linear combination of p and q, that is,

$$\mathcal{R}_{p,q} = \{\, N \mid N = xq + yp,\ x, y \geq 0 \,\}.$$

Then, by (24) and (37), we have

$$f(n) = \begin{cases} [nr^*]_{pq}, & \text{if } [nr^*]_{pq} \in \mathcal{R}_{p,q}, \\ [nr^*]_{pq} + pq, & \text{otherwise.} \end{cases} \tag{39}$$

It is now evident that f is determined by the residue class of r modulo pq. Before stating this formally, let us introduce the convention of writing f_r in place of $f_{\tau,r}$, as long as it is understood that the parameters p and q are fixed. Similarly, we will find it convenient to write χ_r in place of χ_τ under the same circumstances.

Lemma 9. *If* $r \equiv s \pmod{pq}$ *and* $n_1 \equiv n_2 \pmod{pq}$ *then* $f_r(n_1) = f_s(n_2)$.

Proof. Since $[n_1 r^*]_{pq} = [n_2 s^*]_{pq}$ the conclusion follows from (39). □

In addition to assumptions of Lemma 9 we need to impose certain further restrictions in order to guarantee that $\chi_r(n_1) = \chi_s(n_2)$.

Lemma 10. *Suppose that* $\max(p,q) < r < s$ *and that* $r \equiv s \pmod{pq}$. *Then*

$$\chi_r(kr + j) = \chi_s(ks + j), \tag{40}$$

for all $k < pq$ *and* $|j| < r$. *Moreover, if* $|j| < \min(r, pq)$ *then we also have*

$$\chi_r(kr + j - r) = \chi_s(ks + j - r). \tag{41}$$

Proof. The first claim follows from (38) and Lemma 9. The second claim with $j \geq 0$ follows in exactly the same way ((40) contains (41) for $j > 0$). In the remaining case we have

$$\Big\lfloor \frac{kr + j - r}{r} \Big\rfloor = k - 2 \quad \text{and} \quad \Big\lfloor \frac{ks + j - r}{s} \Big\rfloor = k - 1. \tag{42}$$

Moreover, if $j \not\equiv 0 \pmod{pq}$ then

$$f_r(kr + j - r) \neq k - 1, \tag{43}$$

since $f_r(kr + j - r) \equiv k - 1 + jr^* \pmod{pq}$. Combining (42) and (43) with (38) and Lemma 9 completes the proof of the lemma. □

We are now ready to consider functions $A^+(\tau)$ and $A^-(\tau)$. In view of (15), these functions capture all the information about the coefficients of Q_τ as a set. It is plain from our introductory discussion of the function $A(\tau)$ (in the form of $A(t)$) that there are basic gaps in our understanding of these functions. It is interesting to note that in contrast to this the quantity $A^+(\tau) - A^-(\tau)$ is more transparent. Indeed, it is known [1, 2] that the bound

$$A^+(\tau) - A^-(\tau) \leq p$$

is valid for all τ and that it is sharp. Our present aim is the identity (16) for which we need to show that if p and q are fixed then for $r > \max(p,q)$ functions $A^\pm(p,q,r)$ depend only on the residue class of r modulo pq.

Lemma 11. *If* $r, s > \max(p, q)$ *and* $r \equiv s \pmod{pq}$ *then*

$$A^+(p, q, r) = A^+(p, q, s) \quad \textit{and} \quad A^-(p, q, r) = A^-(p, q, s).$$

Proof. Consider the function A^+. With p and q fixed, let us write $A^+(r)$ for $A^+(\tau)$. It suffices to show that if $r > \max(p, q)$ and $s = r + pq$ then

$$A^+(r) = A^+(s). \tag{44}$$

Throughout this argument we adopt the convention that a_m and b_l denote coefficients of $Q_{\{p,q,r\}}$ and $Q_{\{p,q,s\}}$, respectively. We show first that if $0 \le \beta < r$ then

$$a_{\alpha r+\beta} = b_{\alpha s+\beta}. \tag{45}$$

Set $m = \alpha r + \beta$ and $l = \alpha s + \beta$. Observe that, by Lemma 10, we have

$$\chi_r(m - j) = \chi_s(l - j), \tag{46}$$

for all $0 \le j < p + q$. Moreover, (46) also holds with m and l replaced by $m - r$ and $l - s$, respectively. Combining this with (23) establishes (45).

Of course, the inequality $A^+(r) \le A^+(s)$ is an immediate consequence of (45). In fact, (45) implies (44) for we will show that for some α and $0 \le \beta < r$ we have

$$A^+(s) = b_{\alpha s+\beta}. \tag{47}$$

Thus it only remains to prove (47).

Let l_0 be the smallest index for which $b_{l_0} = A^+(s)$. Note that, by (23), $b_0 = 1$ and $b_q = -1$, so l_0 (as well as the corresponding quantity for the function A^-) are well defined – see remarks following (23). Applying (32) to b_{l_0} shows that we must have $l_0 = \alpha_0 s + \beta_0$, with $0 \le \beta_0 < q + p$, and that $\alpha_0 s$ and $\alpha_0 s - s$ are in R_{l_0} (given by (35) with r replaced by s). If, in fact, $\beta_0 < r$ then we are done. So suppose that $r \le \beta_0 < q + p$. We claim that in this case (47) holds with $\alpha s + \beta = l_0 + pq$. In the first place, we have

$$l_0 + pq = (\alpha_0 + 1)s + \beta_0 - r, \quad 0 \le \beta_0 - r < r.$$

Therefore, to prove (47) it remains to show that

$$b_{l_0+pq} = b_{l_0}. \tag{48}$$

Recall that $\alpha_0 s, \alpha_0 s - s \in R_{l_0}$ and observe that they are the only multiples of s in R_{l_0}. Moreover our assumption on β_0 implies that

$$\alpha_0 s \in I_{l_0-q}, \quad \alpha_0 s - s \in I_{l_0-q-s}, \tag{49}$$

$$\alpha_0 s + r \in I_{l_0}, \quad \text{and} \quad \alpha_0 s - s + r \in I_{l_0-s}. \tag{50}$$

Therefore, by (23), (30), (31), and (49), we get

$$b_{l_0-pq} = b_{l_0} - \chi_s(\alpha_0 s - s) + \chi_s(\alpha_0 s). \tag{51}$$

Whence $\chi_s(\alpha_0 s) = 0$ (and $\chi_s(\alpha_0 s - s) = 1$, but we will not need this). Also, by (50), $\alpha_0 s + s \in I_{l_0+pq}$ and $\alpha_0 s \in I_{l_0+pq-s}$, and they are the only multiples of s in R_{l_0+pq}. Therefore, reasoning as in (51), we now get

$$\begin{aligned} b_{l_0} &= b_{l_0+pq} + \chi_s(\alpha_0 s) - \chi_s(\alpha_0 s + s) \\ &= b_{l_0+pq} - \chi_s(\alpha_0 s + s). \end{aligned}$$

This implies (48) and completes the proof in the case of the function A^+.

Essentially identical argument works for the function A^- and we omit the details. □

Proof of Theorem 3. (15) follows from Lemma 6.

The first conclusion in (16) follows from Lemma 11 and (15).

Recall that Kaplan [8] has proved (16) for $r, s > pq$. Using this we deduce the second conclusion in (16) from the first.

Since our method is different from that of [8] it is of interest to give a self-contained treatment for the case $r \equiv -s \pmod{pq}$. We thus conclude this paper with a sketch of our argument. We will show that if a_m is an arbitrary coefficient of $Q_{\{p,q,r\}}$ then there is a coefficient b_l of $Q_{\{p,q,s\}}$ such that $b_l = -a_m$. To do this we make an additional assumption that $r, s \geq p + q$; this is permissible in view of what we already proved. By (32), we may take $m = \alpha r + \beta_1$, with $0 \leq \beta_1 < p + q$. Following Kaplan, we claim that

$$a_{\alpha r+\beta_1} = -b_{\alpha s+\beta_2}, \quad \text{with } \beta_2 = p + q + 1 - \beta_1.$$

To this end we observe that $[(kr + j)r^*]_{pq} = [(ks - j)s^*]_{pq}$, so that

$$f_r(kr + j) = f_s(ks - j).$$

This is the present case equivalent of Lemma 9. From this we deduce that if $|j| < p + q$ then

$$\chi_r(kr + j) = \chi_s(ks - j), \tag{52}$$

the equivalent of (40) in Lemma 10. Now apply (52) to the representations of $a_{\alpha r+\beta_1}$ and $b_{\alpha s+\beta_2}$ given by (23). The proof is completed on observing that the left and the right sides of (52) contribute with the opposite signs to the values of $a_{\alpha r+\beta_1}$ and $b_{\alpha s+\beta_2}$, respectively. □

References

[1] G. Bachman, On the coefficients of ternary cyclotomic polynomials, J. Number Theory 100 (2003), 104–116.

[2] G. Bachman, Ternary cyclotomic polynomials with an optimally large set of coefficients, Proc. Amer. Math. Soc. 132 (2004), 1943–1950.

[3] G. Bachman, Flat cyclotomic polynomials of order three, Bull. London Math. Soc. 38 (2006), 53–60.

[4] M. Beiter, Magnitude of the coefficients of the cyclotomic polynomial Φ_{pqr}, II, Duke Math. J. 38 (1971), 591–594.

[5] T. Flanagan, On the coefficients of ternary cyclotomic polynomials, MS Thesis, University of Nevada Las Vegas, 2006.

[6] Y. Gallot and P. Moree, Ternary cyclotomic polynomials having a large coefficient, J. Reine Angew. Math. 632 (2009), 105–125.

[7] Y. Gallot and P. Moree, Neighboring ternary cyclotomic coefficients differ by at most one, J. Ramanujan Math. Soc. 24 (2009), no. 3, 235–248.

[8] N. Kaplan, Flat cyclotomic polynomials of order three, J. Number Theory 127 (2007), 118–126.

[9] B. Lawrence, Bounding the coefficients of $\Phi_{pqr}(x)$. Joint Mathematics Meeting of AMS/MAA (2009), 1046-11-1150.

[10] H. W. Lenstra, Vanishing sums of roots of unity, Proceedings, Bicentennial Congress Wiskundig Genootschap II, Math. Centre Tracts 101 (Math. Centrum, Amsterdam, 1979), pp. 249–268.