ON A CLASS OF TERNARY INCLUSION-EXCLUSION POLYNOMIALS

GENNADY BACHMAN AND PIETER MOREE

ABSTRACT. A ternary inclusion-exclusion polynomial is a polynomial of the form

$$Q_{\{p,q,r\}} = \frac{(z^{pqr}-1)(z^p-1)(z^q-1)(z^r-1)}{(z^{pq}-1)(z^{qr}-1)(z^{rp}-1)(z-1)},$$

where p, q, and r are integers ≥ 3 and relatively prime in pairs. This class of polynomials contains, as its principle subclass, the ternary cyclotomic polynomials corresponding to restricting p, q, and r to be distinct odd prime numbers. Our object here is to continue the investigation of the relationship between the coefficients of $Q_{\{p,q,r\}}$ and $Q_{\{p,q,s\}}$, with $r \equiv s \pmod{pq}$. More specifically, we consider the case where $1 \leq s < \max(p,q) < r$, and obtain a recursive estimate for the function $A(p,q,r)$ – the function that gives the maximum of the absolute values of the coefficients of $Q_{\{p,q,r\}}$. A simple corollary of our main result is the following absolute estimate. If $s \geq 1$ and $r \equiv \pm s \pmod{pq}$, then $A(p,q,r) \leq s$.

1. INTRODUCTION

Throughout this paper we adopt the convention that the integers p, q, and r are relatively prime in pairs and that $p,q,r \geq 3$. To each set $\tau = \{\, p,q,r \,\}$ we associate a polynomial Q_τ given by

$$Q_\tau(z) = \frac{(z^{pqr}-1)(z^p-1)(z^q-1)(z^r-1)}{(z^{pq}-1)(z^{qr}-1)(z^{rp}-1)(z-1)}. \tag{1.1}$$

A routine application of the inclusion-exclusion principle to the roots of the factors on the right of (1.1) shows that Q_τ is indeed a polynomial and we refer to it as a ternary (or of order three) inclusion-exclusion polynomial. This class of polynomials generalizes the class of ternary cyclotomic polynomials which corresponds to restricting the parameters p, q, and r to be distinct odd prime numbers. As the terminology suggests, the notion of inclusion-exclusion polynomials is not restricted to the ternary case, and the reader is referred to [1] for an introductory discussion of inclusion-exclusion polynomials and their relation to cyclotomic polynomials. Our interest in inclusion-exclusion polynomials is motivated by the study of coefficients of cyclotomic polynomials. Thus in the ternary case, the only case we shall consider here, from a certain perspective, questions about coefficients of cyclotomic polynomials are really questions about coefficients of inclusion-exclusion polynomials. We shall see below that adopting this point of view is rather helpful.

Date: March 25, 2010.

1991 *Mathematics Subject Classification.* 11B83, 11C08.

Key words and phrases. Cylcotomic polynomials, inclusion-exclusion polynomials.

We wish to thank Yves Gallot for making available to us his calculations of heights of inclusion-exclusion polynomials.

The degree of Q_τ is

$$\varphi(\tau) = (p-1)(q-1)(r-1), \tag{1.2}$$

see [1], and we write

$$Q_\tau(z) = \sum_{m=0}^{\varphi(\tau)} a_m z^m \quad \big[a_m = a_m(\tau)\big].$$

It is plain from (1.1) that a_m are integral. Polynomial Q_τ is said to be flat if a_m takes on the values ± 1 and 0. The existence of flat Q_τ with an arbitrary large $\min(p,q,r)$ was first established in [2]. This was done by showing that if

$$q \equiv -1 \pmod{p} \quad \text{and} \quad r \equiv 1 \pmod{pq} \tag{1.3}$$

then Q_τ is flat. Actually in [2] this was stated explicitly for cyclotomic polynomials only, but the argument used applies equally well to inclusion-exclusion polynomials. In fact, this observation extends to much of the work on the coefficients of ternary cyclotomic polynomials (cyclotomic polynomials of low order in general - see [1]) and, in particular, to all such work referenced in this paper. Consequently, we shall ignore this distinction in the future and, when appropriate, simply state the corresponding result for inclusion-exclusion polynomials. An improvement on (1.3) was obtained by T. Flanagan [5] who replaced both the -1 and 1 there by ± 1. But the conditions on q in these results were entirely superfluous, for it was shown by N. Kaplan [7] that

$$Q_\tau \text{ is flat if } r \equiv \pm 1 \pmod{pq}. \tag{1.4}$$

Our object here is to establish a general principle of which (1.4) is seen to be a special case. We begin by introducing some conventions. Put

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

Moreover, in a slight abuse of notation, let us agree to write $A(p,q,r)$ in place of $A(\tau)$ when the dependence of A on the parameters p, q, and r needs to be made explicit. Let us emphasize that, in a departure from the usual practice, 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 plays an important role in our development. Correspondingly, we shall explicitly state any additional assumptions on p, q, and r when it is appropriate. In his work on (1.4), Kaplan showed that for $r > \max(p,q)$, $A(\tau)$ is determined completely by the residue class of r modulo pq. More precisely, he showed that if $r \equiv \pm s \pmod{pq}$ and $r, s > \max(p,q)$ then

$$A(p,q,r) = A(p,q,s). \tag{1.5}$$

Moreover, under the stronger assumption $r, s > pq$, he showed that, in fact, we have

$$\mathcal{A}_{\{p,q,r\}} = \begin{cases} \mathcal{A}_{\{p,q,s\}}, & \text{if } r \equiv s \pmod{pq}, \\ -\mathcal{A}_{\{p,q,s\}}, & \text{if } r \equiv -s \pmod{pq}. \end{cases} \tag{1.6}$$

The first of these identities was also proved by Flanagan [5]. These results gave a strong indication that for $r > \max(p,q)$, the set $\mathcal{A}_\tau$ is also determined completely by the residue class of r modulo pq.

We are thus lead to examine the relation between coefficients of $Q_{\{p,q,r\}}$ and $Q_{\{p,q,s\}}$ with $r \equiv s \pmod{pq}$. This problem splits naturally into two parts according to whether

$$r, s > \max(p,q) \quad \text{or} \quad r > \max(p,q) > s \geq 1. \tag{1.7}$$

say. The first of these cases was dealt with completely by the first author in [1]. It was shown there that the identity (1.6) indeed holds in the full range $r, s > \max(p,q)$. Let us mention in passing another interesting property of sets $\mathcal{A}_\tau$ (see [1, 4, 6]): $\mathcal{A}_\tau$ is simply a string of consecutive integers, that is

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

where $A^-(\tau)$ and $A^+(\tau)$ denote the smallest and the largest coefficients of Q_τ, respectively.

That leaves the second alternative in (1.7), and this case is the object of the present paper. The statement of our main result will make use of the following extension of the definition of $A(\tau)$. For $s = 1, 2$ and relatively prime in pairs triples $\{\, p, q, s \,\}$ put

$$A(p,q,s) = s - 1. \tag{1.8}$$

We note that this convention is not inappropriate when considered in the context of the corresponding polynomials $Q_{\{p,q,s\}}$. Indeed, $Q_{\{p,q,2\}}$ is of order 2 and its coefficients are ± 1 and 0, see [1], and, as is immediate from (1.1), $Q_{\{p,q,1\}}(z) \equiv 1$.

Theorem. *If $r \equiv \pm s \pmod{pq}$ and $r > \max(p,q) > s \geq 1$, then*

$$A(p,q,s) \leq A(p,q,r) \leq A(p,q,s) + 1. \tag{1.9}$$

Evidently this case is more complicated than the case covered by (1.5) and, according to the calculations kindly supplied by Yves Gallot, both possibilities implicit in (1.9) do occur quite readily. On the other hand, numerical evidence suggests that in this case too the equality (1.5) is the more likely outcome. We do not know of any simple criteria that can be used to determine which of the two possibilities in (1.9) must hold.

Note that under the hypothesis of the theorem we have, by (1.5),

$$A(p,q,r) = A(p,q,pq \pm s). \tag{1.10}$$

In this light (1.9) is seen as a recursive estimate. Of course, using an absolute upper bound for $A(p,q,s)$ on the right of (1.9) yields the corresponding upper bound for $A(p,q,r)$. The corollary below gives a particularly simple estimate of this type. To get it we use the bound

$$A(p,q,s) \leq s - \lceil s/4 \rceil \quad [s \geq 1], \tag{1.11}$$

proved in [3] (a better estimate for $\min(p,q,s) \geq 7$ was recently announced by J. Zhao and X. Zhang [8]).

Corollary. *Under the hypothesis of the theorem we have*

$$A(p,q,r) \leq s, \tag{1.12}$$

for all $s \geq 1$. Moreover, (1.12) *holds with strict inequality for $s \geq 5$.*

It should be noted that (1.11), and hence the corollary, hold with s replaced by $\min(p,q,s)$. Estimate (1.12) sacrifices precision for convenience and is certainly weaker than the upper bound of the theorem for $s \geq 5$. It is interesting, however, to consider the quality of this estimate for $s \leq 4$–the following observations are based largely on calculations of Yves Gallot. First we observe that the bound (1.11) is sharp in this range. For $s = 1, 2$ this follows by convention (1.8), and for $s = 3, 4$ this is verified computationally, e.g., $A(5,7,3) = 2$ and $A(11,13,4) = 3$. It follows that for $s \leq 4$, (1.12) is just the uniform version of the upper bound of the theorem, and that the possibility of equality in (1.12) is the only remaining question. That is, by (1.10), we are lead to consider the equation

$$A(p,q,pq+s) = s. \tag{1.13}$$

For $s = 1$, (1.13) holds for all choices of p and q since, trivially, $A(p,q,pq+1) \geq 1$. Recall that this is just Kaplan's result (1.4). Equation (1.13) also has solutions for $s = 2, 3$, for instance $A(3,5,17) = 2$ and $A(7,16,7\cdot 16+3) = 3$. On the other hand, no solutions were found for $s = 4$ with $p, q < 100$.

Using the estimate (1.11) carried no penalty for $s \leq 4$. For general s we ought to proceed implicitly and use the function

$$M(s) = \max_{p,q} A(p,q,s).$$

This is well defined by (1.11). Indeed, using $M(s)$ on the right of (1.9) gives a sharp form of (1.12) and leads us to consider the general form of (1.13), namely the equation

$$A(p,q,pq+s) = M(s)+1. \tag{1.14}$$

The main point is that solutions of (1.14) are particularly interesting instances of when the upper bound of the theorem is the best possible. Plainly, the focus here is on the parameter s, and we shall say that s solves (1.14) if the equation holds for some $\{\, p,q,s \,\}$. Thus we summarize the preceding paragraph by saying that (i) $M(s) = s-1$, for $s \leq 4$; and (ii) $s = 1, 2, 3$ are solutions of (1.14). Unfortunately equation (1.14) takes us into a largely unchartered territory. Indeed, in addition to the earlier discussion of $s \leq 4$ we can say with certainty only that $s = 5$ is also a solution. This follows on combining (1.11) with the explicitly computed $A(7,11,5) = 3 = M(5)$ and $A(13,43,13\cdot 43+5) = 4$.

Finally, observe that for certain types of triples τ, the application of the theorem may be iterated providing a very efficient technique for estimating $A(\tau)$. For instance, if p and q are relatively prime we get

$$A(q, pq\pm 1, q(pq\pm 1)\pm p) \leq A(q, pq\pm 1, p) + 1 = 2.$$

The remainder of this paper gives a proof of the theorem and is organized as follows. Our proof naturally splits into two parts corresponding to $s \leq 2$ (the "non-ternary case") and $s \geq 3$. In the next section we collect preliminaries needed for both cases. The non-ternary case is appreciably simpler and its proof is carried out in Section 3. We include the argument for $s = 1$ since it is substantially different from that of [7] and it helps to illuminate the more difficult general argument. Finally, we complete the proof in Section 4.

2. Preliminaries

We begin by observing that given a triple $\{p, q, r\}$, each integer n has a unique representation in the form

$$\begin{gathered} n = x_n qr + y_n rp + z_n pq + \delta_n pqr, \\ 0 \le x_n < p,\ 0 \le y_n < q,\ 0 \le z_n < r,\ \delta_n \in \mathbb{Z}. \end{gathered} \tag{2.1}$$

We shall say that n is (τ-)representable if $\delta_n \ge 0$ and let χ_τ be the characteristic function of representable integers. When τ is understood to be fixed we shall simply write χ in place of χ_τ. For our purposes it will be sufficient to consider only $n < pqr$, as we shall assume henceforth, and in this range the condition $\delta_n \ge 0$ becomes $\delta_n = 0$, so that

$$\chi(n) = \begin{cases} 1, & \text{if } \delta_n = 0, \\ 0, & \text{otherwise.} \end{cases} \tag{2.2}$$

The key role of representable integers is evident from the following identity – for the proof see [1].

Lemma 1. *For all $m < pqr$, we have*

$$a_m = \sum_{m-p<n\le m} \big(\chi(n) - \chi(n-q) - \chi(n-r) + \chi(n-q-r)\big). \tag{2.3}$$

Of course, we interpret a_m as 0 for $m < 0$ and $m > \varphi(\tau)$. Having the identity (2.3) in the "extended range" $m < 0$ and, by (1.2), $\varphi(\tau) < m < pqr$ will prove to be useful for technical reasons.

Recall that we are after a reduction for $A(p, q, r)$ with $r \equiv \pm s \pmod{pq}$, and eventually we shall assume that r satisfies this condition and that $p < q$. Let us emphasize, however, that unless any of these conditions are used there is complete symmetry in the parameters p, q, and r. For instance, Lemma 1 implies that (2.3) with p and r interchanged is also valid. When it is not inconvenient, e.g., (2.1) and (2.2), we make this symmetry perfectly explicit, but we shall opt for convenience, e.g., Lemmas 1 and 2, whenever this choice has to be made.

Lemma 2. $\big|\chi(n) - \chi(n-p) - \chi(n-q) + \chi(n-p-q)\big| \le 1.$

Proof. See [3, Lemma2]. □

Note that, by (2.1) and (2.2),

$$\chi(n) = \chi(n - pq) \quad \text{unless} \quad z_n = \delta_n = 0. \tag{2.4}$$

But $z_n = 0$ if and only if n is a multiple of r, say $n = kr$. Thus

$$\chi(kr + tpq) = \chi(kr) \quad [0 \le t < r]. \tag{2.5}$$

Similarly

$$\chi(kr - tpq) = 0 \quad [t > 0]. \tag{2.6}$$

These simple observations are quite handy. Thus our next lemma [1, Lemma 3] is an immediate consequence of Lemma 1 and (2.4).

Lemma 3. *Let*

$$I_1 = (m - q - p, m - q] \cap \mathbb{Z} \quad \textit{and} \quad I_2 = (m - p, m] \cap \mathbb{Z}. \tag{2.7}$$

Then we have

$$a_m = a_{m-pq},$$

unless there is $n \in I_1 \cup I_2$ *such that* n *is a multiple of* r *and either* n *or* $n-r$ *are representable.*

Next we consider (2.1) modulo pq (modulo a product of two of the parameters). Let r^* be the multiplicative inverse of r modulo pq and set

$$f(n) = f_{\tau,r}(n) = x_n q + y_n p, \tag{2.8}$$

with x_n and y_n given by (2.1). Then, in the first place, we have

$$f(n) \equiv nr^* \pmod{pq}. \tag{2.9}$$

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,

$$\mathcal{R}_{p,q} = \{\, N \mid N = xq + yp,\ x, y \geq 0 \,\}. \tag{2.10}$$

It follows by (2.8)–(2.10) that, in fact,

$$f(n) = \begin{cases} [nr^*]_{pq}, & \text{if } [nr^*]_{pq} \in \mathcal{R}_{p,q}, \\ [nr^*]_{pq} + pq, & \text{otherwise.} \end{cases} \tag{2.11}$$

There is an obvious advantage in considering linear combinations in (2.8) over those in (2.1). This is a useful observation in view of the following relationship between the functions χ and f.

Lemma 4. $\chi(n) = 1$ *if and only if* $f(n) \leq \lfloor n/r \rfloor$.

Proof. See [1, (3.26)] □

Our next lemma will be the only observation in this section that considers triples $\tau = \{\, p, q, r \,\}$ and $\tau' = \{\, p, q, s \,\}$ (with $r \equiv s \pmod{pq}$) simultaneously. To simplify the notation we consider p and q to be fixed and write $f_r(n)$ for $f_{\tau,r}(n)$. In this setting function $f_r(n)$ is a function of two variables but it depends only on the residue classes of r and n modulo pq.

Lemma 5. *If* $r \equiv s$, $n \equiv n' \pmod{pq}$, *then* $f_r(n) = f_s(n')$.

Proof. This is immediate from (2.11). □

Now put

$$\sigma_k(m) = \sum_{m-k<n\leq m} \chi(n). \tag{2.12}$$

Then, by Lemma 1, we have

$$a_m = \sigma_p(m) - \sigma_p(m-r) - \sigma_p(m-q) + \sigma_p(m-q-r). \tag{2.13}$$

For the purpose at hand we shall find it useful to rewrite this identity as follows.

Lemma 6. *If* $r = pq + s$ *and* $s \geq 1$, *then* $a_m = \Sigma_1 + \Sigma_2$, *with* Σ_i *given by*

$$\Sigma_1 = \sigma_s(m) - \sigma_s(m-p) - \sigma_s(m-q) + \sigma_s(m-q-p) \tag{2.14}$$

and

$$\Sigma_2 = \sigma_p(m-s) - \sigma_p(m-s-pq) - \sigma_p(m-q-s) + \sigma_p(m-q-s-pq). \tag{2.15}$$

Proof. Observe that

$$\sigma_p(m) = \sigma_s(m) + \sigma_p(m-s) - \sigma_s(m-p).$$

Whence

$$\begin{aligned}\sigma_p(m) - \sigma_p(m-r) &= \sigma_p(m) - \sigma_p(m-s-pq)\\ &= \sigma_s(m) - \sigma_s(m-p) + \sigma_p(m-s) - \sigma_p(m-s-pq).\end{aligned} \tag{2.16}$$

Of course, (2.16) also holds with $m-q$ in place of m. Combining this with (2.13) proves the claim. □

In the final lemma of this section we evaluate Σ_2 in (2.15). This evaluation depends on whether the two intervals

$$I_1' = (m-s-q-p, m-s-q] \cap \mathbb{Z} \quad \text{and} \quad I_2' = (m-s-p, m-s] \cap \mathbb{Z} \tag{2.17}$$

contain a multiple of r. Note that since $r = pq+s$, the range $I_1' \cup I_2'$ contains at most one multiple of r, which we will denote by αr.

Lemma 7. *If $r = pq+s$, $s \geq 1$, and $p < q$, then*

$$a_m = \begin{cases} \Sigma_1, & \text{if } \alpha r \notin I_1' \cup I_2', \\ \Sigma_1 + (-\chi(\alpha r))^j, & \text{if } \alpha r \in I_j', \end{cases}$$

with Σ_1 given by (2.14).

Proof. By Lemma 6, this is just an evaluation of Σ_2. But

$$\Sigma_2 = \sum_{m-s-p<n\leq m-s} \Big(\big(\chi(n) - \chi(n-pq)\big) - \big(\chi(n-q) - \chi(n-q-pq)\big) \Big).$$

Therefore, by (2.4), (2.6), and (2.17), we have

$$\Sigma_2 = \begin{cases} 0, & \text{if } \alpha r \notin I_1' \cup I_2', \\ (-\chi(\alpha r))^j, & \text{if } \alpha r \in I_j', \end{cases}$$

as claimed. □

3. Proof of theorem: the non-ternary case

At this stage we are ready to break the symmetry and, using the usual convention, put $p < q < r$. Moreover, we note that by (1.5) it suffices to prove (1.9) for $r = pq+s$, as we shall assume henceforth.

In this section we deal with $s \leq 2$. In this case (1.9) becomes,

$$s - 1 \leq A(p, q, pq+s) \leq s,$$

by (1.8), and the first of these inequalities is trivially satisfied. Therefore to complete the proof in the present case we need to show that every coefficient a_m of Q_τ satisfies

$$|a_m| \leq s. \tag{3.1}$$

Since inclusion-exclusion polynomials are reciprocal, see [1], we have $a_m = a_{\varphi(\tau)-m}$, and it suffices to prove (3.1) for $m \leq \varphi(\tau)/2$, as we shall now assume. Note that by (1.2), for m in this range the quantity αr occurring in Lemma 7 satisfies the condition

$$\alpha = \lfloor m/r \rfloor < \tfrac{1}{2}(p-1)(q-1), \tag{3.2}$$

which proves to be quite convenient.

An appeal to Lemma 7 leads us to consider two cases. The simplest case occurs when either $\alpha r \notin I_1' \cup I_2'$ or $\chi(\alpha r) = 0$. In this case Lemma 7 gives

$$a_m = \Sigma_1 = \sum_{m-s<n\le m} \big(\chi(n) - \chi(n-p) - \chi(n-q) + \chi(n-p-q)\big),$$

and the argument is completed by an application of Lemma 2.

Now suppose that $\alpha r \in I_j'$ and $\chi(\alpha r) = 1$. In this case it is simplest to treat $s = 1$ and $s = 2$ separately, and we consider $s = 1$ first. Then by Lemma 7 we have

$$a_m = \chi(m) - \chi(m-p) - \chi(m-q) + \chi(m-p-q) + (-1)^j. \tag{3.3}$$

We will evaluate this sum using Lemma 4. To this end we observe that since $\alpha r \in I_j'$, every argument of the function χ occurring in (3.3) is of the form $\alpha r + i$ with $|i| \le p + q$. Moreover, α satisfies (3.2). But by (2.9)

$$f(\alpha r + i) \equiv \alpha + i \pmod{pq},$$

since both r and its inverse r^* are congruent to 1 modulo pq. It follows from Lemma 4 and (2.11) that if $\chi(\alpha r + i) = 1$, then, in fact, $f(\alpha r + i) = \alpha + i$ and $i \le 0$. In particular, $\chi(m) = 0$. Furthermore, if $\alpha r \in I_1'$, then we also have $\chi(m-q) = \chi(m-p) = 0$, and (3.1) follows from (3.3). Moreover, we reach the same conclusion if $\alpha r \in I_2'$ and $\chi(m-p-q) = 0$. Finally, (3.3) also yields (3.1) under the assumptions $\alpha r \in I_2'$ and $\chi(m-p-q) = 1$, since in this case we must have $\chi(m-q) = 1$. To see this, write $m - p - q = \alpha r - i_0$, so that

$$q \le i_0 < p + q \quad \text{and} \quad f(m-p-q) = \alpha - i_0,$$

and observe that

$$[(m-q)r^*]_{pq} = [\alpha r - i_0 + p]_{pq} = \alpha - i_0 + p = x_{m-p-q}q + (y_{m-p-q} + 1)p,$$

by (2.8). Whence, by (2.11), $f(m-q) = \alpha - i_0 + p$ and the desired conclusion follows by Lemma 4. This completes the proof for $s = 1$.

The subcase $s = 2$ differs from the previous subcase only in some technical details. In place of (3.3) we now have, by Lemma 7,

$$a_m = \sigma_2(m) - \sigma_2(m-p) - \sigma_2(m-q) + \sigma_2(m-p-q) + (-1)^j \tag{3.4}$$

$$= \sum_{m-2<n\le m} \Big(\chi(n) - \chi(n-p) - \chi(n-q) + \chi(n-p-q)\Big) + (-1)^j. \tag{3.5}$$

Since $r = pq + 2$, $r^* = (pq+1)/2$ and it is now better to view arguments of χ in the form $\alpha r + 2i + \epsilon$, with $\epsilon = 0$ or 1. Indeed, by (2.9) we get

$$f(\alpha r + 2i + \epsilon) \equiv \alpha + i + \epsilon\frac{pq+1}{2} \pmod{pq}. \tag{3.6}$$

Now, by Lemma 3 we may assume that αr is either in $I_1 \cap I_1'$ or in $I_2 \cap I_2'$, so that every $\alpha r + 2i + \epsilon$ appearing as an argument in (3.5) satisfies $|2i + \epsilon| < p + q$. But then, by (3.6), (3.2), Lemma 4, and (2.11), we see that if $\chi(\alpha r + 2i + \epsilon) = 1$ then we must have $\epsilon = 0$ and $i \le 0$. It follows that $\sigma_2(m) = 0$ and that

$$\sigma_2(m-p), \sigma_2(m-q), \sigma_2(m-p-q) \le 1.$$

This is sufficient if $\alpha r \in I_2'$, for then (3.1) follows from (3.4). If on the other hand $\alpha r \in I_1'$, then we also have $\sigma_2(m-q) = \sigma_2(m-p) = 0$, and (3.1) follows in this case as well. This completes the proof in the non-ternary case.

4. Proof of theorem: the ternary case

Recall from Section 3 that we fixed $p < q$ and $r = pq + s$. In this section we will estimate $A(\tau)$ in terms of $A(\tau')$, where $\tau = \{ p, q, r \}$, $\tau' = \{ p, q, s \}$, and $3 \le s < q$, and this will require us to consider coefficients of Q_τ and $Q_{\tau'}$ simultaneously. To this end let us adopt the following conventions. We shall continue to write a_m for coefficients of Q_τ and we shall write b_l for coefficients of $Q_{\tau'}$. We shall write χ and χ' for the characteristic functions χ_τ and $\chi_{\tau'}$ defined in (2.1) and (2.2), respectively. We shall also write σ_k and σ'_k for the summatory functions defined in (2.12) with χ and χ', respectively.

Functions χ and χ', and hence σ and σ', are closely related. In the next three lemmas we collect certain properties of these functions.

Lemma 8. *If $|j| < s$ then*

$$\chi(kr + j) = \chi'(ks + j).$$

Proof. Since $f_r(kr+j) = f_s(ks+j)$, by Lemma 5, and $\lfloor (kr+j)/r \rfloor = \lfloor (ks+j)/s \rfloor$, the claim follows by Lemma 4. □

Lemma 9. *For $|k| < pq$, $0 < |j| < s$, and $|\beta| \le \lfloor pq/s \rfloor$, we have*

$$\chi(kr + j + \beta pq) = \chi(kr + j).$$

Proof. There is nothing to prove if $\beta = 0$, so assume that $0 < |\beta| \le \lfloor pq/s \rfloor$. Recall that $[N]_{pq}$ denotes the least nonnegative residue of N modulo pq and that $r^* = s^*$. Write

$$[k + js^*]_{pq} = [k]_{pq} + t_j. \tag{4.1}$$

Evidently

$$\lfloor pq/s \rfloor \le |t_j| \le pq - \lfloor pq/s \rfloor, \tag{4.2}$$

since $t_j s \equiv j \pmod{pq}$. Now suppose that $\chi(kr + j) = 1$. Plainly this is not possible unless $k > 0$. Therefore in this case we may replace $[k]_{pq}$ by k in (4.1) and, by (2.11) and Lemma 4, we get

$$f(kr + j) = k + t_j \quad \text{and} \quad t_j < 0. \tag{4.3}$$

Also, by Lemma 5, $f(kr + j + \beta pq) = f(kr + j)$. But

$$\Big\lfloor \frac{kr + j + \beta pq}{r} \Big\rfloor \ge k - |\beta| \ge k - \lfloor pq/s \rfloor,$$

and the claim in this case follows by (4.2) and Lemma 4.

On the other hand

$$\Big\lfloor \frac{kr + j + \beta pq}{r} \Big\rfloor < k + |\beta| \le k + \lfloor pq/s \rfloor.$$

Therefore if $\chi(kr + j + \beta pq) = 1$ then, by Lemma 4, $f(kr + j) < k + \lfloor pq/s \rfloor$. Arguing as before one readily verifies that this implies that (4.3) must hold. This yields $\chi(kr + j) = 1$, and the proof is complete. □

Lemma 10. *For $|k| < pq$, $0 \le \gamma < s$, and $|\beta| \le \lfloor pq/s \rfloor$, we have*

$$\begin{aligned} \sigma_s(kr + \gamma + \beta pq) - \chi(kr + \beta pq) &= \sigma'_s(ks + \gamma) - \chi'(ks) \\ &= \sigma'_s(ks + \gamma - pq). \end{aligned}$$

Proof. The first identity follows from Lemmas 8 and 9. The second identity follows from (2.4) and (2.6) with χ' in place of χ. □

Our preparation is now complete and we are ready to embark on the main argument. Let a_m be a coefficient of Q_τ and set $\alpha = \lfloor m/r \rfloor$. Recall from Section 3 that we may assume that α satisfies (3.2). Furthermore, by Lemma 3, we may also assume that

$$\alpha r \in I_1 \cup I_2. \tag{4.4}$$

Now write

$$\begin{aligned} m_1 &= m = \alpha r + \beta_1 s + \gamma_1, & m_2 &= m - p = \alpha r + \beta_2 s + \gamma_2, \\ m_3 &= m - q = \alpha r + \beta_3 s + \gamma_3, & m_4 &= m - p - q = \alpha r + \beta_4 s + \gamma_4, \end{aligned} \tag{4.5}$$

with $0 \le \gamma_i < s$. Moreover, set

$$l_i = (\alpha + \beta_i)s + \gamma_i \quad \text{and} \quad l = l_1 \tag{4.6}$$

and observe that

$$l_2 = l - p,\ l_3 = l - q,\ \text{and } l_4 = l - p - q. \tag{4.7}$$

From (4.5), (4.4), and (2.7) we see that $s|\beta_i| < p + q + s$, so that

$$|\beta_i| \le \lfloor 3q/s \rfloor \le \lfloor pq/s \rfloor, \tag{4.8}$$

and, by (3.2),

$$|\alpha + \beta_i| < pq. \tag{4.9}$$

Now, by (4.5), quantities m_i have a representation in the form

$$m_i = (\alpha + \beta_i)r + \gamma_i - \beta_i pq.$$

Therefore, by (4.9), (4.8), Lemma 10, and (4.6), we have

$$\sigma_s(m_i) - \chi\big((\alpha + \beta_i)r - \beta_i pq\big) = \sigma'_s(l_i) - \chi'\big((\alpha + \beta_i)s\big) \tag{4.10}$$

$$= \sigma'_s(l_i - pq). \tag{4.11}$$

We are now in the position to relate the sum Σ_1 given by (2.14) and the coefficient b_l of $Q_{\tau'}$ with l given in (4.6). Using notation (4.5) we write

$$\Sigma_1 = \sum_{i=1}^{4} \theta(i)\sigma_s(m_i), \tag{4.12}$$

where $\theta(i) = 1$, for $i = 1, 4$, and $\theta(i) = -1$, for $i = 2, 3$. On the other hand, by (4.6) and (4.9), Lemma 1 with r replaced by s applies to the coefficient b_l. We implement (2.3) with χ' in place of χ and with p and r replaced by s and p, respectively, to get

$$b_l = \sum_{i=1}^{4} \theta(i)\sigma'_s(l_i), \tag{4.13}$$

by (4.7). Similarly

$$b_{l-pq} = \sum_{i=1}^{4} \theta(i)\sigma'_s(l_i - pq). \tag{4.14}$$

Therefore, by (4.12), (4.13), and (4.10), we have

$$\Sigma_1 - b_l = \sum_{i=1}^{4} \theta(i)\Big(\chi\big((\alpha+\beta_i)r - \beta_i pq\big) - \chi'\big((\alpha+\beta_i)s\big)\Big).$$

Furthermore applying (2.5), Lemma 8, and (2.6) to the right side of this expression gives

$$\begin{aligned}\Sigma_1 - b_l &= \sum_{\beta_i>0} \theta(i)\Big(\chi\big((\alpha+\beta_i)r - \beta_i pq\big) - \chi'\big((\alpha+\beta_i)s\big)\Big)\\ &= -\sum_{\beta_i>0} \theta(i)\chi'((\alpha+\beta_i)s).\end{aligned} \tag{4.15}$$

Moreover if we use (4.14) and (4.11) in place of (4.13) and (4.10) the same computation yields

$$\begin{aligned}\Sigma_1 - b_{l-pq} &= \sum_{i=1}^{4} \theta(i)\chi\big((\alpha+\beta_i)r - \beta_i pq\big)\\ &= \sum_{\beta_i\le 0} \theta(i)\chi\big((\alpha+\beta_i)r - \beta_i pq\big).\end{aligned} \tag{4.16}$$

We complete the proof by considering the two alternatives of Lemma 7. Suppose first that $\alpha r \notin I_1' \cup I_2'$, with I_j' given by (2.17). One then readily verifies that, in view of (4.4) and (4.5), we must have either

$$\beta_1 = 0 > \beta_2 \ge \beta_3 \ge \beta_4, \tag{4.17}$$

if $\alpha r \in I_2$, or

$$\beta_4 < \beta_3 = 0 < \beta_2 \le \beta_1, \tag{4.18}$$

if $\alpha r \in I_1$. In either case $a_m = \Sigma_1$, by Lemma 7, so that (4.15) holds with Σ_1 replaced by a_m. But under (4.17) the right side of (4.15) vanishes and we get

$$a_m = b_l. \tag{4.19}$$

Observe that by (4.6), (3.2), and (1.2), index $l = \alpha s + \gamma_1$ is arbitrary in the range $l \le \varphi(\tau')/2$. Thus (4.19) says that every integer occurring as a coefficient of $Q_{\tau'}$ is also a coefficient of Q_τ and the first inequality in (1.9) follows.

Now consider (4.18). In this case (4.15) yields

$$a_m - b_l = \chi'((\alpha+\beta_2)s) - \chi'((\alpha+\beta_1)s),$$

so that we certainly have

$$|a_m - b_l| \le 1. \tag{4.20}$$

But (4.19) and (4.20) imply the right side of (1.9), and it only remain to consider the second alternative of Lemma 7.

Suppose now that, in addition to (4.4), $\alpha r \in I_1' \cup I_2'$. Then, reasoning as in (4.17) and (4.18), we conclude that either

$$\beta_4 \le \beta_3 \le \beta_2 \le 0 < \beta_1, \tag{4.21}$$

if $\alpha r \in I_2'$, or

$$\beta_4 \le 0 < \beta_3 \le \beta_2 \le \beta_1, \tag{4.22}$$

if $\alpha r \in I_1'$. In the first case we get, by Lemma 7, (4.15), and (4.21),

$$a_m - b_l = \chi(\alpha r) - \chi'((\alpha+\beta_1)s).$$

Therefore (4.20) holds in this case as well. In the second case we appeal to (4.16) instead of (4.15) to get, by Lemma 7 and (4.22),

$$a_m - b_{l-pq} = \chi\big((\alpha+\beta_4)r - \beta_4 pq\big) - \chi(\alpha r).$$

This yields (4.20) with b_l replaced by b_{l-pq}, and completes the proof of the theorem.

References

[1] G. Bachman, On ternary inclusion-exclusion polynomials, Integers, to appear.
[2] ———, Flat cyclotomic polynomials of order three, Bull. London Math. Soc. 38 (2006), 53–60.
[3] ———, On the coefficients of ternary cyclotomic polynomials, J. Number Theory 100 (2003), 104–116.
[4] B. Bzdęga, Bounds on ternary cyclotomic coefficients, Acta Arith., to appear.
[5] T. Flanagan, On the coefficients of ternary cyclotomic polynomials, MS Thesis, University of Nevada Las Vegas, 2006.
[6] Y. Gallot and P. Moree, Neighboring ternary cyclotomic coefficients differ by at most one, J. Ramanujan Math. Soc. 24 (2009), 235–248.
[7] N. Kaplan, Flat cyclotomic polynomials of order three, J. Number Theory 127 (2007), 118–126.
[8] J. Zhao and X. Zhang, A proof of the corrected Beiter conjecture, arXiv:0910.2770v1 [math.NT].

University of Nevada, Las Vegas, Department of Mathematical Sciences, 4505 Maryland Parkway, Las Vegas, Nevada 89154-4020, USA
E-mail address: bachman@unlv.nevada.edu

Max-Planck-Institut für Mathematic, Vivatsgasse 7, D-53111 Bonn, Germany.
E-mail address: moree@mpim-bonn.mpg.de