Max-Planck-Institut für Mathematik
Bonn

Non-Beiter ternary cyclotomic polynomials with an optimally large set of coefficients

by

Pieter Moree
Eugenia Rosu

Max-Planck-Institut für Mathematik
Preprint Series 2011 (81)

Non-Beiter ternary cyclotomic polynomials with an optimally large set of coefficients

Pieter Moree
Eugenia Rosu

Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
Germany

Department of Mathematics
Evans Hall
UC Berkeley
Berkeley CA 94720-3840
USA

MPIM 11-81

Non-Beiter ternary cyclotomic polynomials with an optimally large set of coefficients

Pieter Moree and Eugenia Rosu

Abstract

Let $l \geq 1$ be an arbitrary odd integer and p, q and r primes. We show that there exist infinitely many ternary cyclotomic polynomials $\Phi_{pqr}(x)$ with $l^2 + 3l + 5 \leq p < q < r$ such that the set of coefficients of each of them consists of the p integers in the interval $[-(p-l-2)/2, (p+l+2)/2]$. It is known that no larger coefficient range is possible. The Beiter conjecture states that the cyclotomic coefficients $a_{pqr}(k)$ of Φ_{pqr} satisfy $|a_{pqr}(k)| \leq (p+1)/2$ and thus the above family contradicts the Beiter conjecture. The two already known families of ternary cyclotomic polynomials with an optimally large set of coefficients (found by G. Bachman) satisfy the Beiter conjecture.

1 Introduction

The n-th cyclotomic polynomial is defined by

$$\Phi_n(x) = \prod_{1 \leq j \leq n, (j,n)=1} (x - \zeta_n^j) = \sum_{k=0}^{\varphi(n)} a_n(k) x^k,$$

with $\zeta_n = e^{2\pi i/n}$ and $\varphi(n)$ Euler's totient function. For $k > \varphi(n)$, take $a_n(k) = 0$. We put $A\{n\} = \{a_n(k) : k \geq 0\}$ and $A(n) = \max\{|a_n(k)| : k \geq 0\}$.

In this paper we will restrict to the (so-called ternary) case $n = pqr$, with $2 < p < q < r$ primes. In [1] (Corollary 3) Bachman has proved that the difference between the largest and the smallest coefficient is at most p. Thus the cardinality of $A\{pqr\}$ is at most p. If it is exactly p we say that Φ_{pqr} has an *optimally large set of coefficients*

Sister Beiter [4] conjectured in 1968 that $|a_{pqr}(k)| \leq (p+1)/2$. Beiter's conjecture implies that if $A\{pqr\}$ has cardinality p, then either $A\{pqr\} = \{-(p-1)/2, \ldots, (p+1)/2\}$ or $A\{pqr\} = \{-(p+1)/2, \ldots, (p-1)/2\}$. In 2004 Bachman [2] constructed two infinite families of ternary cyclotomic polynomials having these respective coefficient sets.

Mathematics Subject Classification (2000). 11N37, 11B83

Put $M(p) = \max\{A(pqr) : r > q > p\}$, where (q, r) runs over all prime pairs with $r > q > p$. Gallot and Moree [7] disproved Beiter's conjecture. They showed that $M(p) > (p+1)/2$ for $p \geq 11$ and that, for $0 < \epsilon < 2/3$ one has $M(p) > (2/3 - \epsilon)p$ for every p sufficiently large. They conjectured that $M(p) \leq 2p/3$. We like to point out that the construction of large coefficients given in this paper are in accord with this conjecture. Given an arbitrary integer $\delta \geq 0$ it is thus conceivable that we can have δ_-*-optimal*, respectively δ_+*-optimal* ternary cyclotomic polynomials Φ_{pqr} having $A\{pqr\} = \{-(p+1)/2+\delta, \ldots, (p-1)/2+\delta\}$, respectively $A\{pqr\} = \{-(p-1)/2-\delta, \ldots, (p+1)/2-\delta\}$ as coefficient sets. Thus the construction of $0_\pm$-optimal Φ_{pqr} is due to Bachman. In this paper we give the construction (due to Rosu) of $\delta_\pm$-optimal Φ_{pqr} for every $\delta \geq 1$ (with $\delta = (l+1)/2$). Every so constructed Φ_{pqr} will be a counter-example to Sister Beiter's conjecture.

The following lemma shows that it is enough to construct δ_+-optimal Φ_{pqr}.

Lemma 1 *Suppose that Φ_{pqr} is δ_+-optimal and $r > pq$. Let $s > pq$ be a prime such that $s \equiv -r (\text{mod } pq)$, then Φ_{pqs} is δ_--optimal.*

The proof of this lemma is a corollary of the result of Kaplan [11] that under the conditions of the lemma one has $A\{pqr\} = -A\{pqs\}$. For a sharpening of this result, see Bachman [3].

Theorem 1 *Let $l \geq 1$ be an odd integer and $p \geq l^2 + 3l + 5$ a prime. Then there exists an infinite sequence of prime pairs $\{(q_j, r_j)\}_{j=1}^{\infty}$ with $pq_j < r_j$, $q_{j+1} > q_j$, such that*

$$\{a_{pq_jr_j}(k) : k \geq 0\} = \Big\{ -\frac{p-l-2}{2}, \ldots, \frac{p+l+2}{2} \Big\},$$

and hence $\Phi_{pq_jr_j}$ is $(l+1)/2_+$-optimal.

Proof. Theorem 2 (which is stated and proved in Section 3) and Lemma 4 allow us to determine (q_j, r_j) such that

$$A\{pq_jr_j\} = \Big\{ -\frac{p-l-2}{2}, \ldots, \frac{p+l+2}{2} \Big\}. \tag{1}$$

(For notational convenience we write $-\frac{p-1}{2}$, rather than $-\frac{(p-1)}{2}$, etc..) Using Dirichlet's theorem for primes in arithmetic progressions we see that there exists an infinite family $\{(q_j, r_j)\}_{j=1}^{\infty}$ with $pq_j < r_j$, $q_{j+1} > q_j$, satisfying (1). □

Corollary 1 *The Sister Beiter conjecture is false for every $p \geq 11$.*

Kaplan's Lemma (see Section 2) is the main tool in the proof of Theorem 2. Another helpful result we will use is the 'jump-one property' (see [5, 8, 13]), which states that for ternary n we have $|a_n(k) - a_n(k+1)| \leq 1$. As a warm-up in using these tools the reader may consult the alternative construction, by Gallot and Moree [8], of Bachman's $0_\pm$-optimal family. (When Bachman wrote his paper neither Lemma 1, nor the jump-one property, nor the falsity of the Sister Beiter conjecture were known.)

Let $M(p; q) := \max\{A(pqr) : r > q\}$, where the maximum is over all primes r exceeding q and $p < q$ are fixed primes. In Section 4 applications of the main result, Theorem 2 below, in the study of $M(p; q)$ will be given. A question of Wilms (2010) first posed in [9] will be answered in the positive. Also it is shown that the construction presented here yields a lower bound $M_R(p)$ for $M(p)$ that satisifies $M_R(p) \geq M_{GM}(p)$, with $M_{GM}(p)$ the lower bound that was established in the paper by Gallot and Moree [7]. Numerically one finds many p with $M_R(p) > M_{GM}(p)$.

The problem of finding non-Beiter ternary cyclotomic polynomials with an optimally large set of coefficients was posed by Moree to Rosu as an internship problem. Rosu's solution of this is presented here. The write-up of this construction was a cooperative effort of the authors, baving a rough draft by Rosu as a starting point. The section with the applications is due to the first author.

2 Kaplan's Lemma

Our main tool will be the following result of Kaplan [11], the proof of which uses the identity

$$\Phi_{pqr}(x) = (1 + x^{pq} + x^{2pq} + \cdots)(1 + x + \cdots + x^{p-1} - x^q - \cdots - x^{q+p-1})\Phi_{pq}(x^r).$$

Lemma 2 (Nathan Kaplan, 2007). *Let $2 < p < q < r$ be primes and $k \geq 0$ be an integer. Put*

$$b_i = \begin{cases} a_{pq}(i) & \text{if } ri \leq k; \\ 0 & \text{otherwise.} \end{cases}$$

We have

$$a_{pqr}(k) = \sum_{m=0}^{p-1} (b_{f(m)} - b_{f(m+q)}), \quad (2)$$

where $f(m)$ is the unique integer such that $f(m) \equiv r^{-1}(k - m)(\text{mod } pq)$ and $0 \leq f(m) < pq$.

Lemma 2 reduces the computation of $a_{pqr}(k)$ to that of $a_{pq}(i)$ for various i. These binary cyclotomic polynomial coefficients are computed in the following lemma. For a proof see e.g. Lam and Leung [12].

Lemma 3 *Let $p < q$ be odd primes. Let ρ and σ be the (unique) non-negative integers for which*

$$1 + pq = (\rho + 1)p + (\sigma + 1)q. \quad (3)$$

Let $0 \leq m < pq$. Then either $m = \alpha_1 p + \beta_1 q$ or $m = \alpha_1 p + \beta_1 q - pq$ with $0 \leq \alpha_1 \leq q - 1$ the unique integer such that $\alpha_1 p \equiv m(\text{mod } q)$ and $0 \leq \beta_1 \leq p - 1$ the unique integer such that $\beta_1 q \equiv m(\text{mod } p)$. The cyclotomic coefficient $a_{pq}(m)$ equals

$$\begin{cases} 1 & \text{if } m = \alpha_1 p + \beta_1 q \text{ with } 0 \leq \alpha_1 \leq \rho,\ 0 \leq \beta_1 \leq \sigma; \\ -1 & \text{if } m = \alpha_1 p + \beta_1 q - pq \text{ with } \rho + 1 \leq \alpha_1 \leq q - 1,\ \sigma + 1 \leq \beta_1 \leq p - 1; \\ 0 & \text{otherwise.} \end{cases}$$

We say that $[m]_p = \alpha_1$ is the *p-part of* m and $[m]_q = \beta_1$ is the *q-part of* m. It is easy to see that

$$m = \begin{cases} [m]_p p + [m]_q q & \text{if } [m]_p \le \rho \text{ and } [m]_q \le \sigma; \\ [m]_p p + [m]_q q - pq & \text{if } [m]_p > \rho \text{ and } [m]_q > \sigma; \\ [m]_p p + [m]_q q - \delta_m pq & \text{otherwise,} \end{cases}$$

with $\delta_m \in \{0, 1\}$. Using this observation we find that, for $i < pq$,

$$b_i = \begin{cases} 1 & \text{if } [i]_p \le \rho, [i]_q \le \sigma \text{ and } [i]_p p + [i]_q q \le k/r; \\ -1 & \text{if } [i]_p > \rho, [i]_q > \sigma \text{ and } [i]_p p + [i]_q q - pq \le k/r; \\ 0 & \text{otherwise.} \end{cases}$$

Thus in order to evaluate $a_{pqr}(n)$ using Kaplan's lemma it suffices to compute $[f(m)]_p$, $[f(m)]_q$, $[f(m+q)]_p$ and $[f(m+q)]_q$. Indeed, as $[f(m)]_p = [f(m+q)]_p$, it suffices to compute $[f(m)]_p$, $[f(m)]_q$, and $[f(m+q)]_q$. Note that, modulo pq,

$$f(m+q) \equiv \frac{k-m}{r} - \frac{q}{r} \equiv f(m) + q\left(\left[-\frac{1}{r}\right]_p p + \left[-\frac{1}{r}\right]_q q\right) \equiv f(m) + q^2\left[-\frac{1}{r}\right]_q,$$

and hence

$$f(m+q) \equiv f(m) + q^2\left[-\frac{1}{r}\right]_q \pmod{pq}. \tag{4}$$

We will say that the p and q-parts of γ are in the same range if $0 \le [\gamma]_p \le \rho$ and $0 \le [\gamma]_q \le \sigma$ or if $\rho + 1 \le [\gamma]_p \le q - 1$ and $\sigma + 1 \le [\gamma]_q \le p - 1$.

3 The main construction

Let $l \ge 1$ be an arbitrary odd integer.

The main construction only works if the residue $2/(l+2)$ modulo p is in an union of two intervals. The next lemma will be used to show that if $p \ge l^2 + 3l + 5$, then the residue is in the union of these two intervals.

Lemma 4 *Let* $(l+2)a \equiv 2 (\text{mod } p)$*, where* $0 \le a \le p - 1$ *and* $p \ge l^2 + 3l + 5$*. Then* $a \in [l+2, (p-l-2)/2] \cup [(p+l+2)/2, p-l-2]$*.*

Proof. The integer a is of the form $(2 + np)/(l+2)$ for some positive integer n and hence

$$a \ge \frac{n(l+1)(l+2)+2}{l+2} > l+1.$$

Suppose that

$$p - 1 \ge \frac{np+2}{l+2} \ge p - l - 1.$$

Then

$$l + 2 - \frac{l+4}{p} \ge n \ge l + 2 - \frac{l^2+3l+4}{p} > l+1,$$

contradiction. Thus $a \le p-l-2$.

Finally suppose that

$$\frac{p-l}{2} \le \frac{np+2}{l+2} \le \frac{p+l}{2}.$$

Then

$$l+2-\frac{l(l+2)+4}{p} \le 2n \le l+2+\frac{l(l+2)-4}{p},$$

implying $2n = l+2$, which is not possible as l is odd. □

The following lemma is important in the proof of the main construction:

Lemma 5 *Let u and t be integers and α, β, r, p and q be positive integers, with $\beta > \alpha$ and $r > pq$. Put $k(t) = ur + tpq$. Then*

$$\alpha < \frac{k(t_1)}{r} < \beta, \tag{5}$$

where

$$t_1 = \left[\frac{(\alpha-u)r}{pq}\right] + 1.$$

Proof. The inequality $\alpha < k(t)/r < \beta$ is equivalent with

$$t \in \Big(\frac{(\alpha-u)r}{pq}, \frac{(\beta-u)r}{pq}\Big).$$

Since this interval has length exceeding one, t_t is in it and hence (5) is satisfied. □

It is practical to note that $1+pq = (\rho+1)p + (\sigma+1)q$ can be rewritten as $(p-1)(q-1) = \rho p + \sigma q$. By $[x]$ we denote the largest integer $\le x$.

Theorem 2 *Let $l \ge 1$ be an arbitrary odd integer. Let $2 < p < q$ be primes satisfying*

$$q \ge \frac{(p+l)p}{2}, \ q \equiv \frac{2}{l+2} (\text{mod } p).$$

Let ρ and σ be the (unique) non-negative integers for which $1+pq = (\rho+1)p + (\sigma+1)q$. Write $\rho = (p+l)s/2 + \tau$ with $0 \le \tau < (p+l)/2$ (thus $s = [2\rho/(p+l)]$). Let $r_1, r_2 > pq$ be primes such that

$$-\frac{1}{r_1} \equiv q - sp (\text{mod } pq) \text{ and } r_2 \equiv -r_1 (\text{mod } pq). \tag{6}$$

Let $\alpha_1^+ = (p+l)q/2$ and $\alpha_1^- = (\rho+s)p - q$. Let $u_1^+, t_1^+, u_1^-, t_1^-, u_2^+, t_2^+, u_2^-, t_2^-$ be as in Table 1 and define

$$k_1^+ = r_1u_1^+ + t_1^+pq, \ k_1^- = r_1u_1^- + t_1^-pq, \ k_2^+ = r_2u_2^+ + t_2^+pq, \ k_2^- = r_2u_2^- + t_2^-pq.$$

Let $w(l+2) \equiv 2 (\text{mod } p)$, with $0 \le w \le p-1$.
If $l+2 \le w \le (p-l-2)/2$, then

$$a_{pqr_1}(k_1^-) = -\frac{p-l-2}{2}, \ a_{pqr_1}(k_1^+) = \frac{p+l+2}{2},$$

and $\{a_{pqr_1}(k) : k \geq 0\} = \{-(p-l-2)/2, \ldots, (p+l+2)/2\}$.
If $(p+l+2)/2 \leq w \leq p-l-2$, *then*

$$a_{pqr_2}(k_2^-) = -\frac{p-l-2}{2}, \; a_{pqr_2}(k_2^+) = \frac{p+l+2}{2},$$

and $\{a_{pqr_2}(k) : k \geq 0\} = \{-(p-l-2)/2, \ldots, (p+l+2)/2\}$.

In both cases we have $M(p;q) := \max\{A(pqr) : r > q\} = (p+l+2)/2 < 2p/3$.

TABLE 1

u_1^+, t_1^+	$(\rho - \tau)p$	$\left[(\alpha_1^+ - u_1^+)r_1/pq\right] + 1$
u_1^-, t_1^-	$-(p-l-2)q/2 + ((p-1)s + \tau)p$	$\left[(\alpha_1^- - u_1^-)r_1/pq\right] + 1$
u_2^+, t_2^+	$(p-1)q - (p-l-2)sp/2$	$\left[(\alpha_1^+ - u_2^+)r_2/pq\right] + 1$
u_2^-, t_2^-	$(p+l)q/2 + \tau p$	$\left[(\alpha_1^- - u_2^-)r_2/pq\right] + 1$

The idea of the proof is the following:

- In all cases, we take k of the form $k = ut + pqr$, with $t = [(\alpha - u)r/pq] + 1$.
- We tabulate the p-parts and q-parts of $f(m)$, respectively of $f(m+q)$. We will claim what values each $b_{f(m)}$ must take, first for $0 \leq m \leq p-1$, then for $q \leq m \leq q+p-1$.
- If the p-parts and q-parts of $f(m)$ are in different ranges, then $b_{f(m)} = 0$ by Kaplan's Lemma and Lemma 3.
- If the p-parts and q-parts of $f(m)$ are in the same range we have to check whether $f(m) \leq k/r$ or not, in order to deduce that $b_{f(m)} = 1$, respectively $b_{f(m)} = 0$.
- In this way we find as a lower bound the number α that we chose in the definition of k and as an upper bound a number β.
- We check that α, β and k verify the conditions of Lemma 5, which implies that
  - $k > 0$, thus $a_{pqr}(k)$ is well-defined
  - the inequalities claimed are true and the $b_{f(m)}$ take the claimed values.
  - $a_{pqr}(k)$ can be computed by (2)
- We invoke the jump one property and a known upper bound on $M(p;q)$ to finish the proof.

We like to point out that in Kaplan's Lemma one is allowed to take any positive integer k. If applying it yields $a_{pqr}(k) \neq 0$, then this implies that $0 \leq k \leq \varphi(pqr)$. In particular $k_1^+, k_1^-, k_2^+, k_2^-$ are all in the range $(0, \varphi(pqr)]$. An a posteriori check like this leaves one often with cleaner hands than checking this a priori.

Definition 1 *We will use Kaplan's Lemma for the following* (k,r)*-pairs:* (k_1^-, r_1), (k_1^+, r_1), (k_2^-, r_2), (k_2^+, r_2) *and denote the corresponding* f*-function by, respectively,* $f_1^-, f_1^+, f_2^-, f_2^+$.

TABLE 2

m	$[f_1^+(m)]_p$	$[f_1^+(m)]_q$	$[f_1^+(m+q)]_q$
0	$\rho-\tau$	0	w
1	$\rho-\tau-s$	1	$1+w$
2	$\rho-\tau-2s$	2	$2+w$
$\dots$	$\dots$	$\dots$	$\dots$
$\frac{p+l}{2}-w$	$\rho-\tau-\left(\frac{p+l}{2}-w\right)s$	$\frac{p+l}{2}-w$	$\frac{p+l}{2}$
$\dots$	$\dots$	$\dots$	$\dots$
$\frac{p+l}{2}$	0	$\frac{p+l}{2}$	$\frac{p+l}{2}+w$
$\frac{p+l+2}{2}$	$q-s$	$\frac{p+l+2}{2}$	$\frac{p+l+2}{2}+w$
$\dots$	$\dots$	$\dots$	$\dots$
$p-1-w$	$q-\left(\frac{p-l-2}{2}-w\right)s$	$p-1-w$	$p-1$
$p-w$	$q-\left(\frac{p-l}{2}-w\right)s$	$p-w$	0
$\dots$	$\dots$	$\dots$	$\dots$
$p-1$	$q-\frac{p-l-2}{2}s$	$p-1$	$w-1$

Proof of Theorem 2. In the case where $w=(p-l-2)/2$ or $w=(p+l+2)/2$ our argument will need some minor modification and those cases will be left to the interested reader.

If $l+2>(p-l-2)/2$ there is nothing to prove, so assume that $p\ge 3l+8$. Note that $(p+l+2)q\equiv 2 (\text{mod } p)$. Since $l\le p-4$, we infer that $q^*=(p+l+2)/2$, so $\sigma=q^*-1=(p+l)/2$. Knowing σ, we compute 2ρ as

$$\rho=\frac{pq-(l+2)q-2p+2}{2p} \tag{7}$$

from (3). We have $\rho<q/2$. Clearly we can write $\rho=(p+l)s/2+\tau$, with $0\le\tau<(p+l)/2$. Note that

$$q>\frac{pq}{p+l}>\frac{2\rho p}{p+l}\ge sp \text{ and } q\ge\frac{(p+l)p}{2}\ge(\tau+1)p,$$

and hence

$$q\ge\max\{sp+1,(\tau+1)p\}. \tag{8}$$

We have

$$2\rho\ge\frac{(p-(l+4))q}{p}\ge(p-(l+4))\frac{(p+l)}{2}\ge(l+2)(p+l),$$

and hence $s\ge l+2$. Using that $1\le s<q$, we infer $(q-sp,pq)=1$. By Dirichlet's theorem we then find that there are infinitely many primes $r_1,r_2>pq$ satisfying congruence (6).

-The computation of $a_{pqr_1}(k_1^+)$

Claim A: Assume that $l+2 \le w \le (p-l-4)/2$. Then Tables 2 and 3 are correct.
Proof of Claim A. Note that $f_1^+(0) \equiv \dfrac{k_1^+}{r_1} \equiv u_1^+ \equiv (\rho-\tau)p (\mathrm{mod}\ pq)$. By (6) we have $[-\frac{1}{r_1}]_q = 1$. Using (4) and $q \equiv w (\mathrm{mod}\ p)$ we get

$$f_1^+(m+q) \equiv f_1^+(m) + q^2\left[-\frac{1}{r_1}\right]_q \equiv f_1^+(m) + wq (\mathrm{mod}\ pq). \tag{9}$$

This shows that the entries in the first row of Table 2 are as given. It is now very easy to compute the remaining entries. We note that $f_1^+(m+1) \equiv f_1^+(m) - \frac{1}{r_1}(\mathrm{mod}\ pq)$. Together with (6) it then follows that in order to get the $(j+1)$th row from the jth, we have to subtract s from the p-part in row j and add 1 to the q-part in row j and reduce the result in such a way that the p-part is in $[0, q-1]$ and the q-part is in $[0, p-1]$. Since $\rho = (p+l)s/2 + \tau$, we get at p-part zero in row $\frac{p+l}{2}$. The correctness of Table 2 is established once we show that the last entry in the second column is non-negative. In fact, we have

$$q - \frac{p-l-2}{2}s > \rho. \tag{10}$$

Indeed, since $\rho = \frac{p+l}{2}s + \tau$ and $2\rho < q$, we have $q - \rho > \rho > \dfrac{p-l-2}{2}s$. Using (10) and $\sigma = \frac{p+l}{2}$ one eesily sees that the fourth and fifth column in Table 3 are correct.

Next we consider $f_1^+(m)$ for the range $0 \le m \le (p+l)/2$. Since $q > sp$ and $f_1^+(m)$ for that range is increasing (we have $f_1^+(m) = f_1^+(0) + m(q-sp)$), in order to show that $f_1^+(m) \le k_1^+/r_1$ in that range, we need only establish this inequality for $m = (p+l)/2$. Since $f_1^+(\frac{p+l}{2}) = \frac{p+l}{2}q$ we have to show that

$$\frac{p+l}{2}q \le \frac{k_1^+}{r_1}, \tag{11}$$

Recalling that $\alpha_1^+ = (p+l)q/2$, $k_1^+ = u_1^+ r_1 + t_1^+ pq$, with $t_1^+ = \left[(\alpha_1^+ - u_1^+)r_1/pq\right] + 1$ and $pq < r_1$, it follows by Lemma 5 that the inequality (11) indeed holds true.

Since $f_1^+(m) \ge f_1^+(\dfrac{p+l+2}{2})$ for $\dfrac{p+l+2}{2} \le m \le p-1$, it is enough to check

$$(q-s)p + \frac{p+l+2}{2}q - pq > \frac{k_1^+}{r_1}, \tag{12}$$

in order to verify the correctness of the sixth column in Table 3. In order to establish (12), we will use Lemma 5. We see that (12) follows if $\beta - 1 \ge \alpha_1^+$, where β denotes the left hand side in (12). Now since $\beta - \alpha_1^+ = q - sp \ge 1$ this is obvious. The final column in Table 3 is derived from the previous three, Lemma 2 and Lemma 3. $\square$

Claim B: Assume that $l+2 \le w \le (p-l-4)/2$. Then Table 4 is correct.
Proof of Claim B. The second and third column are taken from Table 2, where we used that $[f_1^+(m+q)]_p = [f_1^+(m)]_p$. To finish the proof we have to show that

- $[f_1^+(m)]_p \le \rho$ and $[f_1^+(m+q)]_q \le \sigma$ for $0 \le m \le (p+l)/2 - w$;
- $[f_1^+(m)]_p \le \rho$ and $[f_1^+(m+q)]_q > \sigma$ for $(p+l+2)/2 - w \le m \le (p+l)/2$;
- $[f_1^+(m)]_p > \rho$ and $[f_1^+(m+q)]_q > \sigma$ for $(p+l+2)/2 \le m \le p-1-w$;
- $[f_1^+(m)]_p > \rho$ and $[f_1^+(m+q)]_q \le \sigma$ for $p-w \le m \le p-1$.

In fact, these inequalities are obviously true, since $w \le (p+l)/2 = \sigma$ and (10) holds. $\square$

`Claim C`: We have $b_{f_1^+(m+q)} = 0$ for $0 \le m \le p-1$.
Proof of Claim C. From Table 4 we infer that $b_{f_1^+(m+q)} = 0$ for $(p+l+2)/2-w \le m \le (p+l)/2$ and $p-w \le m \le p-1$ (since then the p-part and q-part are not in the same range).

- Since $f_1^+(m+q) \ge f_1^+(q)$ for $0 \le m \le \dfrac{p+l}{2} - w$, it suffices to check that
$$(\rho-\tau)p + wq > \frac{k_1^+}{r_1}, \tag{13}$$
in order to verify that $b_{f_1^+(m+q)} = 0$ in this m-range.

- Since $f_1^+(m+q) \ge f_1^+\left(q + \dfrac{p+l+2}{2}\right)$ for $\dfrac{p+l+2}{2} \le m \le p-1-w$, it suffices to check that
$$(q-s)p + \frac{p+l+2}{2}q + wq - pq > \frac{k_1^+}{r_1}, \tag{14}$$
in order to verify that $b_{f_1^+(m+q)} = 0$ in this m-range.

If both (13) and (14) are satisfied, then Claim C follows. By Lemma 5 inequality (13) follows if we can show that $(\rho-\tau)p + wq - \frac{p+l}{2}q \ge 1$. Indeed, using (7), (8) and $w \ge l+2$ (by assumption), we find

$$(\rho-\tau)p + wq - \frac{p+l}{2}q = (w-(l+1))q - p + 1 - \tau p \ge 1 + q - (\tau+1)p \ge 1.$$

That (14) is satisfied is obvious on noting that the left hand side exceeds the left hand side in (12). $\square$

By Kaplan's Lemma, Table 3 and Claim C we now infer that $a_{pqr_1}(k_1^+) = (p+l+2)/2$.

`-The computation of` $a_{pqr_2}(k_2^+)$

Here we assume that $(p+l+4)/2 \le w \le p-l-2$, which ensures that $l+2 \le p-w \le (p-l-4)/2$. Using Lemma 5 one finds that $\alpha_1^+ \le \frac{k_2^+}{r_2} < \beta_2^+$, where

$$\beta_2^+ = \min\{(q-s)p + (p+l+2)q/2 - pq, (\rho-\tau)p + (p-w)q\},\ \alpha_1^+ = (p+l)q/2.$$

TABLE 3

m	$[f_1^+(m)]_p$	$[f_1^+(m)]_q$	$[f_1^+(m)]_p$	$[f_1^+(m)]_q$	$f_1^+(m)$	$b_{f_1^+(m)}$
0	$\rho-\tau$	0	$\leq \rho$	$\leq \sigma$	$\leq k_1^+/r_1$	1
1	$\rho-s-\tau$	1	$\leq \rho$	$\leq \sigma$	$\leq k_1^+/r_1$	1
2	$\rho-2s-\tau$	2	$\leq \rho$	$\leq \sigma$	$\leq k_1^+/r_1$	1
...	...	...	...	...	...	...
$\frac{p+l}{2}$	0	$\frac{p+l}{2}$	$\leq \rho$	$\leq \sigma$	$\leq k_1^+/r_1$	1
$\frac{p+l+2}{2}$	$q-s$	$\frac{p+l+2}{2}$	$> \rho$	$> \sigma$	$> k_1^+/r_1$	0
...	...	...	...	...	...	...
$p-1$	$q-\frac{p-l-2}{2}s$	$p-1$	$> \rho$	$> \sigma$	$> k_1^+/r_1$	0

By Lemma 5 it follows from this that the analogues of (11), (12), (13) and (14) hold, where we replace k_1^+/r_1 by k_2^+/r_2 and w in (13) and (14) by $p-w$.

We will show that

$$\begin{aligned} a_{pqr_2}(k_2^+) &= \sum_{m=0}^{p-1}\left(b_{f_2^+(m)} - b_{f_2^+(m+q)}\right) = \sum_{m=0}^{p-1}\left(b_{f_1^+(p-1-m)} - b_{f_1^+(p-1-m+q)}\right) \\ &= a_{pqr_1}(k_1^+) = \frac{p+l+2}{2}. \end{aligned} \tag{15}$$

Note that $u_2^+ \equiv (p-1)q-(p-l-2)sp/2 \equiv u_1^+ + (p-1)(q-sp) (\bmod pq)$. Using this observation it is easy to see that $f_1^+(m) = f_2^+(p-1-m)$:

$$\begin{aligned} f_1^+(m) &\equiv \frac{k_1^+}{r_1} - \frac{m}{r_1} \equiv u_1^+ + m(q-sp) \equiv u_2^+ + (p-1-m)(sp-q) \\ &\equiv \frac{k_2^+}{r_2} - \frac{p-1-m}{r_2} \equiv f_2^+(p-1-m) (\bmod pq). \end{aligned}$$

Since the analogues of (11) and (12) with k_1^+/r_1 replaced by k_2^+/r_2 hold, we infer that $b_{f_1^+(m)} = b_{f_2^+(p-1-m)}$.

Note that using (4) we get

$$f_2^+(m+q) \equiv f_2^+(m) + q^2\left[-\frac{1}{r_2}\right]_q \equiv f_1^+(p-1-m) + (p-w)q (\bmod pq).$$

By assumption we have $l+2 \leq p-w \leq (p-l-4)/2$. As this is the only condition that we have used in obtaining the inequalities that involve $[f_1^+(m+q)]_q$, we can investigate whether the same bounds for $f_2^+(m+q)$ as for $f_1^+(p-1-m+q)$, where $0 \leq m \leq p-1$, hold. Since as we have remarked (13) and (14) with k_1^+/r_1 replaced by k_2^+/r_2 and w by $p-w$, hold, this is indeed so, and hence we conclude that $b_{f_2^+(m+q)} = b_{f_1^+((p-1-m)+q)}$. Thus we have

$$b_{f_2^+(m)} = b_{f_1^+(p-1-m)},\ b_{f_2^+(m+q)} = b_{f_1^+(p-1-m+q)},\ 0 \leq m \leq p-1,$$

implying (15).

-The computation of $a_{pqr_1}(k_1^-)$

TABLE 4

m	$[f_1^+(m+q)]_p$	$[f_1^+(m)]_q$	$[f_1^+(m)]_p$	$[f_1^+(m+q)]_q$
0	$\rho-\tau$	w	$\leq\rho$	$\leq\sigma$
1	$\rho-\tau-s$	$1+w$	$\leq\rho$	$\leq\sigma$
2	$\rho-\tau-2s$	$2+w$	$\leq\rho$	$\leq\sigma$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
$\frac{p+l}{2}-w$	$\rho-\tau-\left(\frac{p+l}{2}-w\right)s$	$\frac{p+l}{2}$	$\leq\rho$	$\leq\sigma$
$\frac{p+l+2}{2}-w$	$\rho-\tau-\left(\frac{p+l+2}{2}-w\right)s$	$\frac{p+l+2}{2}$	$\leq\rho$	$>\sigma$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
$\frac{p+l}{2}$	0	$\frac{p+l}{2}+w$	$\leq\rho$	$>\sigma$
$\frac{p+l+2}{2}$	$q-s$	$\frac{p+l+2}{2}+w$	$>\rho$	$>\sigma$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
$p-1-w$	$q-\left(\frac{p-l-2}{2}-w\right)s$	$p-1$	$>\rho$	$>\sigma$
$p-w$	$q-\left(\frac{p-l}{2}-w\right)s$	0	$>\rho$	$\leq\sigma$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
$p-1$	$q-\frac{p-l-2}{2}s$	$w-1$	$>\rho$	$\leq\sigma$

Remark. For reasons of space we used the header $[f_1^+(m)]_p(=[f_1^+(m+q)]_p)$.

`Claim D`: Assume that $l+2\leq w<(p-l-4)/2$. Then Tables 5 and 6 are correct. If $w=(p-l-4)/2$ they are also correct, but with the first three rows (starting with $0,1,\dots$) omitted in Table 5.
Proof of Claim D. Note that

$$\frac{k_1^-}{r_1}\equiv\frac{p+l+2}{2}q+\left(\rho+\frac{p-l-2}{2}s\right)p-pq(\text{mod }pq).$$

Since $(p+l+2)/2<p$ and $\rho+(p-l-2)s/2<ps<q$ we have $[f_1^-(0)]_p=(p+l+2)/2$ and $[f_1^-(0)]_q=\rho+(p-l-2)s/2$. This together with $f_1^-(m+q)\equiv f_1^-(m)+wq(\text{mod }pq)$, cf. the derivation of (9), yields the correctness of the first row. From the first row, the remaining ones are easily determined, see the remarks made in the proof of claim A.

Note that

- $[f_1^-(m)]_p>\rho$ and $[f_1^-(m)]_q>\sigma$ for $0\leq m\leq(p-l-4)/2$;
- $[f_1^-(m)]_p\leq\rho$ and $[f_1^-(m)]_q\leq\sigma$ for $(p-l-2)/2\leq m\leq p-1$,

showing the ocrrectness of columns four and five in Table 6.
Subclaim:
1) $f_1^-(m)\leq k_1^-/r_1$ for $0\leq m\leq(p-l-4)/2$;
2) $f_1^-(m)>k_1^-/r_1$ for $(p-l-2)/2\leq m\leq p-1$.
Proof of Subclaim. Recall that $sp<q$.

TABLE 5

m	$[f_1^-(m)]_p$	$[f_1^-(m)]_q$	$[f_1^-(m+q)]_q$
0	$\rho+\frac{p-l-2}{2}s$	$\frac{p+l+2}{2}$	$\frac{p+l+2}{2}+w$
1	$\rho+\frac{p-l-4}{2}s$	$\frac{p+l+4}{2}$	$\frac{p+l+4}{2}+w$
$\dots$	$\dots$	$\dots$	$\dots$
$\frac{p-l-4}{2}-w$	$\rho+(w+1)s$	$p-1-w$	$p-1$
$\frac{p-l-2}{2}-w$	$\rho+ws$	$p-w$	0
$\dots$	$\dots$	$\dots$	$\dots$
$\frac{p-l-4}{2}$	$\rho+s$	$p-1$	$w-1$
$\frac{p-l-2}{2}$	ρ	0	w
$\dots$	$\dots$	$\dots$	$\dots$
$p-w-1$	$\rho-\left(\frac{p+l}{2}-w\right)s$	$\frac{p+l}{2}-w$	$\frac{p+l}{2}$
$p-w$	$\rho-\left(\frac{p+l+2}{2}-w\right)s$	$\frac{p+l+2}{2}-w$	$\frac{p+l+2}{2}$
$\dots$	$\dots$	$\dots$	$\dots$
$p-2$	$\tau+s$	$\frac{p+l-2}{2}$	$\frac{p+l-2}{2}+w$
$p-1$	τ	$\frac{p+l}{2}$	$\frac{p+l}{2}+w$

Remark. If $w=\frac{p-l-4}{2}$ one should delete the first three rows in the table.

- Since $f_1^-(m) \le f_1^-\left(\frac{p-l-4}{2}\right)$ for $0 \le m \le \frac{p-l-4}{2}$, we need to check that

$$(\rho+s)p+(p-1)q-pq=(\rho+s)p-q \le \frac{k_1^-}{r_1}, \tag{16}$$

in order to verify part 1.

- Since $f_1^-(m) \ge f_1^-\left(\frac{p-l-2}{2}\right)$ for $\frac{p-l-2}{2} \le m \le p-1$, we have to check that

$$\rho p > \frac{k_1^-}{r_1}, \tag{17}$$

in order to verify part 2.

Note that the inequality (16) is simply $\alpha_1^- \le k_1^-/r_1$. We need to check that $\alpha_1^- > 0$. Since

$$\alpha_1^- \ge (\rho+1)p-q \ge (p-l-4)q/2 > 0, \tag{18}$$

this is easy. In order to verify (17) we need to show that $\rho p-\alpha_1^- \ge 1$, which is clear since $\rho p-\alpha_1^- = \rho p-(\rho+s)p+q = q-sp \ge 1$. This complets the proof of

TABLE 6

m	$[f_1^-(m)]_p$	$[f_1^-(m)]_q$	$[f_1^-(m)]_p$	$[f_1^-(m)]_q$	$f_1^-(m)$	$b_{f_1^-(m)}$
0	$\rho+\dfrac{p-l-2}{2}s$	$\dfrac{p+l+2}{2}$	$>\rho$	$>\sigma$	$\leq k_1^-/r_1$	-1
1	$\rho+\dfrac{p-l-4}{2}s$	$\dfrac{p+l+4}{2}$	$>\rho$	$>\sigma$	$\leq k_1^-/r_1$	-1
...	...	...	$>\rho$	$>\sigma$	$\leq k_1^-/r_1$	-1
$\dfrac{p-l-4}{2}$	$\rho+s$	$p-1$	$>\rho$	$>\sigma$	$\leq k_1^-/r_1$	-1
$\dfrac{p-l-2}{2}$	ρ	0	$\leq\rho$	$\leq\sigma$	$>k_1^-/r_1$	0
...	...	...	$\leq\rho$	$\leq\sigma$	$>k_1^-/r_1$	0
$p-2$	$\tau+s$	$\dfrac{p+l-2}{2}$	$\leq\rho$	$\leq\sigma$	$>k_1^-/r_1$	0
$p-1$	τ	$\dfrac{p+l}{2}$	$\leq\rho$	$\leq\sigma$	$>k_1^-/r_1$	0

the sublclaim.

Now the final column in Table 6 is deduced from the previous three (by Kaplan's Lemma and Lemma 3). □

Claim E: We have $b_{f_1^-(m+q)}=0$ for $0\leq m\leq p-1$.
Proof of Claim E. We assert that

- $[f_1^-(m)]_p>\rho$ and $[f_1^-(m+q)]_q>\sigma$ for $0\leq m\leq (p-l-4)/2-w$;
- $[f_1^-(m)]_p>\rho$ and $[f_1^-(m+q)]_q\leq\sigma$ for $(p-l-2)/2-w\leq m\leq (p-l-4)/2$;
- $[f_1^-(m)]_p\leq\rho$ and $[f_1^-(m+q)]_q\leq\sigma$ for $(p-l-2)/2\leq m\leq p-1-w$;
- $[f_1^-(m)]_p\leq\rho$ and $[f_1^-(m+q)]_q>\sigma$ for $p-w\leq m\leq p-1$.

In fact, these are obviously true, since $w>0$ and $\tau\leq\rho$. We immediately infer that $b_{f_1^-(m+q)}=0$ for $(p-l-2)/2-w\leq m\leq (p-l-4)/2$ and $p-w\leq m\leq p-1$.

- Since $f_1^-(m+q)\geq f_1^-(q)$ for $0\leq m\leq \dfrac{p-l-4}{2}-w$, we need to check that
$$\left(\rho+\frac{p-l-2}{2}s\right)p+\left(\frac{p+l+2}{2}+w\right)q-pq>\frac{k_1^-}{r_1},\tag{19}$$
in order to show that $b_{f_1^-(m+q)}=0$ in this m-range.

- Since $f_1^-(m+q)\geq f_1^-((p-l-2)/2+q)$ for $\dfrac{p-l-2}{2}\leq m\leq p-w-1$, we need to check that
$$\rho p+wq>\frac{k_1^-}{r_1},\tag{20}$$
in order to show that $b_{f_1^-(m+q)}=0$ in this m-range.

If both (19) and (20) are satisfied, then Claim E follows.

TABLE 7

m	$[f_1^-(m+q)]_p$	$[f_1^-(m+q)]_q$	$[f_1^-(m)]_p$	$[f_1^-(m+q)]_q$
0	$\rho + \frac{p-l-2}{2}s$	$\frac{p+l+2}{2} + w$	$> \rho$	$> \sigma$
1	$\rho + \frac{p-l-4}{2}s$	$\frac{p+l+4}{2} + w$	$> \rho$	$> \sigma$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
$\frac{p-l-4}{2} - w$	$\rho + (w+1)s$	$p-1$	$> \rho$	$> \sigma$
$\frac{p-l-2}{2} - w$	$\rho + ws$	0	$> \rho$	$\leq \sigma$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
$\frac{p-l-4}{2}$	$\rho + s$	$w-1$	$> \rho$	$\leq \sigma$
$\frac{p-l-2}{2}$	ρ	w	$\leq \rho$	$\leq \sigma$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
$p-w-1$	$\rho - \left(\frac{p+l}{2} - w\right)s$	$\frac{p+l}{2}$	$\leq \rho$	$\leq \sigma$
$p-w$	$\rho - \left(\frac{p+l+2}{2} - w\right)s$	$\frac{p+l+2}{2}$	$\leq \rho$	$> \sigma$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
$p-2$	$\tau + s$	$\frac{p+l-2}{2} + w$	$\leq \rho$	$> \sigma$
$p-1$	τ	$\frac{p+l}{2} + w$	$\leq \rho$	$> \sigma$

Remark. For reasons of space we used the header $[f_1^-(m)]_p (= [f_1^-(m+q)]_p)$.

We denote

$$\beta_1^- = \min\{\rho p + \frac{p-l-2}{2}sp + \frac{p+l+2}{2}q + wq - pq, \rho p + wq\}.$$

Thus, in order to check inequalities (19) and (20) it is enough to show that

$$\frac{k_1^-}{r_1} < \beta_1^-.$$

In order to prove this, we will use Lemma 5. Recalling that $k_1^- = u_1^- r_1 + t_1^- pq$, with $t_1^- = \left[(\alpha_1^- - u_1^-)r_1/pq\right] + 1$ and $pq < r_1$, we need to check that $\beta_1^- > \alpha_1^-$. For this we need to show that the following difference is strictly positive:

$$d := \left(\rho + \frac{p-l-2}{2}s\right)p + \frac{p+l+2}{2}q + wq - pq - ((\rho+s)p - q)$$

Using the assumption $w \geq l+2$, we get $d \geq d_1$ with

$$2d_1 = (p-l-4)sp + (3l+8-p)q.$$

Then, by first substituting $sp/2 = (\rho p - \tau p)/(p+l)$, then using the inequality

$q \geq (\tau+1)p$ and finally using (18), we obtain:

$$\begin{aligned} d_1 &= \frac{p-l-4}{p+l}((\rho+1)p-(\tau+1)p)+\frac{(3l+8)q-pq}{2} \\ &> \frac{p-l-4}{p+l}((\rho+1)p-q)+\frac{(3l+8)q-pq}{2}. \\ &> \frac{p-l-4}{2(p+l)}(p-l-4)q+\frac{(3l+8)q-pq}{2}. \end{aligned}$$

Thus it suffices to show that

$$d_2 := \frac{(p-l-4)^2}{p+l}+3l+8-p>0.$$

Simplifying the above expression gives

$$d_2 = \frac{3l^2+8l+16}{p+l}>0.$$

Thus the conditions of Lemma 5 are satisfied and hence $0<\alpha_1^- \leq \frac{k_1^-}{r_1}<\beta_1^-$ and claim E is established. $\square$

By Kaplan's Lemma, Table 6 and Claim E we now infer that

$$a_{pqr_1}(k_1^-) = -\frac{p-l-2}{2}. \tag{21}$$

-`The computation of` $a_{pqr_2}(k_2^-)$

We claim that $b_{f_2^-(m)} = b_{f_1^-(p-1-m)}$ and $b_{f_2^-(m+q)} = b_{f_1^-(p-1-m+q)}$. This, using (21) then yields $a_{pqr_2}(k_2^-) = a_{pqr_1}(k_1^-) = -(p-l-2)/2$, as required.

First, note that

$$\frac{k_2^-}{r_2} \equiv u_2^- \equiv \frac{p+l}{2}q+\tau p \equiv u_1^- + (p-1)(q-sp) (\text{mod } pq).$$

Using this observation, it is easy to see that $f_2^-(m) = f_1^-(p-1-m_2)$:

$$\begin{aligned} f_2^-(m) &\equiv \frac{k_2^- - m}{r_2} \equiv u_2^- + m(sp-q) \\ &\equiv u_1^- + (p-1)(q-sp)+m(sp-q) \\ &\equiv u_1^- + (q-sp)(p-1-m) \\ &\equiv \frac{k_1^- - (p-1-m)}{r_1} \equiv f_1^-(p-1-m) (\text{mod } pq). \end{aligned}$$

In order to have $b_{f_2^-(m)} = b_{f_1^-(p-1-m)}$, we must have the same inequalities for $f_1^-(p-1-m)$ as for $f_2^-(m)$.

Similarly, $f_2^-(m+q) \equiv f_1^-(p-1-m)+(p-w)q$ (mod pq). We want to have $b_{f_2^-(m+q)} = b_{f_1^-(p-1-m+q)}$. The assumption we have made on w ensures that $l+2 \leq p-w \leq (p-l-4)/2$. As this is the only condition that we have used in obtaining the inequalities that involve $[f_1^-(m+q)]_q$, we can ask for exactly the same bounds for $f_2^-(m+q)$ as for $f_1^-(p-1-m+q)$, where $0 \le m \le p-1$.

Using Lemma 5 one checks that the analogues of (16), (17), (19) and (20) with k_1^-/r_1 replaced by k_2^-/r_2 and w by $p-w$, hold true. Hence we deduce that $b_{f_2^-(m)} = b_{f_1^-(p-1-m)}$ and $b_{f_2^-(m+q)} = b_{f_1^-(p-1-m+q)}$.

Thus we have finished the computation of $a_{pqr_1}(k_1^+)$, $a_{pqr_1}(k_2^+)$, $a_{pqr_2}(k_1^-)$ and $a_{pqr_1}(k_2^-)$. Since the difference of the largest coefficient and the smallest coefficient in $\Phi_{pqr}(x)$ is at most p, cf. [2], we infer that

$$\max A\{pqr_j\} = a_{pqr_j}(k_j^+), \ \ \min A\{pqr_j\} = a_{pqr_j}(k_j^-).$$

By the jump one property, cf. [8], we have $|a_{pqr}(k) - a_{pqr}(k+1)| \le 1$ and hence we infer that $A\{pqr_j\} = \{a_{pqr_j}(k_j^-), \ldots, a_{pqr_j}(k_j^+)\}$, as asserted. We have $M(p;q) \ge a_{pqr_j}(k_j^+) = (p+l+2)/2$. Recall that $q \equiv \frac{2}{l+2} \equiv w(\text{mod } p)$. We let $1 \le w^* \le p-1$ be the inverse of w modulo p. Note that $w^* = (p+l+2)/2$. We have $p/2 < w^* < 3p/4$. By Lemma 3 of [9] it then follows that $M(p;q) \le w^* = (p+l+2)/2$ and hence $M(p;q) = (p+l+2)/2$. Since $p \ge 3l+8$, it follows that $(p+l+2)/2 < 2p/3$. □

`Remark`. The upper bound on $M(p;q)$ can also be proved by directly invoking the main result of B. Bzdęga [5].

4 Implications for the study of $M(p;q)$ and $M(p)$

Various papers in the literature study $M(p)$ and therefore it is perhaps natural to refine this to the study of $M(p;q)$, as was first done by Gallot, Moree and Wilms [10], see the MPIM-report [9] for the full version. So far no algorithm is known to compute $M(p)$, whereas computing $M(p;q)$ is easy.

Gallot, Moree and Wilms [10] raise various questions, one of them (by Wilms), being:

Question 1 *Given an integer $k \ge 1$, does there exist $p_0(k)$ and a function $q_k(p)$ such that if $q \equiv 2/(2k+1)(\text{mod } p)$, $q \ge q_k(p)$ and $p \ge p_0(k)$, then $M(p;q) = (p+2k+1)/2$?*

Combining Theorem 2 with Lemma 4 gives a positive answer to this question (with $l = 2k-1$, $p_0(k) = 4k^2+2k+3$ and $q_k(p) = (p+2k-1)p/2$).

Theorem 3 *Let $l \ge 1$ be an odd integer and $p \ge l^2+3l+5$ a prime. Let $q \ge (p+l)p/2$ be a prime satisfying $q \equiv 2/(l+2)(\text{mod } p)$. Then $M(p;q) = (p+l+2)/2$, where $M(p;q) = \max\{A(pqr) : r > q\}$, where r runs over all primes exceeding q.*

Given a prime p and a progression $a(\text{mod } p)$ with $p \nmid a$, there are various results that ensure that $M(p;q)$ assumes the same value, say v, for all primes $q \equiv a(\text{mod } p)$ large enough. In this case we write $m_p(a) = v$. Given an $1 \le \beta \le p$ we let β^* be the unique integer $1 \le \beta^* \le p-1$ with $\beta\beta^* \equiv 1(\text{mod } p)$.

Put

$$\mathcal{B}_1(p) = \{\beta : \ 1 \le \beta \le (p-3)/2, \ \beta + \beta^* \ge p, \ \beta^* \le 2\beta\},$$

$$\mathcal{B}_2(p) = \{\beta : \ 1 \le \beta \le (p-3)/2, \ p \le \beta + 2\beta^* + 1, \ \beta > \beta^*\},$$

$$\mathcal{B}_3(p) = \{\beta : \ 1 \le \beta \le (p-3)/2, \ p \le 2\beta + \beta^*, \ \beta \ge \beta^*\}.$$

$$\mathcal{B}_{GM}(p) := \mathcal{B}_1(p) \cup \mathcal{B}_2(p), \ \mathcal{B}_R(p) := \mathcal{B}_1(p) \cup \mathcal{B}_3(p).$$

Note that $\mathcal{B}_2(p) \subseteq \mathcal{B}_3(p)$ and hence $\mathcal{B}_{CM}(p) \subseteq \mathcal{B}_R(p)$. Furthermore, we have $\mathcal{B}_1(p) \cap \mathcal{B}_3(p) = \emptyset$. Using Kloosterman sums and Weil's estimate, Cobeli [6] can estimate the cardinality of these sets:

$$\left|\#\mathcal{B}_{GM}(p) - \frac{p}{16}\right| \le 104p^{3/4}\log p\,, \quad \left|\#\mathcal{B}_R(p) - \frac{p}{12}\right| \le 104p^{3/4}\log p. \qquad (22)$$

The idea is that if say in the definition of $\mathcal{B}_1(p)$ we replace β by x and β^* by y and x and y are real numbers, we get a triangle Δ_1. It is seen to have area asymptotic to $p^2/24$. Likewise, the triangles associated to $\mathcal{B}_2(p)$ and $\mathcal{B}_3(p)$ have asymptotically area $p^2/48$, respectively $p^2/24$. Assuming now that the inverses are uniformly distributed we expect asymptotically (as p tends to infinity) area$(\Delta)/p$ points (β, β^*) inside the triangle Δ. This indeed can be proved. Since $\Delta_1 \cap \Delta_2 = \emptyset$ and $\Delta_1 \cap \Delta_3 = \emptyset$, we then arrive at the main terms $p/16(= p/24 + p/48)$ and $p/12 = (p/24 + p/24)$ in (22) above.

The earlier large coefficient construction and the one presented in this paper can be formulated on the same footing (as was pointed out to us by Yves Gallot).

Proposition 1
1) (Gallot and Moree). *Let $\beta \in \mathcal{B}_{GM}(p)$. Then $m_p(\beta) \ge p - \beta$.*
If $\beta \in \mathcal{B}_1(p)$ and $p = \beta + \beta^*$, then $m_p(\beta) = p - \beta$.
2) (Rosu). *Let $\beta \in \mathcal{B}_R(p)$. Then $m_p(p - \beta^*) = p - \beta$.*

Proof. 1) This is merely a consequence of the main theorem of Gallot and Moree [7].
2) We use the notation of Theorem 2, Write $\beta = (p - l - 2)/2$. Note that $\beta^* = p - w$. The inclusion $w \in [l + 2, (p - l - 2)/2] \cup [(p + l + 2)/2, p - l - 2]$ is seen to be equivalent with $\beta \in \mathcal{B}_R(p)$. Now invoke Theorem 2. □

Let $S_i(p)$ be the set of $1 \le v \le p$ for which part i of the latter proposition applies and yields an identity or lower bound for $m_p(v)$ (thus $S_1(p) = \mathcal{B}_{GM}(p)$ and $S_2(p) = \{p - \beta^* \ : \ \beta \in \mathcal{B}_R(p)\}$). A natural question that arises is to determine the intersection $S_1(p) \cap S_2(p)$. Proposition 3 gives the answer, its proof depends on the next proposition.

Proposition 2 *Suppose that $\beta_1 = p - \beta_2^*$ and $\beta_1, \beta_2 \in \mathcal{B}_R(p)$. Then $\beta_1, \beta_2 \in \mathcal{B}_1(p)$ and $\beta_1 = \beta_2$.*

Proof.
-First case: $\beta_1, \beta_2 \in \mathcal{B}_1(p)$.
The assumption $\beta_1 = p - \beta_2^*$ implies that $\beta_1^* = p - \beta_2$ and hence $\beta_1 + \beta_1^* = 2p - \beta_2 - \beta_2^*$. Since $\beta_i + \beta_i^* \ge p$, we infer that $\beta_i + \beta_i^* = p$. This together with $\beta_1 = p - \beta_2^*$ yields $\beta_1 = \beta_2$.
-Second case: $\beta_1 \in \mathcal{B}_1(p)$, $\beta_2 \in \mathcal{B}_3(p)$.
From $\beta_1 \in \mathcal{B}_1(p)$ and $\beta_1 = p - \beta_2^*$ we infer that $\beta_1 \ge \beta_1^*$. Now $p \le \beta_1 + \beta_1^* \le 2\beta_1$,

contradicting $\beta_1 \leq (p-3)/2$.
-Third case: $\beta_1 \in \mathcal{B}_3(p)$, $\beta_2 \in \mathcal{B}_1(p)$.
We have $\beta_i \leq (p-3)/2$ and hence $\beta_1 + \beta_2 \leq p-3$. The assumption $\beta_1 = p - \beta_2^*$ implies that $\beta_1^* = p - \beta_2$. Since $\beta_1 \in \mathcal{B}_3(p)$ we have $\beta_1^* \leq \beta_1$ and hence $p - \beta_2 = \beta_1^* \leq \beta_1$ and so $p \leq \beta_1 + \beta_2$. Contradiction.
-Fourth case: $\beta_1, \beta_2 \in \mathcal{B}_3(p)$.
We have $\beta_i \leq (p-3)/2$ and hence $\beta_1 + \beta_2 \leq p-3$. Since $\beta_2 \in \mathcal{B}_3(p)$, we have $\beta_2^* \leq \beta_2$ and thus from $\beta_1 = p - \beta_2^*$ we infer that $p = \beta_1 + \beta_2^* \leq \beta_1 + \beta_2$. Contradiction. □

Proposition 3 *Let $\mathcal{P}_1$ be the set of primes $p \equiv 1 (\bmod\ 4)$ such that the smallest solution, $x_0(p)$, of $x^2 + 1 \equiv 0 (\bmod\ p)$ satisfies $p/3 \leq x_0(p) \leq (p-3)/2$. We have*

$$S_1(p) \cap S_2(p) = \begin{cases} \emptyset & \text{if } p \notin \mathcal{P}_1; \\ \{x_0(p)\} & \text{otherwise.} \end{cases}$$

If $p \in \mathcal{P}_1$, then both parts of Proposition 1 yield $m_p(x_0(p)) = p - x_0(p)$.

Proof. By Proposition 3 we have

$$S_1(p) \cap S_2(p) = \{\beta \ :\ 1 \leq \beta \leq (p-3)/2,\ \beta + \beta^* = p,\ \beta^* \leq 2\beta\}.$$

The rest of the proof is left to the reader. □

This result together with Cobeli's estimate and Dirichlet's theorem for arithmetic progressions, shows that as p tends to infinity, there is a set of primes Q of density $\geq 7/48$ such that $M(p;q) > (p+1)/2$. Thus counter-examples to the Sister Beiter conjecture arise rather frequently.

Gallot et al. [10] give conjectural values for $m_p(a)$ for $13 \leq p \leq 23$. Some of these can be shown to be true by Proposition 1, which gives $m_{13}(5) = 8$, $m_{17}(12) = 10$, $m_{19}(7) = 11$, $m_{23}(16) = 13$ and $m_{23}(5) = 14$. Of these only the first is not new, as $S_1(13) \cap S_2(13) = \{5\}$ and so also part 1 of Proposition 1 yields $m_{13}(5) = 8$.

Definition 2 *Put $M_{GM}(p) = p - \min\{\mathcal{B}_{GM}(p)\}, M_R(p) = p - \min\{\mathcal{B}_R(p)\}$.*

Since $\mathcal{B}_2(p) \subseteq \mathcal{B}_3(p)$, we have

$$M(p) \geq M_R(p) \geq M_{GM}(p).$$

If $M_R(p) > M_{GM}(p)$, then the construction presented in this paper yields a better lower bound for $M(p)$ than that established earlier by Gallot and Moree [7]. The primes $p < 400$ with $M_R(p) > M_{GM}(p)$ are precisely: 29, 37, 41, 83, 107, 109, 149, 179, 181, 223, 227, 233, 241, 269, 281, 317, 347, 367, 379, 383, 389.

Question 2 *Are there infinitely many primes p such that $M_R(p) > M_{GM}(p)$? If yes, give an estimate for the number of such primes $\leq x$.*

Numerically it seems that with increasing p occasionally larger and larger differences $M_R(p) - M_{GM}(p)$ occur.

Question 3 *Is it true that* $\limsup\ (M_R(p) - M_{GM}(p)) = \infty$*?*

5 Acknowledgement

Rosu would like to thank Pieter Moree at the Max Planck Institute for Mathematics in Bonn for suggesting the problem and for the great help and feedback he offered here during her two month-internship (summer 2010) at the MPIM Bonn.

Moree likes to point out that Rosu was unaware of the question by Wilms' and that it hence came as a present surprise that her construction as a by-product led to an answer of this question.

The construction was found by paper and pencil work only and later underwent numerical checks by Yves Gallot. Furthermore, Gallot made many interesting remarks, in particular he introduced the set $\mathcal{B}_R(p)$. Merci beaucoup, Yves!

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, On ternary inclusion-exclusion polynomials, *Integers 10* (2010), A48, 623-638.

[4] M. Beiter, Magnitude of the coefficients of the cyclotomic polynomial $F_{pqr}(x)$, *Amer. Math. Monthly* **75** (1968), 370–372.

[5] B. Bzdęga, Bounds on ternary cyclotomic coefficients, *Acta Arith.* **144** (2010), 5–16.

[6] C. Cobeli, unpublished manuscript, updated version, 2011.

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

[8] Y. Gallot and P. Moree, Neighboring ternary cyclotomic coefficients differ by at most one, *J. Ramanujan Math. Soc.* **24** (2009), 235–248.

[9] Y. Gallot, P. Moree and R. Wilms, The family of ternary cyclotomic polynomials with one free prime, MPIM-preprint 2010-11, pp. 32.

[10] Y. Gallot, P. Moree and R. Wilms, The family of ternary cyclotomic polynomials with one free prime, *Involve*, to appear, http://front.math.ucdavis.edu/1110.4590.

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

[12] T.Y. Lam and K.H. Leung, On the cyclotomic polynomial $\Phi_{pq}(X)$, *Amer. Math. Monthly* **103** (1996), 562–564.

[13] S. Rosset, The coefficients of cyclotomic like polynomials of order 3, unpublished manuscript (2008) pp. 5.

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

Department of Mathematics, Evans Hall,
UC Berkeley, Berkeley CA 94720-3840, USA.
e-mail: rosu@math.berkeley.edu