Neighboring ternary cyclotomic coefficients differ by at most one

Yves Gallot and Pieter Moree

Abstract

A cyclotomic polynomial $\Phi_n(x)$ is said to be ternary if $n = pqr$ with p, q and r distinct odd prime factors. Ternary cyclotomic polynomials are the simplest ones for which the behaviour of the coefficients is not completely understood. Eli Leher showed in 2007 that neighboring ternary cyclotomic coefficients differ by at most four. We show that, in fact, they differ by at most one. Consequently, the set of coefficients occurring in a ternary cyclotomic polynomial consists of consecutive integers.

As an application we reprove in a simpler way a result of Bachman from 2004 on ternary cyclotomic polynomials with an optimally large set of coefficients.

1 Introduction

The nth cyclotomic polynomial $\Phi_n(x)$ is defined by

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

with ζ_n a nth primitive root of unity (one can take $\zeta_n = e^{2\pi i/n}$). It has degree $\varphi(n)$, with φ Euler's totient function. We write

$$f(x) = \sum_{k=0}^{\infty} c_k x^k = \sum_{k=0}^{\deg(f)} c_k x^k,$$

and put $\mathcal{C}(f) = \{c_k : 0 \le k \le \deg(f)\}$ and $\mathcal{C}_0(f) = \{c_k : k \ge 0\}$. Note that $\mathcal{C}_0(f) = \mathcal{C}(f) \cup \{0\}$. For notational convenience we will write $\mathcal{C}(n)$ instead of $\mathcal{C}(\Phi_n)$ and $\mathcal{C}_0(n)$ instead of $\mathcal{C}_0(\Phi_n)$.

Definition 1 *If $\mathcal{C}_0(n) \subseteq \{-1, 0, 1\}$, then Φ_n is said to be flat.*

Mathematics Subject Classification (2000). 11T22, 11B83

In the 19th century it was noted that Φ_n has a strong tendency to be flat and this intrigued various mathematicians enough to study the coefficients of Φ_n more intensively. For some recent contributions see e.g. Bachman [3] and Kaplan [8].

Using Lemma 2 below it is not difficult to establish the classical fact that if Φ_n is not flat, then n has at least three distinct odd prime factors. The simplest case arises when $n = pqr$ with $2 < p < q < r$ odd primes. In this case n is said to be ternary and Φ_n is said to be a ternary cyclotomic polynomial. Given Φ_{pqr} one of the basic problems is to determine the maximum (in absolute value) of its coefficients. Put $M(p) = \max\{|m| : m \in \mathcal{C}(n),\ n = pqr,\ p < q < r \text{ primes }\}$. Here it is known [1] that $M(p) \leq 3p/4$. In 1968 it was conjectured by Sister Marion Beiter [4] (see also [5]) that $M(p) \leq (p+1)/2$. She proved it for $p \leq 5$. The first to show that Beiter's conjecture is false seems to have been Eli Leher [10, p. 70], who gave the counter-example $a_{17\cdot 29\cdot 41}(4801) = -10$, showing that $M(17) \geq 10 > 9 = (17+1)/2$. The present authors [7] provided infinitely many counter-examples for the case $p = 17$ and in fact for every $p \geq 11$. Moreover, they have shown that for every $\epsilon > 0$ and p sufficiently large $M(p) > (\frac{2}{3} - \epsilon)p$. Thus only for $p = 7$ the Beiter conjecture remains open.

In his PhD thesis on numerical semigroups Leher shows that in case n is ternary one has $|a_n(k) - a_n(k-1)| \leq 4$ ([10, Theorem 57]) and remarks that he does not know whether this bound is sharp. Here we show that it is not.

Theorem 1 *Let n be ternary, that is $n = pqr$ with $2 < p < q < r$ odd primes. Then, for $k \geq 1$, $|a_n(k) - a_n(k-1)| \leq 1$.*

Corollary 1 *If n is ternary, then $\mathcal{C}(n) = \{a, a+1, \ldots, b-1, b\}$ with a and b integers, that is $\mathcal{C}(n)$ consists of a range of consecutive integers.*

For convenience we will say that $f \in \mathbb{Z}[x]$ has the *jump one* property if neighboring coefficients differ by at most one. Thus Theorem 1 says that a ternary Φ_n has the jump one property. If $\mathcal{C}_0(n)$ consists of a range of consecutive integers, we say Φ_n is *coefficient convex*. Thus Corollary 1 says that a ternary Φ_n is coefficient convex. Notice that if Φ_n is flat, then Φ_n is coefficient convex. In Section 6 we consider the problem of determining those n for which Φ_n is coefficient convex.

Leher uses ideas from the theory of semigroups to prove his result. In Section 2 we discuss the connection between numerical semigroups and cyclotomic polynomials, for further details we refer to Leher's PhD thesis.

In Section 4 we prove Theorem 1. The proof does not use any semigroup ideas, but rests on a recent lemma of Kaplan that is discussed in Section 2, along with some examples.

In Section 5 we show how our main result makes detecting so-called optimal ternary cyclotomic polynomials easier and demonstrate this by giving a reproof of the main result in Bachman [2]. The proof crucially rests on the examples considered in Section 3.1.

For a nice survey of basic properties of cyclotomic coefficients we refer to Thangadurai [14].

2 Binary cyclotomic polynomials and numerical semigroups

A number m is said to be a *natural combination* of the integers $a_1, \ldots, a_m$ if there are non-zero integers $k_1, \ldots, k_m$ such that $n = k_1a_1 + \cdots + k_ma_m$. Let $A = \{a_1, \ldots, a_m\}$ be a set of natural numbers and $S = S(A) = S(a_1, \ldots, a_m)$ be the set of all natural combinations of the a_i's. Then S is a *semigroup* (that is, it is closed under addition). The semigroup S is *numerical* if its complement $\mathbb{Z}_{\geq 0}\backslash S$ is finite. If S is numerical, then $\max\{\mathbb{Z}_{\geq 0}\backslash S\} = F(S)$ is the *Frobenius number* of S. It is not difficult to prove that $S(a_1, \ldots, a_m)$ is numerical iff $a_1, \ldots, a_m$ are relatively prime. The *Hilbert series* of the numerical semigroup S is the formal power series $H_G(x) = \sum_{s\in S} x^s \in \mathbb{Z}[[x]]$. For a numerical semigroup S, $(1-x)H_S(x)$ is a polynomial of degree $F(S)+1$. Leher writes $P_S(x) = (1-x)H_S(x)$ and calls $P_S(x)$ the *semigroup polynomial.* It can be shown that $P_{S(p,q)}(x) = \Phi_{pq}(x)$. This leads to the following interpretation of the coefficients $a_{pq}(k)$:

$$a_{pq}(k) = \begin{cases} 1 & \text{if } k \in S(p,q),\ k-1 \notin S(p,q); \\ -1 & \text{if } k \notin S(p,q),\ k-1 \in S(p,q); \\ 0 & \text{otherwise.} \end{cases}$$

Lemma 2 below gives an explicit evaluation of the binary coefficients $a_{pq}(k)$. Leher [10, Theorem 50] shows that an analogous evaluation holds for the coefficients of $P_{S(p,q)}(x)$ in case p and q are relatively prime positive integers exceeding one.

The above material leads to some natural questions. For which numerical semigroups S do we have that $\sum_{x\in S} x^s$ divides $x^m - 1$ for some m ? Another question is to determine all integers n for which

$$(1-x)\sum_{s\in S_n} x^s = \Phi_n(x), \tag{1}$$

for some set of integers S_n.

3 Kaplan's lemma reconsidered

Our main tool will be the following recent result due to Kaplan [8], 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 1 (Nathan Kaplan, 2007). *Let $2 < p < q < r$ be primes and $k \geq 0$ be an integer. Put*

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

We have

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

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

This lemma 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 [9] or Thangadurai [14].

Lemma 2 *Let $p < q$ be odd primes. Let ρ and σ be the (unique) non-negative integers for which $1 + pq = (\rho + 1)p + (\sigma + 1)q$. Let $0 \le m < pq$. Then either $m = \alpha_1 p + \beta_1 q$ or $m = \alpha_1 p + \beta_1 q - pq$ with $0 \le \alpha_1 \le q - 1$ the unique integer such that $\alpha_1 p \equiv m (\mathrm{mod}\ q)$ and $0 \le \beta_1 \le p - 1$ the unique integer such that $\beta_1 q \equiv m (\mathrm{mod}\ p)$. The cyclotomic coefficient $a_{pq}(m)$ equals*

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

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 is not necessary to compute $f(m)$ and $f(m + q)$ (as we did in [7]), it suffices to compute $[f(m)]_p$, $[f(m)]_q$, $[f(m + q)]_p$ and $[f(m + q)]_q$ (which is easier). Indeed, as $[f(m)]_p = [f(m + q)]_p$, it suffices to compute $[f(m)]_p$, $[f(m)]_q$, and $[f(m + q)]_q$.

For future reference we provide a version of Kaplan's lemma in which the computation of b_i has been made explicit, and thus is selfcontained.

Lemma 3 *Let $2 < p < q < r$ be primes and $k \ge 0$ be an integer. We put $\rho = [(p - 1)(q - 1)]_p$ and $\sigma = [(p - 1)(q - 1)]_q$. Furthermore, we put*

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

We have

$$a_{pqr}(k) = \sum_{m=0}^{p-1} (b_{f(m)} - b_{f(m+q)}), \tag{3}$$

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

Note that if i and j have the same p-part, then $b_i b_j \ne -1$, that is b_i and b_j cannot be of opposite sign. From this it follows that $|b_{f(m)} - b_{f(m+q)}| \le 1$, and thus we infer from Kaplan's lemma that $|a_{pqr}(k)| \le p$. It is possbile to improve on this argument and get a sharper bound for $|a_{pqr}(k)|$. We hope to return to this issue in a future paper. Of course if i and j have the same q-part, then $b_i b_j \ne -1$ also.

3.1 Examples of computing coefficients with Kaplan's lemma

In this section we carry out a sample computation using Kaplan's lemma. For more involved examples the reader is referred to [7].

We remark that the result that $a_n(k) = (p+1)/2$ in Lemma 4 is due to Herbert Möller [12]. The reproof we give is rather different. The foundation for Möller's result is due to Emma Lehmer [11], who already in 1936 had shown that $a_n(\frac{1}{2}(p-3)(qr+1)) = (p-1)/2$ with p, q, r and n satisfying the conditions of Lemma 4.

Lemma 4 *Let $p < q < r$ be primes satisfying*

$$p > 3,\ q \equiv 2(\text{mod } p),\ r \equiv \frac{p-1}{2}(\text{mod } p),\ r \equiv \frac{q-1}{2}(\text{mod } q).$$

Put $n = pqr$ and $k = (p-1)(qr+1)/2$. Then $a_n(k-r) = -(p-1)/2$ and $a_n(k) = (p+1)/2$.

Proof. First it will be shown that $a_n(k) = (p+1)/2$. Using that $q \equiv 2(\text{mod } p)$, we infer from $1 + pq = (\rho+1)p + (\sigma+1)q$ that $\sigma = \frac{p-1}{2}$ and $(\rho+1)p = 1 + (\frac{p-1}{2})q$ (and hence $\rho = (p-1)(q-2)/(2p)$). On invoking the Chinese remainder theorem on checks that

$$-\frac{1}{r} \equiv 2 \equiv -(\frac{q-2}{p})p + q(\text{mod } pq). \tag{4}$$

Furthermore, writing $f(0)$ as a linear combination of p and q we see that

$$f(0) \equiv \frac{k}{r} \equiv (\frac{p-1}{2})q + \frac{p-1}{2r} \equiv (\frac{p-1}{2})q + 1 - p \equiv \rho p(\text{mod } pq). \tag{5}$$

From (4) and (5) we infer that, for $0 \le m \le (p-1)/2$, we have $[f(m)]_p = \rho - m(q-2)/p \le \rho$ and $[f(m)]_q = m \le \sigma$. On noting that $[f(m)]_p p + [f(m)]_q q = \rho p + 2m \le \rho p + p - 1 = [k/r]$, we infer that $a_{pq}(f(m)) = b_{f(m)} = 1$ in this range (see also Table 1).

TABLE 1

m	$[f(m)]_p$	$[f(m)]_q$	$f(m)$	$a_{pq}(f(m))$	$b_{f(m)}$
0	ρ	0	ρp	1	1
1	$\rho-(q-2)/p$	1	$\rho p+2$	1	1
$\ldots$	$\ldots$	$\ldots$	$\ldots$	1	1
j	$\rho - j(q-2)/p$	j	$\rho p + 2j$	1	1
$\ldots$	$\ldots$	$\ldots$	$\ldots$	1	1
$(p-1)/2$	0	$(p-1)/2$	$(p-1)q/2$	1	1

Note that $f(m) \equiv f(0) - m/r \equiv \rho p + 2m(\text{mod } pq)$, from which one easily infers that $f(m) = \rho p + 2m$ for $0 \le m \le p-1$ (as $\rho p + 2m \le \rho p + 2(p-1) < pq$). In the range $\frac{p+1}{2} \le m \le p-1$ we have $f(m) \ge \rho p + p + 1 = (p-1)q/2 + 2 > k/r$, and hence $b_{f(m)} = 0$.

On noting that $f(m+q) \equiv f(m) - q/r \equiv f(m) + 2q \equiv \rho p + 2m + 2q(\text{mod } pq)$, one easily finds, for $0 \le m \le p-1$, that $f(m+q) = \rho p + 2m + 2q > k/r$ and hence $b_{f(m+q)} = 0$.

By Kaplan's lemma one infers that

$$a_n(k) = \sum_{m=0}^{p-1} (b_{f(m)} - b_{f(m+q)}) = \sum_{m=0}^{(p-1)/2} 1 = \frac{p+1}{2}.$$

Next we show that $a_n(k-r) = -(p-1)/2$. Put $k' = k-r$ and $f_1(m) \equiv r^{-1}(k-r-m) (\mathrm{mod}\ pq)$ with $0 \le f_1(m) < pq$. Furthermore we put $b''_{f_1(m)} = a_{pq}(f_1(m))$ if $f_1(m) \le k'/r$ and zero otherwise. By (5) we deduce that

$$f_1(0) \equiv f(0) - 1 \equiv (q-1)p + (\frac{p-1}{2})q (\mathrm{mod}\ pq).$$

An easy calculation yields the correctness of Table 2.

TABLE 2

m	$[f_1(m)]_p$	$[f_1(m)]_q$	$f_1(m)$	$b''_{f_1(m)}$
0	$q-1$	$(p-1)/2$	$(p-1)q/2 - p$	0
1	$q-1-(q-2)/p$	$(p+1)/2$	$(p-1)q/2 - p + 2$	-1
$\ldots$	$\ldots$	$\ldots$	$\ldots$	-1
j	$q-1-j(q-2)/p$	$(p-1)/2 + j$	$(p-1)q/2 - p + 2j$	-1
$\ldots$	$\ldots$	$\ldots$	$\ldots$	-1
$(p-1)/2$	$q-1-\rho$	$p-1$	$(p-1)q/2 - 1$	-1
$(p+1)/2$	$q-1-\rho-(q-2)/p$	0	$(p-1)q/2 + 1$	0

For $(p+1)/2 \le m \le p-1$ one finds that $f_1(m) > k'/r$ and hence $b''_{f_1(m)} = 0$. On noting that, for $0 \le m \le p-1$, $f_1(m+q) = (\frac{p-1}{2})q - p + 2m + 2q > k'/r$, we find that $b''_{f_1(m+q)} = 0$ in this range. Kaplan's lemma now gives

$$a_n(k-r) = \sum_{m=0}^{p-1} (b''_{f_1(m)} - b''_{f_1(m+q)}) = -\sum_{m=1}^{(p-1)/2} 1 = -\frac{(p-1)}{2},$$

completing the proof. $\square$

We recall from [7] the following result, which is implicit in Kaplan's paper [8].

Lemma 5 *Let $2 < p < q < r$ be primes and $n \ge 0$ be an integer. Suppose that $a_{pqr}(n) = m$. Write $n = [\frac{n}{r}]r + n_0$ with $0 \le n_0 < r$. Let $t > pq$ be a prime satisfying $t \equiv -r (\mathrm{mod}\ pq)$. Let $0 \le n_1 < pq$ be the unique integer such that $n_1 \equiv q + p - 1 - n_0 (\mathrm{mod}\ pq)$. Then*

$$a_{pqt}\Big(\Big[\frac{n}{r}\Big]t + n_1\Big) = -m.$$

Using the latter lemma one immediately gets from Lemma 4 the following one, however with the condition $r_1 > q$ replaced by $r_1 > pq$. On proceeding as in the proof of Lemma 4, one gets the feeling of déjà vu. Indeed, it turns out that on running through $m = 0, \ldots, p-1$, $m = q, q+1, \ldots, q+p-1$, the $f(m)$ in the setup of Lemma 4 correspond to the $f(m)$ for $q + p - 1 - m$ in the setup of Lemma 6, the effect being that the corresponding ternary coefficients differ by a minus sign. On doing this it turns out that the condition $r_1 > pq$ can be relaxed to the condition $r_1 > q$.

Lemma 6 *Let $p < q < r$ be primes satisfying*

$$p > 3,\ q \equiv 2 (\text{mod } p),\ r_1 \equiv \frac{p+1}{2} (\text{mod } p),\ r_1 \equiv \frac{q+1}{2} (\text{mod } q).$$

Put $n_1 = pqr_1$ and $k_1 = (p-1)(qr_1+1)/2 + q$. Then $a_{n_1}(k_1 - r_1) = (p-1)/2$ and $a_{n_1}(k_1) = -(p+1)/2$.

`Remark`. Note that, in Lemma 4, $r = (lpq-1)/2$ for some odd $l \geq 1$ and that $r_1 = (l_1pq+1)/2$ for some odd $l_1 \geq 1$.

4 Proof of the jump one property

Having Kaplan's lemma at our disposal we are ready to give a proof of the jump one property.

Proof of Theorem 1. Let $f'(m)$ be the unique integer $0 \leq f'(m) < pq$ such that $f'(m) \equiv r^{-1}(k-1-m)(\text{mod } pq)$. Let b_i' be defined as b_i, but with k replaced by $k-1$. Note that

$$b_i - b_i' = \begin{cases} b_{\frac{k}{r}} & \text{if } r|k \text{ and } i = \frac{k}{r}; \\ 0 & \text{otherwise.} \end{cases} \tag{6}$$

If $r|k$, then $f(0) = k/r$. For $j = 0, \ldots, p-2$ we have $f'(j) = f(j+1)$ and since $f(j+1) \neq f(0)$, we infer using (6) that

$$\gamma_1 := \sum_{j=0}^{p-1} \left(b_{f(j)} - b'_{f'(j)} \right) = b_{f(0)} - b'_{f'(p-1)}.$$

Likewise we see that

$$\gamma_2 := \sum_{j=0}^{p-1} \left(b_{f(j+q)} - b'_{f'(j+q)} \right) = b_{f(q)} - b'_{f'(p-1+q)}.$$

By Kaplan's lemma it then follows that

$$a_n(k) - a_n(k-1) = \gamma_1 - \gamma_2 = b_{f(0)} - b_{f(q)} - b'_{f'(p-1)} + b'_{f'(p-1+q)}. \tag{7}$$

Denote $f(0), f(q), f'(p-1), f'(p-1+q)$ by, respectively, $\alpha_1, \alpha_2, \alpha_3, \alpha_4$. Note that modulo pq we have

$$\alpha_1 \equiv \frac{k}{r},\ \alpha_2 \equiv \frac{k-q}{r},\ \alpha_3 \equiv \frac{k-p}{r},\ \alpha_4 \equiv \frac{k-p-q}{r}.$$

Denote $b_{f(0)}, b_{f(q)}, b'_{f'(p-1)}, b'_{f'(p-1+q)}$ by, respectively, $\beta_1, \beta_2, \beta_3$ and β_4. Thus we can rewrite (7) as

$$a_n(k) - a_n(k-1) = \beta_1 - \beta_2 - \beta_3 + \beta_4. \tag{8}$$

Since α_1 and α_2 have equal p-part, β_1 and β_2 cannot be of opposite sign and hence $|\beta_1 - \beta_2| \leq 1$ and by a similar argument we find $|\beta_3 - \beta_4| \leq 1$. It follows that $|a_n(k) - a_n(k-1)| \leq 2$.

Since α_1 and α_3 have the same q-part, β_1 and β_3 cannot be of opposite sign. Likewise, β_2 and β_4 cannot be of opposite sign. Put $\overline{\beta} = (\beta_1, \beta_2, \beta_3, \beta_4)$. It follows that if $a_n(k) - a_n(k-1) = 2$, then

$$\overline{\beta} = (1, 0, 0, 1) \text{ or } \overline{\beta} = (0, -1, -1, 0). \tag{9}$$

Likewise we infer that if $a_n(k) - a_n(k-1) = -2$, then

$$\overline{\beta} = (-1, 0, 0, -1) \text{ or } \overline{\beta} = (0, 1, 1, 0). \tag{10}$$

The proof is completed if we can show that none of these four possibilities for $\overline{\beta}$ can occur.

`-Excluding` $\overline{\beta} = (1, 0, 0, 1)$: We have $\alpha_1 = [\alpha_1]_p p + [\alpha_1]_q q$.and $\alpha_4 = [\alpha_4]_p p + [\alpha_4]_q q$ with $[\alpha_1]_p \leq \rho, [\alpha_1]_q \leq \sigma, [\alpha_4]_p \leq \rho, [\alpha_4]_q \leq \sigma$, $\alpha_1 \leq k/r$ and $\alpha_4 \leq (k-1)/r$. Since α_2 has the same p-part as α_1 and the same q-part as α_4, we find that $\alpha_2 \equiv [\alpha_1]_p p + [\alpha_4]_q q (\text{mod } pq)$. Since $[\alpha_1]_p p + [\alpha_4]_q q \leq \rho p + \sigma q < pq$, it follows that $\alpha_2 = [\alpha_1]_p p + [\alpha_4]_q q$. Since by assumption $\beta_2 = 0$, we must have $\alpha_2 > k/r$ (if $\alpha_2 \leq k/r$, then we would have $\beta_2 = 1$). Likewise we infer that $\alpha_3 = [\alpha_4]_p p + [\alpha_1]_q q$ and $\alpha_3 > (k-1)/r$. It follows that $\alpha_2 + \alpha_3 > (2k-1)/r$. On the other hand, $\alpha_2 + \alpha_3 = \alpha_1 + \alpha_4 \leq (2k-1)/r$. This contradiction shows that the case $\overline{\beta} = (1, 0, 0, 1)$ cannot occur.

`-Excluding` $\overline{\beta} = (0, -1, -1, 0)$: We have

$$\alpha_2 = [\alpha_2]_p p + [\alpha_2]_q q - pq, \ \alpha_3 = [\alpha_3]_p p + [\alpha_3]_q q - pq$$

with $[\alpha_2]_p > \rho, [\alpha_2]_q > \sigma, [\alpha_3]_p > \rho, [\alpha_4]_q > \sigma$, $\alpha_2 \leq k/r$ and $\alpha_3 \leq (k-1)/r$. Since α_1 has the same p-part as α_2 and the same q-part as α_3, we find that $\alpha_1 \equiv [\alpha_2]_p p + [\alpha_3]_q q - pq (\text{mod } pq)$. Since $0 \leq [\alpha_2]_p p + [\alpha_3]_q q - pq < pq$, we infer that $\alpha_1 = [\alpha_2]_p p + [\alpha_3]_q q - pq$. Since by assumption $\beta_1 = 0$, we must have $\alpha_1 > k/r$ (for otherwise we would have $\beta_1 = -1$). Likewise we infer that $\alpha_4 = [\alpha_3]_p p + [\alpha_2]_q q - pq$. On the one hand we have $\alpha_2 + \alpha_3 \leq (2k-1)/r$, on the other hand we have $\alpha_2 + \alpha_3 = \alpha_1 + \alpha_4 > (2k-1)/r$, a contradiction showing that $\overline{\beta} = (0, -1, -1, 0)$ cannot occur.

`-Excluding the two remaining cases`: can be done by minor variations of the above arguments and is left to the interested reader.

Thus the proof is completed. □

`Remark`. The result of Leher that $|a_n(k) - a_n(k-1)| \leq 4$ is of course an immediate consequence of (7).

5 Coefficient optimal ternary polynomials

In this section we give an application of the jump one property.

The difference between the largest and the smallest coefficients of Φ_{pqr} is known to be at most p [2, (1.5)]. We say that Φ_{pqr} is coefficient optimal if the difference between the largest and smallest coefficient is exactly p. Bachman [2] found two infinite families of coefficient optimal ternary polynomials Φ_{pqr}, with $\mathcal{C}(pqr) = [-(p-1)/2, (p+1)/2]$ for one family and $\mathcal{C}(pqr) = [-(p+1)/2, (p-1)/2]$ for the other family. Using the jump one property one immediately infers the following result.

Lemma 7 *Let $p < q < r$ be odd primes. If $a, b \in \mathcal{C}(pqr)$ and $b - a = p$, then $\mathcal{C}(pqr) = \{-a, a+1, \ldots, b-1, b\}$.*

Thus the jump one property might be helpful in studying families of coefficient optimal ternary cyclotomic polynomials. We demonstrate this by showing how it can be used to reprove the main result in Bachman (whose proof is very different).

Theorem 2 *Let p, q, r, k, n be as in Lemma 4. Then Φ_n is coefficient optimal and in particular*

$$\mathcal{C}(n) = \{a_n(k-r), a_n(k-r+1), \ldots, a_n(k)\} = [-(p-1)/2, (p+1)/2] \cap \mathbb{Z}. \quad (11)$$

Let p, q, r_1, k_1, n_1 be as in Lemma 6. Then Φ_{n_1} is coefficient optimal and in particular

$$\mathcal{C}(n_1) = \{a_{n_1}(k_1 - r_1), \ldots, a_{n_1}(k_1)\} = [-(p+1)/2, (p-1)/2] \cap \mathbb{Z}. \quad (12)$$

Proof. By Lemma 4 one has $a_n(k-r) = -(p-1)/2$ and $a_n(k) = (p+1)/2$. By the jump one property it then follows that the second equality in (11) holds. By Lemma 7 with $b = (p+1)/2$ and $a = -(p-1)/2$ it follows that the first equality in (11) holds.

The proof of the remaining assertion (12) is completely similar, but makes use of Lemma 6 instead of Lemma 4. □

6 Coefficient convexity

Theorem 1 gives naturally rise to the notion of (strong) coefficient convexity. In this section we consider the issue of coefficient convexity of cyclotomic(-like) polynomials in somewhat greater detail, leaving the proofs for a future publication [6].

Definition 2 *We say that Φ_n is coefficient convex if $\mathcal{C}_0(n) = I_n \cap \mathbb{Z}$ for some interval I_n in the reals. We say it is strongly coefficient convex if $\mathcal{C}(n) = I_n \cap \mathbb{Z}$ for some interval I_n in the reals.*

A cyclotomic polynomial can be coefficient convex without being strongly coefficient convex, e.g. Φ_{2p} (p being an odd prime) is coefficient convex but not strongly coefficient convex. The latter cyclotomic polynomial also shows that a cyclotomic polynomial can be flat without being strongly coefficient convex. Moreover, Theorems 3 and 4 below are false if one replaces 'coefficient convex' by 'strongly coefficient convex'.

Using Theorem 1 it is not difficult to establish the following result.

Theorem 3 *Suppose that n has at most 3 prime factors, then Φ_n is coefficient convex.*

Numerical computations suggest that if Φ_n is ternary, then Φ_{2n} is coefficient convex. If this would be true, then in Theorem 3 one can replace '3 prime factors' by '3 distinct odd prime factors'. This is best possible as the following examples show:

$n = 7735 = 5 \cdot 7 \cdot 13 \cdot 17$, $\mathcal{C}(n) = [-7, 5] - \{-9\}$
$n = 530689 = 17 \cdot 19 \cdot 31 \cdot 53$, $\mathcal{C}(n) = [-50, 52] - \{-48, 47, 48, 49, 50, 51\}$.
(Here we write $[-a, b]$ for the range of integers $[-a, b] \cap \mathbb{Z}$.)

We note that if n is ternary, then Φ_{2n} in general does not have the jump one property.

Lemma 8 *If the ternary polynomial Φ_n is not flat, then Φ_{2n} does not have the jump one property.*

Proof. Suppose that $a_n(k) = m$ and $|m| > 1$. Then by Theorem 1 and the identity $\Phi_{2n}(x) = \Phi_n(-x)$, we infer that

$$|a_{2n}(k) - a_{2n}(k-1)| = |a_n(k) + a_n(k-1)| \geq 2|m| - 1 > 1,$$

completing the proof. □

Put

$$\Psi_n(x) = \frac{x^n - 1}{\Phi_n(x)} = \prod_{\substack{1 \leq j \leq n \\ (j,n)>1}} (x - \zeta_n^j).$$

Write $\Psi_n(x) = \sum_{k=0}^{n-\varphi(n)} c_n(k)x^k$. The coefficients $c_n(k)$ are integers that turn out to behave in a way quite similar to the cyclotomic coefficients $a_n(k)$. Apparently Moree [13] was the first to systematically study these coefficients, which he called inverse cyclotomic polynomial coefficients. Here it is not difficult to prove the following result.

Theorem 4 *Suppose that n has at most 3 distinct odd prime factors, then Ψ_n is coefficient convex.*

If n has four or more distinct odd prime factors, then Ψ_n need not be coefficient convex, since we have for example
$n = 60095 = 5 \cdot 7 \cdot 17 \cdot 101$, $\mathcal{C}(\Psi_n) = [-12, 12] - \{-11, 11\}$.
$n = 207805 = 5 \cdot 13 \cdot 23 \cdot 139$, $\mathcal{C}(\Psi_n) = [-16, 16] - \{-15, -13, 13, 15\}$.
$n = 335257 = 13 \cdot 17 \cdot 37 \cdot 41$, $\mathcal{C}(\Psi_n) = [-40, 40] - \{-39, -37, -36, 37, 39\}$.

As we have seen the polynomials $\Phi_n(x)$ and $\Psi_n(x)$ are divisors of $x^n - 1$ that have the tendency to be coefficient convex. One can wonder to what extent other divisors of $x^n - 1$ have the same tendency. (Notice that any divisor of $x^n - 1$ can be written as a product of cyclotomic polynomials.) This problem will be considered in [6].

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 $F_{pqr}(x)$, *Amer. Math. Monthly* **75** (1968), 370–372.

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

[6] A. Decker and P. Moree, The coefficients of divisors of $x^n - 1$, in preparation.

[7] Y. Gallot and P. Moree, Ternary cyclotomic polynomials having a large coefficient, *Crelle's Journal*, to appear.

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

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

[10] E. Leher, Applications of the minimal transversal method in numerical semigroups, PhD thesis, Tel Aviv University, 2007.

[11] E. Lehmer, On the magnitude of the coefficients of the cyclotomic polynomials, *Bull. Amer. Math. Soc.* **42** (1936), 389–392.

[12] H. Möller, Über die Koeffizienten des n-ten Kreisteilungspolynoms, *Math. Z.* **119** (1971), 33–40.

[13] P. Moree, Inverse cyclotomic polynomials, to appear in *J Number Theory.*

[14] R. Thangadurai, On the coefficients of cyclotomic polynomials, *Cyclotomic fields and related topics* (Pune, 1999), 311–322, Bhaskaracharya Pratishthana, Pune, 2000.

12 bis rue Perrey,
31400 Toulouse, France.
e-mail: galloty@orange.fr

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