The upper bound of a class of ternary cyclotomic polynomials
by
Bin Zhang

Abstract
Let $A_+(n)$ denote the largest coefficients of $n$-th cyclotomic polynomial $\Phi_n(x)$. Let $w > 1$ be an integer and $p < q < r$ be odd primes such that $p \equiv 1 \pmod{w}$, $q \equiv 1 \pmod{pw}$ and $r \equiv w \pmod{pq}$. In this paper, we prove that $A_+(pqr) = 1$.

Key Words: cyclotomic polynomial; ternary cyclotomic polynomial; upper bounds of cyclotomic polynomial.

2010 Mathematics Subject Classification: Primary 11B83, Secondary 11C08

1 Introduction

The $n$-th cyclotomic polynomial is the monic polynomial whose roots are the primitive $n$th roots of unity. It is defined by

$$\Phi_n(x) = \prod_{1 \leq j \leq n, (j,n)=1} (x - e^{2\pi ij/n}) = \sum_{k=0}^{\phi(n)} a(n,k)x^k,$$

where $\phi$ is the Euler totient function. Let $A_+(n)$ and $A_-(n)$ be the largest and smallest coefficients of $\Phi_n(x)$, respectively, i.e.,

$$A_+(n) = \max_{0 \leq k \leq \phi(n)} \{a(n,k)\} \quad \text{and} \quad A_-(n) = \min_{0 \leq k \leq \phi(n)} \{a(n,k)\}.$$

If $A_+(n) \leq 1$ and $A_-(n) \geq -1$, then $\Phi_n(x)$ is said to be flat. To study the flatness of $\Phi_n(x)$, it suffices to consider only odd, square-free integers $n$.

In the rest of this paper, we assume that $p < q < r$ are odd primes. It is well-known that all the cyclotomic polynomials $\Phi_p(x)$ and $\Phi_{pq}(x)$ are flat, see [5, 10, 11, 12]. Unlike this, the flatness of ternary cyclotomic polynomials $\Phi_{pqr}(x)$ becomes much more complicated. Since it is hard to determine all flat ternary cyclotomic polynomials, special cases of $p$, $q$, $r$ are usually considered, see [1, 2, 3, 4, 6, 7, 8, 9, 13].

Let $w$ be the smallest positive integer such that $r \equiv \pm w \pmod{pq}$.

The case $w = 1$ has been studied by Kaplan [9], Bachman [2], Flanagan [7], and we know that $\Phi_{pqr}(x)$ is flat if $r \equiv \pm 1 \pmod{pq}$. 
In 2009, Broadhurst [4] made the following conjecture

**Conjecture 1.** Let \( p < q < r \) be odd primes and \( w > 1 \) be an integer such that \( p \equiv 1 \pmod{w} \), \( q \equiv 1 \pmod{pw} \) and \( r \equiv \pm w \pmod{pq} \). Then  
(i) \( A_+(pqr) = 1 \);
(ii) \( A_-(pqr) = -1 \).

In 2012, Elder [6] (arXiv:1207.5811v1) proved this conjecture by considering the cyclotomic polynomial as a gcd of simpler polynomials. In this paper, we establish the following theorem, giving an alternative proof of Conjecture 1 (i).

**Theorem 1.** Let \( p < q < r \) be odd primes and \( w > 1 \) be an integer such that \( p \equiv 1 \pmod{w} \), \( q \equiv 1 \pmod{pw} \) and \( r \equiv w \pmod{pq} \). Then \( A_+(pqr) = 1 \).

In [9], Kaplan proved that \( A_+(pqr) = -A_-(pq) \) whenever \( s > q \) is a prime congruent to \(-r \pmod{pq}\). Combining this result and Theorem 1, we obtain

**Corollary 1.** Let \( p < q < r \) be odd primes and \( w > 1 \) be an integer such that \( p \equiv 1 \pmod{w} \), \( q \equiv 1 \pmod{pw} \) and \( r \equiv -w \pmod{pq} \). Then \( A_-(pqr) = 1 \).

## 2 Preliminaries

By applying Möbius inversion it follows from \( \prod_{d | n} \Phi_d(x) = x^n - 1 \) that

\[
\Phi_{pqr}(x) = \prod_{d | pqr} (x^d - 1)^\mu(pqr) \\
= (1 - x^q - x^r + x^{q+r}) \sum_{l=0}^{p-1} x^l \sum_{i=0}^{p-1} x^{qr+i} \sum_{j=0}^{q-1} x^{pr+j} \sum_{k=0}^{r-1} x^{pq+k} (\mod x^{\phi(pqr)+1}). \tag{2.1}
\]

Observe that each non-negative integer \( n \) has an unique representation in the form

\[
n = x_n qr + y_n pr + z_n pq - \delta_n pqr,
\]

with \( 0 \leq x_n \leq p - 1, 0 \leq y_n \leq q - 1, 0 \leq z_n \leq r - 1 \) and \( \delta_n \in \mathbb{Z} \), so that

\[
n \mapsto (x_n, y_n, z_n, \delta_n)
\]

is well defined. Set

\[
\chi(n) = \begin{cases} 
1 & \text{if } n \geq 0 \text{ and } \delta_n = 0, \\
0 & \text{if } n \geq 0 \text{ and } \delta_n \neq 0, \\
0 & \text{if } n < 0.
\end{cases}
\]

On invoking (2.1), it is easy to get the following identity.

**Lemma 1.**

\[
a(pqr, m) = \sum_{m-p+1 \leq n \leq m} (\chi(n) - \chi(n-q) - \chi(n-r) + \chi(n-q-r)). \tag{2.3}
\]
Since the coefficients of cyclotomic polynomials are symmetric (see, for example, [11]), it suffices to estimate \( a(pqr, n) \) for \( n \) in the range

\[
0 \leq n \leq \frac{1}{2} \phi(pqr).
\]

Observe that in this range the quantity \( \delta_n \) takes on one of three values: 0, 1, 2.

**Lemma 2.** Let \( 0 \leq n \leq \frac{\phi(pqr)}{2} \). Then \( \chi(n) = 1 \) if and only if \( n \) satisfies the inequality

\[
\frac{x_n}{p} + \frac{y_n}{q} \leq \frac{n}{pqr},
\]

**Proof.** Dividing (2.2) by \( pqr \) gives

\[
\frac{x_n}{p} + \frac{y_n}{q} + \frac{z_n}{r} - \delta_n = \frac{n}{pqr},
\]

from which the claim readily follows. \( \square \)

As an immediate consequence of Lemma 2, we have

**Lemma 3.** Let \( 0 \leq n \leq \frac{\phi(pqr)}{2} \). If \( x_n \geq \frac{p}{2} \) or \( y_n \geq \frac{q}{2} \), then \( \chi(n) = 0 \).

**Lemma 4.** Let \( p < q < r \) be odd primes and \( w > 1 \) be an integer such that \( p \equiv 1 \mod{w} \), \( q = kwp + 1 \) and \( r \equiv w \mod{pq} \). Then we have

\[
\begin{align*}
x_1 &= p - \frac{p-1}{w}, & y_1 &= q - k, \\
x_p &= 0, & y_p &= q - kp, \\
x_q &= p - \frac{p-1}{w}, & y_q &= 0, \\
x_r &= 1, & y_r &= q - wk.
\end{align*}
\]

Moreover, we have

\[
\begin{align*}
x_{n \pm 1} &\equiv x_n \pm \frac{p-1}{w} \pmod{p}, & y_{n \pm 1} &\equiv y_n \pm k \pmod{q}, \\
x_{n \pm q} &\equiv x_n \pm \frac{p-1}{w} \pmod{p}, & y_{n \pm q} &\equiv y_n \pmod{q}, \\
x_{n \pm r} &\equiv x_n \pm 1 \pmod{p}, & y_{n \pm r} &\equiv y_n \mp wk \pmod{q}.
\end{align*}
\]

**Proof.** The first display follows by a straightforward calculation from \( n \equiv wx_n \pmod{p} \) and \( n \equiv wpq_n \pmod{q} \). These, in turn, yield the second display, since \( x_{n \pm m} \equiv x_n \pm x_m \pmod{p} \) and \( y_{n \pm m} \equiv y_n \pm y_m \pmod{q} \). \( \square \)

**Lemma 5.** Let \( 0 \leq n \leq \frac{\phi(pqr)}{2} \). Let \( p < q < r \) be odd primes and \( w > 1 \) be an integer such that \( p \equiv 1 \pmod{w} \), \( q = kwp + 1 \) and \( r \equiv w \pmod{pq} \).

1. If \( \chi(n) = 1 \) and \( y_n \geq wk \), then \( \chi(n+r) = 1 \). In other words, if \( y_n \geq wk \), then \( \chi(n+r) \geq \chi(n) \).
2. If \( 0 \leq x_n < \frac{p-1}{w} - 1 \), then \( \chi(n + q + r) = 0 \).
Proof. (1) If \( \chi(n) = 1 \), then, by Lemma 2, we have \( \frac{x_n}{p} + \frac{y_n}{q} \leq \frac{n}{pqr} \). Note that \( x_{n+r} = x_n + 1 \) and \( y_{n+r} = y_n - wk \). So

\[
\frac{x_{n+r}}{p} + \frac{y_{n+r}}{q} \leq \frac{n}{pqr} + \frac{1}{p} - \frac{wk}{q} = \frac{n + r}{pqr}.
\]

This yields \( \chi(n + r) = 1 \) from Lemma 2.

(2) If \( 0 \leq x_n < \frac{p-1}{w} - 1 \), then we have \( x_{n+q+r} = x_n - \frac{p-1}{w} + 1 + p > \frac{q}{2} \). It follows from Lemma 3 that \( \chi(n + q + r) = 0 \), as desired. \( \square \)

Set

\[ Q(n) := \chi(n) - \chi(n + q) - \chi(n + r) + \chi(n + q + r). \]

**Lemma 6.** Let \( 0 \leq n \leq \frac{\varphi(pqr)}{2} \). Let \( p < q < r \) be odd primes and \( w > 1 \) be an integer such that \( p \equiv 1 \pmod{w} \), \( q = kwp + 1 \) and \( r \equiv w \pmod{pq} \).

(1) If \( \frac{p-1}{w} \leq x_n < p \), then \( Q(n) \leq 0 \).

(2) If \( x_n = p - 1 \), then \( Q(n) \leq -\chi(n + r) \). Namely, \( Q(n-1) \leq -\chi(n-1 + r) \).

Proof. (1) Observe that, by Lemma 4, we have \( x_{n+q+r} = x_n - \frac{p-1}{w} + 1 \) and \( y_{n+q+r} = y_n - wk \). Then by Lemma 3, \( \chi(n + q + r) = 0 \). If \( \chi(n) = 1 \), we have \( \frac{x_n}{p} + \frac{y_n}{q} \leq \frac{n}{pqr} \) by Lemma 2. So

\[
\frac{x_{n+q}}{p} + \frac{y_{n+q}}{q} = \frac{x_n - \frac{p-1}{w}}{p} + \frac{y_n}{q} \leq \frac{n}{pqr} - \frac{p-1}{wpq} < \frac{n + q}{pqr}.
\]

By using Lemma 2, we get \( \chi(n + q) = 1 \), implying that \( \chi(n) - \chi(n + q) \leq 0 \). Hence, we have \( Q(n) \leq 0 \).

Next, suppose that \( y_n \geq wk \). In this case, Lemma 5 gives \( \chi(n + r) \geq \chi(n) \). If \( \chi(n + q + r) = 1 \), we have

\[
\frac{x_{n+q+r}}{p} + \frac{y_{n+q+r}}{q} = \frac{x_n - \frac{p-1}{w} + 1}{p} + \frac{y_n - wk}{q} \leq \frac{n + q + r}{pqr}.
\]

This allows us to write

\[
\frac{x_{n+q}}{p} + \frac{y_{n+q}}{q} = \frac{x_n - \frac{p-1}{w}}{p} + \frac{y_n}{q} \leq \frac{n + q}{pqr}.
\]

By using Lemma 2, we get \( \chi(n + q) = 1 \), implying that \( \chi(n + q + r) - \chi(n + q) \leq 0 \). Hence, we have \( Q(n) \leq 0 \).

(2) In this case, we have \( x_n = p - 1 > \frac{p}{2} \) and \( x_{n+q+r} = p - \frac{p-1}{w} > \frac{p}{2} \). By Lemma 3, this gives \( \chi(n) = \chi(n + q + r) = 0 \). Hence \( Q(n) = -\chi(n + q) - \chi(n + r) \leq -\chi(n + r) \). \( \square \)
Lemma 7. Let $p < q < r$ be odd primes and $w > 1$ be an integer such that $p \equiv 1 \pmod{w}$, $q = kwp + 1$ and $r \equiv w \pmod{pq}$. Suppose that $n$ satisfies $m - p - q - r + 1 \leq n \leq m - q - r$ and $0 \leq x_n < \frac{p-1}{w}$, then there exists at most one integers $n$ with $y_n < wk$.

Proof. Assume that there exist two integers $n < n'$ satisfying these conditions. Let $n' = n + l$, where $1 \leq l \leq p - 1$. If $w \leq l \leq p - 1$, we have $y_{n'} = y_n - lk + q > wk$, contradicting the assumption $y_{n'} < wk$. If $1 \leq l < w$, we have $x_{n'} = x_n - \frac{p-1}{w}l + p > \frac{p-1}{w}$, contradicting the condition $0 \leq x_n < \frac{p-1}{w}$. This completes the proof of Lemma 7. \[\square\]

3 The Proof of Theorem 1

Note that for every $\Phi_{pqr}(x)$, we have $a(pqr,0) = a(pqr,1) = 1$. To prove Theorem 1, it suffices to show that $A_+(pqr) \leq 1$.

Since $a(pqr, \phi(pqr) - m) = a(pqr, m)$, we only consider $a(pqr, m)$ for $m$ in the range $0 \leq m \leq \frac{1}{2} \phi(pqr)$. As $n$ takes on $p$ consecutive integer values, $x_n$ takes on every integer value 0 through $p - 1$ exactly once. For $0 \leq i \leq p - 1$, let $n_i \in [m - p - q - r + 1, m - q - r]$ be such that $x_{n_i} = i$.

We rewrite (2.3) in the form

$$
a(pqr, m) = \sum_{m - p - q - r + 1 \leq n \leq m - q - r} (\chi(n) - \chi(n + q) - \chi(n + r) + \chi(n + q + r))
= \sum_{m - p - q - r + 1 \leq n \leq m - q - r} Q(n)
= \sum_{0 \leq x_n < \frac{p-1}{w}} Q(n) + \sum_{\frac{p-1}{w} \leq x_n \leq p-2} Q(n) + Q(n_{p-1}).
$$

By Lemma 7, we split the proof into two cases.

Case 1. For any $x_n \in [0, \frac{p-1}{w})$, we have $y_n \geq wk$.

By using (3.1), Lemma 6 and Lemma 5 (1), we infer that

$$
a(pqr, m) \leq \sum_{0 \leq x_n < \frac{p-1}{w}} Q(n)
\leq \sum_{0 \leq x_n < \frac{p-1}{w}} (\chi(n + q + r) - \chi(n + q))
\leq \sum_{0 \leq x_n < \frac{p-1}{w}} \chi(n + q + r).
$$

If $0 \leq x_n < \frac{p-1}{w} - 1$, by using Lemma 5 (2), we have $\chi(n + q + r) = 0$. So we obtain

$$
a(pqr, m) \leq \chi(n_{\frac{p-1}{w} - 1} + q + r) \leq 1.
$$
Hence, by Lemma 2, we have \( \chi \). So, by Lemma 2, \( \chi \). Combining this with Lemma 5 yields

\[
\chi(n_{\frac{p-1}{w}-1} + q+r) = 0.
\]

So, by Lemma 2, \( \chi(n_{\frac{p-1}{w}-1} + q+r) = 0 \). Combining with Lemma 6 and Lemma 5, we then infer that

\[
a(pqr, m) \leq \sum_{0 \leq x_n \leq \frac{p-1}{w}} Q(n) - \chi(n_{p-1} + r).
\]

Combining this with Lemma 5 yields

\[
a(pqr, m) \leq \sum_{0 \leq x_n \leq \frac{p-1}{w}} Q(n) + Q(n_j) + Q(n_{\frac{p-1}{w}-1}) - \chi(n_{p-1} + r) \leq \chi(n_j) + \chi(n_{\frac{p-1}{w}-1} + q + r) - \chi(n_{p-1} + r).
\]

Since \( n_j \equiv jqr \pmod{p} \) and \( n_{p-1} \equiv (p-1)qr \pmod{p} \), we have \( n_j - n_{p-1} \equiv wj + w \pmod{p} \). So

\[
n_j = n_{p-1} + wj + w \text{ or } n_j = n_{p-1} + wj + w - p.
\]

Case 2.2.1. \( n_j = n_{p-1} + wj + w \).

In this case, we have \( x_{n_{p-1}+r} = 0 \) and \( y_{n_{p-1}+r} = y_{n_j} + wjk \). If \( \chi(n_j) = 0 \), then \( a(pqr, m) \leq 1 \). If \( \chi(n_j) = 1 \), then

\[
\frac{x_{n_j}}{p} + \frac{y_{n_j}}{q} \leq \frac{n_j}{pqr}.
\]

So

\[
\frac{x_{n_{p-1}+r}}{p} + \frac{y_{n_{p-1}+r}}{q} = \frac{j}{p} + \frac{y_{n_j}}{q} - \frac{rj}{pqr} \leq \frac{n_j}{pqr} - \frac{rj}{pqr} < \frac{n_{p-1} + r}{pqr}.
\]

Hence, by Lemma 2, we have \( \chi(n_{p-1} + r) = 1 \), implying that \( a(pqr, m) \leq 1 \).
Case 2.2.2. \( n_j = n_{p-1} + wj + w - p \).
In this case, we have \( n_{p-1} - n_j \equiv -wj - w - 1 \pmod{p} \), and then \( n_{p-1} - n_j = p - wj - w - 1 \). By using Lemma 4, we get
\[
y_{n_{p-1} - 1} + q + r = y_{n_j} + ((w - 1)p + 1 + wj)k + 1 > \frac{q}{2}.
\]
So \( \chi(n_{p-1} + q + r) = 0 \), implying that \( a(pqr, m) \leq 1 \). This completes the proof of Theorem 1.

**Acknowledgements.** This work was supported by Natural Science Foundation of Shandong Province (Grant No. ZR2016AP10), National Natural Science Foundation of China (Grant Nos. 11626137, 11471162) and Science and Technology Project of Qufu Normal University (Grant No. xkj201605)

We would like to thank Professor Chungang Ji and Lijun Huang for useful discussions.
We would also like to thank the referee and editor for valuable comments and helpful suggestions.

**References**


Received: 21.4.2016
Accepted: 18.10.2016