Numerical semigroups, cyclotomic polynomials and Bernoulli numbers

Pieter Moree

Abstract

We give two proofs of a folklore result relating numerical semigroups of embedding dimension two and binary cyclotomic polynomials and explore some consequences. In particular, we give a more conceptual reproof of a result of Hong et al. (2012) on gaps between the exponents of non-zero monomials in a binary cyclotomic polynomial.

The intent of the author with this paper is to better unify the various results within the cyclotomic polynomial and numerical semigroup communities.

1 Introduction

Let $a_1, \ldots, a_m$ be positive integers, and let $S = S(a_1, \ldots, a_m)$ be the set of all non-negative integer linear combinations of $a_1, \ldots, a_m$, that is,

$$S = \{ x_1 a_1 + \cdots + x_m a_m \mid x_i \in \mathbb{Z}_{\geq 0} \}.$$ 

Then $S$ is a semigroup (that is, it is closed under addition). The semigroup $S$ is said to be numerical if its complement $\mathbb{Z}_{\geq 0} \setminus S$ is finite. It is not difficult to prove that $S(a_1, \ldots, a_m)$ is numerical if and only if $a_1, \ldots, a_m$ are relatively prime (see, e.g., [15, p. 2]). If $S$ is numerical, then $\max(\mathbb{Z}_{\geq 0} \setminus S) = F(S)$ is the Frobenius number of $S$. Alternatively, by setting $d(k, a_1, \ldots, a_m)$ equal to the number of non-negative integer representations of $k$ by $a_1, \ldots, a_m$, one can characterize $F(S)$ as the largest $k$ such that $d(k, a_1, \ldots, a_m) = 0$. The value $d(k, a_1, \ldots, a_m)$ is called the denumerant of $k$. That $F(S(4, 6, 9, 20)) = 11$ is well-known to fans of Chicken McNuggets, as 11 is the largest number of McNuggets that cannot be exactly purchased; hence the notion of of the Frobenius number is less abstract than it might appear at first glance. A set of generators of a numerical semigroup is a minimal system of generators if none of its proper subsets generates the numerical semigroup. It is known that every numerical semigroup $S$ has a unique minimal system of generators and also that this minimal system of generators is finite (see, e.g., [18, Theorem 2.7]). The cardinality of the minimal set of generators is called the embedding dimension of the numerical semigroup $S$ and is denoted by $e(S)$. The smallest member in the minimal system of generators is called the

---

*Mathematics Subject Classification (2000)*. 20M14, 11C08, 11B68
multiplicity of the numerical semigroup $S$ and is denoted by $m(S)$. The Hilbert series of the numerical semigroup $S$ is the formal power series

$$H_S(x) = \sum_{s \in S} x^s \in \mathbb{Z}[x].$$

It is practical to multiply this by $1 - x$ as we then obtain a polynomial, called the semigroup polynomial:

$$P_S(x) = (1 - x)H_S(x) = x^{F(S)} + 1 - x \sum_{0 \leq s \leq F(S)} x^s = 1 + (x - 1) \sum_{s \not\in S} x^s. \quad (1)$$

From $P_S$ one immediately reads off the Frobenius number:

$$\text{deg}(P_S(x)) = F(S) + 1. \quad (2)$$

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

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

with $\zeta_n$ a $n$th primitive root of unity (one can take $\zeta_n = e^{2\pi i/n}$). It has degree $\varphi(n)$, with $\varphi$ Euler’s totient function. The polynomial $\Phi_n(x)$ is irreducible over the rationals, see, e.g., Weintraub [22], and has integer coefficients. The polynomial $x^n - 1$ factors as

$$x^n - 1 = \prod_{d|n} \Phi_d(x) \quad (3)$$

over the rationals. By Möbius inversion it follows from (3) that

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}, \quad (4)$$

where $\mu(n)$ denotes the Möbius function. From (4) one deduces that if $p|n$ is a prime, then

$$\Phi_{pn}(x) = \Phi_n(x^p). \quad (5)$$

A good source for further properties of cyclotomic polynomials is Thangadurai [19].

A purpose of this paper is to popularise the following folklore result and point out some of its consequences.

**Theorem 1** Let $p, q > 1$ be coprime integers, then

$$P_{S(p,q)}(x) = (1 - x) \sum_{s \in S(p,q)} x^s = \frac{(x^{pq} - 1)(x - 1)}{(x^p - 1)(x^q - 1)}.$$

In case $p$ and $q$ are distinct primes it follows from (4) and Theorem 1 that

$$P_{S(p,q)}(x) = \Phi_{pq}(x). \quad (6)$$
Already Carlitz [5] in 1966 implicitly mentioned this result without proof. The Bernoulli numbers $B_n$ can be defined by

$$\frac{z}{e^z - 1} = \sum_{n=0}^{\infty} B_n \frac{z^n}{n!}, \quad |z| < 2\pi. \quad (7)$$

One easily sees that $B_0 = 1, B_1 = -1/2, B_2 = 1/6, B_3 = 0, B_4 = -1/30$ and $B_n = 0$ for all odd $n \geq 3$. The most basic recurrence relation is, for $n \geq 1$,

$$\sum_{j=0}^{n} \binom{n+1}{j} B_j = 0. \quad (8)$$

The Bernoulli numbers first arose in the study of power sums $S_j(n) := \sum_{k=0}^{n-1} k^j$. Indeed, one has, cf. Rademacher [14],

$$S_j(n) = \frac{1}{j+1} \sum_{i=0}^{j} \binom{j+1}{i} B_i n^{j+1-i}. \quad (9)$$

In Section 5 we consider an infinite family of recurrences for $B_m$ of which the following is typical

$$B_m = \frac{m}{4m-1} (1 + 2^{m-1} + 3^{m-1} + 5^{m-1} + 6^{m-1} + 9^{m-1} + 10^{m-1} + 13^{m-1} + 17^{m-1}) + \frac{7^m}{4(1-4^m)} \sum_{r=0}^{m-1} \binom{m}{r} \left(\frac{4}{7}\right)^r (1 + 2^{m-r} + 3^{m-r}) B_r.$$

The natural numbers 1, 2, 3, 5, 6, 9, 10, 13 and 17 are precisely those that are not in the numerical semigroup $S(4,7)$.

Let $f = c_1 x^{e_1} + \cdots + c_s x^{e_s}$, where the coefficients $c_i$ are non-zero and $e_1 < e_2 < \cdots < e_s$. Then the maximum gap of $f$, written as $g(f)$, is defined by

$$g(f) = \max_{1 \leq i < s} (e_{i+1} - e_i), \quad g(f) = 0 \text{ when } s = 1.$$

Hong et al. [9] studied $g(\Phi_n)$ (inspired by a cryptographic application [10]). They reduce the study of these gaps to the case where $n$ is square-free and odd and established the following result for the simplest non-trivial case.

**Theorem 2** [9]. If $p$ and $q$ are arbitrary primes with $2 < p < q$, then $g(\Phi_{pq}) = p - 1$.

In Section 6 a conceptual proof of Theorem 2 using numerical semigroups is given.

# 2 Inclusion-exclusion polynomials

It will turn out to be convenient to work with a generalisation of the cyclotomic polynomials, introduced by Bachman [1]. Let $\rho = \{r_1, r_2, \ldots, r_s\}$ be a set of natural numbers satisfying $r_i > 1$ and $(r_i, r_j) = 1$ for $i \neq j$, and put

$$n_0 = \prod_i r_i, \quad n_i = \frac{n_0}{r_i}, \quad n_{ij} = \frac{n_0}{r_ir_j} [i \neq j], \ldots.$$
For each such \( \rho \) we define a function \( Q_\rho \) by

\[
Q_\rho(x) = \frac{(x^{n_0} - 1) \cdot \prod_{i<j} (x^{n_{ij}} - 1) \cdots}{\prod_i (x^{n_i} - 1) \cdot \prod_{i<j<k} (x^{n_{ijk}} - 1) \cdots}.
\]

(10)

For example, if \( \rho = \{p, q\} \), then

\[
Q_{\{p,q\}}(x) = (x^{pq} - 1)(x - 1)(x^p - 1)(x^q - 1).
\]

(11)

It can be shown that \( Q_\rho(x) \) defines a polynomial of degree \( d = \prod_i (r_i - 1) \). We define its coefficients \( a_\rho(k) \) by

\[
Q_\rho(x) = \sum_{k \geq 0} a_\rho(k)x^k.
\]

Furthermore, \( Q_\rho(x) \) is selfreciprocal; that is \( a_\rho(k) = a_\rho(d - k) \) or, what amounts to the same thing,

\[
Q_\rho(x) = x^d Q_\rho\left(\frac{1}{x}\right).
\]

(12)

If all elements of \( \rho \) are prime, then comparison of (10) with (4) shows that

\[
Q_\rho(x) = \Phi_{r_1 r_2 \cdots r_s}(x).
\]

(13)

If \( n \) is an arbitrary integer and \( \gamma(n) = p_1 \cdots p_s \) its squarefree kernel, then by (5) and (13) we have \( Q_{\{p_1, \ldots, p_s\}}\left(x^{n/\gamma(n)}\right) = \Phi_{\gamma}(x) \) and hence inclusion-exclusion polynomials generalize cyclotomic polynomials. They can be expressed as products of cyclotomic polynomials.

**Theorem 3** [1]. Given \( \rho = \{r_1, \ldots, r_s\} \) and

\[
D_\rho = \{d : d \mid \prod_i r_i \text{ and } (d, r_i) > 1 \text{ for all } i\},
\]

then

\[
Q_\rho(x) = \prod_{d \in D_\rho} \Phi_d(x).
\]

**Example.** We have \( Q_{\{4,7\}} = \Phi_{28}\Phi_{14} \).

### 2.1 Binary inclusion-exclusion polynomials: a close-up

Lam and Leung [11] discuss binary cyclotomic polynomials \( \Phi_{pq} \) in detail, with \( p \) and \( q \) primes (their results were anticipated by Lenstra [12]). Now, let \( p, q > 1 \) be positive coprime integers. All arguments in their paper easily generalize to this setting (instead of taking \( \xi \) to be a primitive \( pq \)th-root of unity as they do, one has to take \( \zeta \) a \( pq \)th root of unity satisfying \( \zeta^p \neq 1 \) and \( \zeta^q \neq 1 \)). One finds that

\[
Q_{\{p,q\}}(x) = \sum_{i=0}^{\rho-1} x^{ip} \sum_{j=0}^{\sigma-1} x^{jq} - x^{-pq} \sum_{i=0}^{q-1} x^{ip} \sum_{j=0}^{\sigma-1} x^{jq},
\]

(14)

where \( \rho \) and \( \sigma \) are the (unique) non-negative integers for which \( 1 + pq = \rho p + \sigma q \). On noting that upon expanding the products in identity (14), the resulting monomials are all different, we arrive at the following result.
Lemma 1 Let \( p, q > 1 \) be coprime integers. Let \( \rho \) and \( \sigma \) be the (unique) non-negative integers for which \( 1 + \rho q = \rho p + \sigma q \). Let \( 0 \leq m < pq \). Then either \( m = \alpha p + \beta q \) or \( m = \alpha p + \beta q - pq \) with \( 0 \leq \alpha \leq \rho - 1 \) the unique integer such that \( \alpha p \equiv m \pmod{q} \) and \( 0 \leq \beta \leq p - 1 \) the unique integer such that \( \beta q \equiv m \pmod{p} \).

The inclusion-exclusion coefficient \( a_{\{p,q\}}(m) \) equals

\[
\begin{cases} 
1 & \text{if } m = \alpha p + \beta q \text{ with } 0 \leq \alpha \leq \rho - 1, \ 0 \leq \beta \leq \sigma - 1; \\
-1 & \text{if } m = \alpha p + \beta q - pq \text{ with } \rho \leq \alpha \leq q - 1, \ \sigma \leq \beta \leq p - 1; \\
0 & \text{otherwise.}
\end{cases}
\]

Corollary 1 The number of positive coefficients in \( Q_{\{p,q\}}(x) \) equals \( \rho \sigma \) and the number of negative ones equals \( \rho \sigma - 1 \). The number of non-zero coefficients equals \( 2\rho \sigma - 1 \).

This corollary (in case \( p \) and \( q \) are distinct primes) is due to Carlitz [5].

Lemma 1 can be nicely illustrated with an LLL-diagram (for Lenstra, Lam and Leung). Here is one such diagram for \( p = 5 \) and \( q = 7 \).

\[
\begin{array}{cccccccc}
28 & 33 & 3 & 8 & 13 & 18 & 23 \\
21 & 26 & 31 & 1 & 6 & 11 & 16 \\
14 & 19 & 24 & 29 & 34 & 4 & 9 \\
7 & 12 & 17 & 22 & 27 & 32 & 2 \\
0 & 5 & 10 & 15 & 20 & 25 & 30 \\
\end{array}
\]

We start with 0 in the lower left and add \( p \) for every move to the right and \( q \) for every move upwards. Reduce modulo \( pq \). Every integer \( 0, \ldots, pq - 1 \) is obtained precisely once in this way (by the Chinese remainder theorem).

Lemma 1 can be reformulated in the following way.

Lemma 2 Let \( p, q > 1 \) be coprime integers. The numbers in the lower left corner of the LLL-diagram are the exponents of the terms in \( Q_{\{p,q\}} \) with coefficient 1. The numbers in the upper right corner are the exponents of the terms in \( Q_{\{p,q\}} \) with coefficient -1. All other coefficients equal 0.

3 Two proofs of the main (folklore) result

In terms of inclusion-exclusion polynomials we can reformulate Theorem 1 as follows.

Theorem 4 If \( p, q > 1 \) are coprime integers, then \( P_{S(p,q)}(x) = Q_{\{p,q\}}(x) \).

Our first proof will make use of ‘what is probably the most versatile tool in numerical semigroup theory’ [18, p. 8], namely Apéry sets.

First proof of Theorem 1 The Apéry set of \( S \) with respect to a nonzero \( m \in S \) is defined as

\[ \text{Ap}(S; m) = \{ s \in S : s - m \not\in S \} \]

Note that

\[ S = \text{Ap}(S; m) + m\mathbb{Z}_{\geq 0} \]
and that $\text{Ap}(S; m)$ consists of a complete set of residues modulo $m$. Thus we have

$$H_S(x) = \sum_{w \in \text{Ap}(S; m)} x^w = \frac{1}{1-x^m} \sum_{w \in \text{Ap}(S; m)} x^w.$$  

Note that if $S = \langle a_1, \ldots, a_n \rangle$, then $\text{Ap}(S; a_1) \subseteq \langle a_2, \ldots, a_n \rangle$. It follows that $\text{Ap}(S(p, q); p)$ consists of multiples of $q$. The latter set equals the minimal set of multiples of $q$ representing every congruence class modulo $p$ and hence $\text{Ap}(S(p, q); p) = \{0, q, \ldots, (p - 1)q\}$ (see [16, Proposition 1] or [13, Example 8.22]). Hence

$$H_{S(p, q)}(x) = \frac{1 + x^q + \cdots + x^{(p - 1)q}}{1 - x^q} = \frac{1 - x^p}{(1 - x^q)(1 - x^p)}.$$  

Using this identity and (11) easily completes the proof. \hfill \Box

Remark. This proof is an adaptation of the arguments given in [16]. Indeed, once we know the Apéry set of a numerical semigroup $S$, by using [16, (4)], we obtain an expression for $H_S(x)$ and consequently for $P_S(x)$. Theorem 4 is a particular case of [16] Proposition 2, with $\{p, q\} = \{a, a + d\}$ and $k = 1$.

Our second proof uses the denumerant (see [15, Chapter 4] for a survey) and the starting point is the observation that

$$\frac{1}{(1-x^p)(1-x^q)} = \sum_{j \geq 0} r(j)x^j,$$  

where $r(j)$ denotes the cardinality of the set $\{(a, b) : a \geq 0, b \geq 0, ap + bq = j\}$. In the terminology of the introduction, we have $r(j) = d(j; p, q)$. Concerning $r(j)$ we make the following observation.

Lemma 3 Suppose that $k \geq 0$, then $r(k + pq) = r(k) + 1$.

Proof. Put $\alpha \equiv kp^{-1}(\text{mod } q)$, $0 \leq \alpha < q$ and $\beta \equiv kq^{-1}(\text{mod } p)$, $0 \leq \beta < p$ and $k_0 = \alpha p + \beta q$. Note that $k_0 < 2pq$. We have $k \equiv k_0(\text{mod } pq)$. Now if $k \not\in S$, then $k < k_0$ and $k + pq = k_0 \in S$ (since $k_0 < 2pq$). It follows that if $r(k) = 0$, then $r(k + pq) = 1$. If $k \in S$, then $k = k_0 + tpq$ for some $t \geq 0$ and we have $r(k) = 1 + t$, where we use that

$$k = (\alpha + tq)p + \beta q = (\alpha + (t - 1)q)p + (\beta + 1)p = \cdots = \alpha p + (\beta + tq)p.$$  

We see that $r(k + pq) = 1 + t + 1 = r(k) + 1$. \hfill \Box

Remark. It is not difficult to derive an explicit formula for $r(n)$ (see, e.g., [2, Section 1.3] or [13, pp. 213-214]). Let $p^{-1}, q^{-1}$ denote inverses of $p$ modulo $q$, respectively $q$ modulo $p$. Then we have

$$r(n) = \frac{n}{pq} - \left\{\frac{p^{-1}n}{q}\right\} - \left\{\frac{q^{-1}n}{p}\right\} + 1,$$
where \( \{x\} \) denote the fractional-part function. Note that Lemma 3 is a corollary of this formula.

**Second proof of Theorem 4.** From Lemma 3 we infer that

\[
(1 - x^{pq}) \sum_{j \geq 0} r(j)x^j = \sum_{j=0}^{pq-1} r(j)x^j + \sum_{j=pq}^{\infty} (r(j) - r(j-pq))x^j = \sum_{j=0}^{pq-1} r(j)x^j + \sum_{j \geq pq} x^j,
\]

where we used that \( r(j) \leq 1 \) for \( j < pq \) and \( r(j) \geq 1 \) for \( j \geq pq \). Using this identity and (16) easily completes the proof. \( \square \)

### 4 Symmetric numerical semigroups

A numerical semigroup \( S \) is said to be **symmetric** if

\[
S \cup (F(S) - S) = \mathbb{Z},
\]

where \( F(S) - S = \{F(S) - s | s \in S\} \). Symmetric semigroups occur in the study of monomial curves that are complete intersections, Gorenstein rings, and the classification of plane algebraic curves, see, e.g. [15, p. 142]. For example, Herzog and Kunz showed that a Noetherian local ring of dimension one and analytically irreducible is a Gorenstein ring if and only if its associate value semigroup is symmetric.

We will now show that the selfreciprocity of \( Q_{\{p,q\}}(x) \) implies that \( S(p,q) \) is symmetric (a well-known result, see, e.g., [18, Corollary 4.7]).

**Theorem 5** Let \( S \) be a numerical semigroup. Then \( S \) is symmetric if and only if \( P_S(x) \) is selfreciprocal.

**Proof.** If \( s \in S \cap (F(S) - S) \), then \( s = F(S) - s_1 \) for some \( s_1 \in S \). This implies that \( F(S) \in S \), a contradiction. Thus \( S \) and \( F(S) - S \) are disjoint sets. Since every integer \( n \geq F(S) + 1 \) is in \( S \) and every integer \( n \leq -1 \) is in \( F(S) - S \), the assertion is equivalent to showing that

\[
\sum_{0 \leq j \leq F(S), j \in S} x^j + \sum_{0 \leq j \leq F(S), j \notin S} x^{F(S) - j} = 1 + x + \cdots + x^{F(S)},
\]

if and only if \( P_S(x) \) is selfreciprocal. On noting by (11) that

\[
x^{F(S)+1}P_S\left(\frac{1}{x}\right) - P_S(x) = 1 - x^{F(S)+1} + (x - 1)\left(\sum_{0 \leq j \leq F(S), j \in S} x^j + \sum_{0 \leq j \leq F(S), j \notin S} x^{F(S) - j}\right),
\]

we see that \( x^{F(S)+1}P_S(1/x) = P_S(x) \) if and only if (17) holds. Clearly (17) holds if and only if \( S \) is symmetric. \( \square \)

Using the latter result and Theorem 4 we infer the following classical fact.
Theorem 6  A numerical semigroup of embedding dimension 2 is symmetric.

Theorem 4 together with Theorem 3 shows that if \( e(S) = 2 \), then \( P_S(x) \) can be written as a product of cyclotomic polynomials. This leads to the following problem.

Problem 1  Characterize the numerical semigroups \( S \) for which \( P_S(x) \) can be written as a product of cyclotomic polynomials.

Since \( P_S(0) \neq 0 \), the product cannot involve \( \Phi_1(x) = x - 1 \) and so it is selfreciprocal. Therefore, by Theorem 5 such an \( S \) must be symmetric. Ciolan et al. \[6\] make some progress towards solving this problem and show, e.g., that \( P_S(x) \) can be written as a product of cyclotomic polynomials also if \( e(S) = 3 \) and \( S \) is symmetric.

5  Gap distribution

The non-negative integers not in \( S \) are called the **gaps** of \( S \). E.g., the gaps in \( S(4,7) \) are \( 1, 2, 3, 5, 6, 9, 10, 13 \) and \( 17 \). The number of gaps of \( S \) is called the **genus** of \( S \), and denoted by \( N(S) \). The set of gaps is denoted by \( G(S) \). The following well-known result holds, cf. \[15\] Lemma 7.2.3 or \[18\] Corollary 4.7.

**Theorem 7**  We have \( 2N(S) \geq F(S) + 1 \) with equality if and only if \( S \) is symmetric.

**Proof.** The proof of Theorem 5 shows that \( 2\#\{0 \leq j \leq F(S) : j \in S\} \leq F(S) + 1 \) with equality if and only if \( S \) is symmetric. Now use that \( \#\{0 \leq j \leq F(S) : j \in S\} = F(S) + 1 - N(S) \).

From (2) and Theorem 4 we infer the following well-known result due to Sylvester:

\[
F(S(p,q)) = pq - p - q. \tag{18}
\]

From Theorem 6, Theorem 7 and (18), we obtain another well-known result of Sylvester:

\[
N(S(p,q)) = (p-1)(q-1)/2. \tag{19}
\]

For four different proofs of (18) and more background see \[15\], pp. 31-34; the shortest proof of (18) and (19) the author knows of is in the book by Wilf \[23\], p. 88.

Additional information on the gaps is given by the so-called **Sylvester sum**

\[
\sigma_k(p,q) := \sum_{s \notin S(p,q)} s^k.
\]

By (19) we have \( \sigma_0(p,q) = (p-1)(q-1)/2 \). By (11) and Theorem 4 we infer that

\[
\sum_{j \notin S(p,q)} x^j = \frac{1 - Q_{\{p,q\}}(x)}{1 - x}. \tag{20}
\]
It is not difficult to derive a formula for $\sigma_k(p, q)$ for arbitrary $k$. On substituting $x = e^z$ and recalling the Taylor series expansion $e^z = \sum_{k \geq 0} z^k / k!$, we obtain from (20) and (11) the identity

$$\sum_{k=0}^{\infty} \sigma_k(p, q) \frac{z^k}{k!} = \frac{e^{pqz} - 1}{(e^z - 1)(e^{qz} - 1)} - \frac{1}{e^z - 1}. \quad (21)$$

We obtain from (21), on multiplying by $z$ and using the Taylor series expansion (7), that

$$\sum_{m=1}^{\infty} m\sigma_{m-1}(p, q) \frac{z^m}{m!} = \sum_{i=0}^{\infty} B_i p^i \frac{z^i}{i!} \sum_{j=0}^{\infty} B_j q^j \frac{z^j}{j!} \sum_{k=0}^{\infty} (pqz)^k \frac{1}{(k+1)!} - \sum_{m=0}^{\infty} B_m \frac{z^m}{m!}.$$

Equating coefficients of $z^m$ then leads to the following result.

**Theorem 8** [17]. For $m \geq 1$ we have

$$m\sigma_{m-1}(p, q) = \frac{1}{m+1} \sum_{i=0}^{m} \sum_{j=0}^{m-i} \binom{m+1}{i, j, m+1-i-j} B_i B_j p^{m-j} q^{m-i} - B_m.$$

Using this formula we find e.g. that $\sigma_1(p, q) = \frac{1}{12} (p-1)(q-1)(12pq - p - q - 1)$ (this result is due to Brown and Shiue [3]) and $\sigma_2(p, q) = \frac{1}{12} (p-1)(q-1)pq(pq - p - q)$. The proof we have given here of Theorem 8 is due to Rødseth [17], with the difference that we gave a different proof of the identity (21).

By using the formula (9) for power sums we obtain from Theorem 8 the identity

$$m\sigma_{m-1}(p, q) = \sum_{r=0}^{m} \binom{m}{r} p^{m-r} q^r S_r(p) - B_m,$$

giving rise to the following recursion formula for $B_m$:

$$B_m = \frac{m}{p^m-1} \sigma_{m-1}(p, q) + \frac{q^m}{p(1-p^m)} \sum_{r=0}^{m-1} \binom{m}{r} \left( \frac{p}{q} \right)^r B_r S_{m-r}(p).$$

On taking $p = 4$ and $q = 7$, we obtain the recursion for $B_m$ stated in the introduction.

Tuenter [20] established the following characterization of the gaps in $S(p, q)$. For every finite function $f$,

$$\sum_{n \not\in S} (f(n+p) - f(n)) = \sum_{n=1}^{p-1} (f(nq) - f(n)),$$

where $p$ and $q$ are interchangeable. He shows that by choosing $f$ appropriately one can recover all earlier results mentioned in this section and in addition the identity

$$\prod_{n \not\in S(p, q)} (n + p) = q^{p-1} \prod_{n \not\in S(p, q)} n.$$

Wang and Wang [21] obtained results similar to those of Tuenter for the alternate Sylvester sums $\sum_{s \not\in S(p, q)} (-1)^s s^k$.  

9
6 A reproof of Theorem 2

As mentioned previously, the gaps for $S(4,7)$ are given by $1, 2, 3, 5, 6, 9, 10, 13$ and $17$. One could try to break this down in terms of gap blocks, that is blocks of consecutive gaps, (also known in the literature as deserts [7, Definition 16]): \{1, 2, 3\}, \{5, 6\}, \{9, 10\}, \{13\}, and \{17\}. It is interesting to compare this with the distribution of the element blocks, that is finite blocks of consecutive elements in $S$. For $S(4,7)$ we get \{0\}, \{4\}, \{7, 8\}, \{11, 12\} and \{14, 15, 16\}. The longest gap block we denote by $g(G(S))$ and the longest element block by $g(S)$.

The following result gives some information on gap blocks and element blocks in a numerical semigroup of embedding dimension 2. Recall that the smallest positive integer of $S$ is called the multiplicity and denoted by $m(S)$.

Lemma 4
1) The longest gap block, $g(G(S))$, has length $m(S) - 1$.
2) The longest element block, $g(S)$, has length not exceeding $m(S) - 1$.
3) If $S$ is symmetric, then $g(S) = m(S) - 1$.

Proof. 1) Let $S = \{s_0, s_1, s_2, s_3, \ldots\}$ be the elements of $S$ written in ascending order, i.e., $0 = s_0 < s_1 < s_2 < \cdots$. Since $s_0 = 0$ and $s_1 = m(S)$ we have $g(G(S)) \geq m(S) - 1$. Since all multiples of $m(S)$ are in $S$, it follows that actually $g(G(S)) = m(S) - 1$.
2) If $g(S) \geq m(S)$, it would imply that we can find $k, k + 1, \ldots, k + m(S) - 1$ all in $S$ such that $k + m(S) \not\in S$. This is clearly a contradiction.
3) If $S$ is symmetric, then we clearly have $g(S) = g(G(S)) = m(S) - 1$. \hfill $\Box$

Remark. The second observation was made by my intern Alexandru Ciolan. It allows one to prove Theorem 10.

Finally, we will generalize a result of Hong et al. [9].

Theorem 9 If $p, q > 1$ are coprime integers, then $g(Q_{(p,q)}(x)) = \min\{p, q\} - 1$.

Proof. Note that $g(Q_{(p,q)}(x))$ equals the maximum of the longest gap block length and the longest element block length and hence by Lemma 4 equals $m(S(p,q)) - 1 = \min\{p, q\} - 1$. \hfill $\Box$

This result can be easily generalized further.

Theorem 10 We have $g(P_S(x)) = m(S) - 1$.

Proof. Using that $P_S(x) = (1 - x)H_S(x)$ and Lemma 4 we infer that $g(P_S(x)) = \max\{g(S), g(G(S))\} = m(S) - 1$. \hfill $\Box$

7 The LLL-diagram revisited

It is instructive to indicate (we do this in boldface) the gaps of $S(p,q)$ in the LLL-diagram. They are those elements $\alpha p + \beta q$ with $0 \leq \alpha \leq q - 1$, $0 \leq \beta \leq p - 1$ for which $\alpha p + \beta q > pq$. Note that the Frobenius number equals $(q - 1)p + (p - 1)q - pq$ and so appears in the top right hand corner of the LLL-diagram. We will demonstrate this (again) for $p = 5$ and $q = 7$. 


Theorem 11 If we get the following reformulation of Theorem 4 at the coefficient level.

As a check we can verify that \( N(S(p,q)) = (p-1)(q-1)/2 \) integers appear in boldface.

On comparing coefficients in the identity \( (1-x) \sum_{j \in S(p,q)} x^j = \sum_{j \geq 0} a_{p,q}(j)x^j \) we get the following reformulation of Theorem 4 at the coefficient level.

Theorem 12 If \( p,q > 1 \) are coprime integers, then

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

Corollary 2 The non-zero coefficients of \( Q_{p,q} \) alternate between 1 and \(-1\).

The next result gives an example where an existing result on cyclotomic coefficients yields information about numerical semigroups.

Theorem 12 Let \( p,q, \rho \) and \( \sigma \) be as in Lemma 4. If \( S = S(p,q) \), then there are \( \rho \sigma - 1 \) gap blocks and \( \rho \sigma - 1 \) element blocks.

Proof. In view of Theorem 11 we have \( a_{p,q}(k) = 1 \) if and only if \( k \) is at the start of an element block (including the infinite block \([F(S) + 1, \infty) \cap \mathbb{Z}\)). Moreover, \( a_{p,q}(k) = -1 \) if and only if \( k \) is at the end of a gap block. The proof is now completed by invoking Corollary 1. \( \square \)

Using Lemma 2 and Theorem 11 our folklore result can now be reformulated in terms of the LLL-diagram.

Theorem 13 Let \( p,q > 1 \) be coprime integers and denote \( S(p,q) \cap \{0, \ldots, pq-1\} \) by \( T \). The integers \( k \in T \) such that \( k-1 \notin T \) are precisely the integers in the lower left corner of the LLL-diagram. The integers \( k \notin T \) such that \( k-1 \in T \) are precisely the integers in the upper right corner. If \( k \) is not in the lower left or upper right corner, then either \( k \in T \) and \( k-1 \in T \) or \( k \notin T \) and \( k-1 \notin T \).

Denote \( S(p,q) \) by \( S \). Note that the upper right integer in the lower left corner of the LLL-diagram equals \( F(S) + 1 \) and that the remaining integers in the lower left corner are all \( < F(S) \). This observation together with (19) then leads to the following corollary of Theorem 13.

Corollary 3 If \( p,q > 1 \) are coprime integers, then

\[
\begin{align*}
\{0 \leq k \leq F(S) : k \in S, k-1 \in S\} &= (p-1)(q-1)/2 - \rho \sigma + 1; \\
\{0 \leq k \leq F(S) : k \in S, k-1 \notin S\} &= \rho \sigma - 1; \\
\{0 \leq k \leq F(S) : k \notin S, k-1 \in S\} &= \rho \sigma - 1; \\
\{0 \leq k \leq F(S) : k \notin S, k-1 \notin S\} &= (p-1)(q-1)/2 - \rho \sigma - 1.
\end{align*}
\]
The distribution of the quantity $\rho \sigma$ that appears at various places in this article has been recently studied using deep results from analytic number theory by Bzdęga [4] and Fouvry [8]. In particular they are interested in counting the number of integers $m = pq \leq x$ with $p, q$ distinct primes such that $\theta(m)$, the number of non-zero coefficients of $\Phi_m$, satisfies $\theta(m) \leq m^{1/2+\gamma}$, with $\gamma > 0$ fixed. (Note that by Corollary 1 we have $\theta(m) = 2\rho \sigma - 1$.)

Acknowledgement. I like to thank Matthias Beck, Scott Chapman, Alexandru Ciolan, Pedro A. García-Sánchez, Nathan Kaplan, Bernd Kellner, Jorge Ramírez Alfonsín, Ali Sinan Sertöz, Paul Tegelaar and the three referees for helpful comments. Alexandru Ciolan pointed out to me that $g(S) \leq m(S) - 1$, which allows one to prove Theorem 10.

References

[1] G. Bachman, On ternary inclusion-exclusion polynomials, *Integers* 10 (2010) A48 623–638.

[2] M. Beck and S. Robins, *Computing the continuous discretely. Integer-point enumeration in polyhedra*, Undergraduate Texts in Mathematics. Springer, New York, 2007.

[3] T.C. Brown and P. J.-S. Shiue, A remark related to the Frobenius problem, *Fibonacci Quart.* 31 (1993) 32–36.

[4] B. Bzdęga, Sparse binary cyclotomic polynomials, *J. Number Theory* 132 (2012) 410–413.

[5] L. Carlitz, The number of terms in the cyclotomic polynomial $F_{pq}(x)$, *Amer. Math. Monthly* 73 (1966) 979-981.

[6] A. Ciolan, P.A. García-Sánchez and P. Moree, Cyclotomic numerical semigroups, in preparation.

[7] J.I. Farrán and C. Munuera, Goppa-like bounds for the generalized Feng-Rao distances, International Workshop on Coding and Cryptography (WCC 2001) (Paris), *Discrete Appl. Math.* 128 (2003) 145–156.

[8] É. Fouvry, On binary cyclotomic polynomials, *Algebra Number Theory* 7 (2013) 1207–1223.

[9] H. Hong, E. Lee, H.-S. Lee and C.-M. Park, Maximum gap in (inverse) cyclotomic polynomial, *J. Number Theory* 132 (2012) 2297–2315, available at [http://dx.doi.org/10.1016/j.jnt.2012.04.008](http://dx.doi.org/10.1016/j.jnt.2012.04.008).

[10] H. Hong, E. Lee, H.-S. Lee and C.-M. Park, Simple and exact formula for minimum loop length in Ate$_i$ pairing based on Brezing-Weng curves, *Des. Codes Cryptogr.* 67 (2013) 271–292.
[11] T.Y. Lam and K.H. Leung, On the cyclotomic polynomial \( \Phi_{pq}(x) \), *Amer. Math. Monthly* 103 (1996) 562–564.

[12] H. W. Lenstra, Vanishing sums of roots of unity, Proceedings, Bicentennial Congress Wiskundig Genootschap (Vrije Univ., Amsterdam, 1978), Part II, 249–268, Math. Centre Tracts 101, Math. Centrum, Amsterdam, 1979.

[13] I. Niven, H.S. Zuckerman and H.L. Montgomery, *An introduction to the theory of numbers*, 5th edition, John Wiley & Sons, Inc., New York, 1991.

[14] H. Rademacher, *Topics in analytic number theory*, Die Grundlehren der mathematischen Wissenschaften 169, Springer-Verlag, New York-Heidelberg, 1973.

[15] J.L. Ramírez Alfonsín, *The Diophantine Frobenius problem*, Oxford Lecture Series in Mathematics and its Applications 30, Oxford University Press, Oxford, 2005.

[16] J.L. Ramírez Alfonsín and Ø.J. Rødseth, Numerical semigroups: Apéry sets and Hilbert series, *Semigroup Forum* 79 (2009) 323–340.

[17] Ø.J. Rødseth, A note on Brown and Shiue’s paper on a remark related to the Frobenius problem, *Fibonacci Quart.* 32 (1994) 407–408.

[18] J.C. Rosales and P.A. García-Sánchez, *Numerical semigroups*, Developments in Mathematics 20, Springer, New York, 2009.

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

[20] H.J.H. Tuenter, The Frobenius problem, sums of powers of integers, and recurrences for the Bernoulli numbers, *J. Number Theory* 117 (2006), 376–386.

[21] W. Wang and T. Wang, Alternate Sylvester sums on the Frobenius set, *Comput. Math. Appl.* 56 (2008) 1328–1334.

[22] S.H. Weintraub, Several proofs of the irreducibility of the cyclotomic polynomials, *Amer. Math. Monthly* 120 (2013) 537–545.

[23] H.S. Wilf, *Generatingfunctionology*, Academic Press, Inc., Boston, MA, 1990.

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