Max-Planck-Institut für Mathematik
Bonn

Numerical semigroups, cyclotomic polynomials and Bernoulli numbers

by

Pieter Moree

Max-Planck-Institut für Mathematik
Preprint Series 2013 (45)

Numerical semigroups, cyclotomic polynomials and Bernoulli numbers

Pieter Moree

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

MPIM 13-45

Numerical semigroups, cyclotomic polynomials and Bernoulli numbers

Pieter Moree

Abstract

We give two proofs of a folkore 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 popularise cyclotomic polynomial work under the numerical semigroup community and vice versa.

1 Introduction

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

$$S = \{a_1x_1 + \cdots + a_mx_m \mid x_i \in \mathbb{Z}_{\geq 0}\}.$$

Then S is a *semigroup* (that is, it is closed under addition). The semigroup S is said to be *numerical* if its complement $\mathbb{Z}_{\geq 0}\backslash S$ is finite. It is not difficult to prove that $S(a_1, \ldots, a_m)$ is numerical iff $a_1, \ldots, a_m$ are relatively prime (see, e.g., [10, p. 2]). If S is numerical, then $\max\{\mathbb{Z}_{\geq 0}\backslash S\} = F(S)$ is the *Frobenius number* of S. Alternatively one can characterize $F(S)$ as the largest integer m such that $d(m; a_1, \ldots, a_m)$, called the *denumerant*, that is the number of non-negative integer representations of m by $a_1, \ldots, a_m$, equals zero. That $F(S(4, 6, 9, 20)) = 11$ is well-known to fans of McNuggets, as 11 is the largest number of McNuggets that cannot be ordered and so the notion of Frobenius numbers 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., [13, 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

Mathematics Subject Classification (2000). 20M14, 11C08, 11B68

is called the *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

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

Note that for a numerical semigroup S, $P_S(x) := (1-x)H_S(x)$ is a polynomial. It is called the *semigroup polynomial.* From it one can easily read off the Frobenius number:

$$\deg(P_S(x)) = F(S) + 1. \tag{1}$$

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

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

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. The polynomial $\Phi_n(x)$ is irreducible over the rationals, see, e.g., Weintraub [17], and has integer coefficients. The polynomial $x^n - 1$ factorizes as

$$x^n - 1 = \prod_{d|n} \Phi_d(x) \tag{2}$$

over the rationals. By Möbius inversion it follows from (2) that

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}, \tag{3}$$

where $\mu(n)$ denotes the Möbius function. From (3) one deduces that if $p|n$ is a prime, then

$$\Phi_{pn}(x) = \Phi_n(x^p). \tag{4}$$

A good source for further properties of cyclotomic polynomials is Thangadurai [14].

The 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 (3) and Theorem 1 that

$$P_{S(p,q)}(x) = \Phi_{pq}(x). \tag{5}$$

Already Carlitz [5] in 1966 implicitly mentioned this result without proof.

The Bernoulli numbers B_n can be defined by

$$\frac{z}{e^z - 1} = \sum_{n=0}^{\infty} B_n \frac{z^n}{n!}, \ |z| < 2\pi. \tag{6}$$

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 $n \geq 1$,

$$\sum_{j=0}^{n} \binom{n+1}{j} B_j = 0. \tag{7}$$

with $B_0 = 1$. 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 [9],

$$S_j(n) = \frac{1}{j+1} \sum_{i=0}^{j} \binom{j+1}{i} B_i n^{j+1-i}. \tag{8}$$

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

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

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 $c_1, \ldots, c_s \neq 0$ and $e_1 < e_2 < \cdots < e_s$. Then the *maximum gap* of f, written as $g(f)$, is defined by

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

Hong et al. [6] studied $g(\Phi_n)$. 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 [6]. *Let $2 < p < q$ be arbitrary primes. 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

$$n_0 = \prod_i r_i, \;\; n_i = \frac{n_0}{r_i}, \;\; n_{ij} = \frac{n_0}{r_i r_j}[i \neq j], \ldots$$

For each such ρ we define a function Q_ρ by

$$Q_\rho(x) = \frac{(x^{n_0} - 1) \cdot \prod_{i<j}(x^{n_{ij}} - 1) \cdots}{\prod_i (x^{n_i} - 1) \cdot \prod_{i<j<k}(x^{n_{ijk}} - 1) \cdots}. \tag{9}$$

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

$$Q_{\{p,q\}}(x) = \frac{(x^{pq}-1)(x-1)}{(x^p-1)(x^q-1)}. \tag{10}$$

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,

$$Q_\rho(x) = x^d Q_\rho(\frac{1}{x}). \tag{11}$$

If all elements of ρ are prime, then comparison of (9) with (3) shows that

$$Q_\rho(x) = \Phi_{r_1 r_2 \cdots r_s}(x). \tag{12}$$

If n is an arbitrary integer and $\gamma(n) = p_1 \cdots p_s$ its squarefree kernel, then by (4) and (12) we have $Q_{\{p_1,\ldots,p_s\}}(x^{n/\gamma(n)}) = \Phi_n(x)$ and hence inclusion-exclusion polynomials generalize cyclotomic polynomials. They can be expressed as products of cyclotomic polynomials.

Theorem 3 [1]. *Given $\rho = \{r_1, \ldots, r_s\}$ let*

$$D_\rho = \{d : d | \prod_i r_i \text{ and } (d, r_i) > 1 \text{ for all } i\}.$$

Then we have $Q_\rho(x) = \prod_{d\in D_\rho} \Phi_d(x)$.

`Example`. We have $Q_{\{4,7\}} = \Phi_{28}\Phi_{14}$.

2.1 Binary inclusion-exclusion polynomials: a close-up

Lam and Leung [7] discuss binary cyclotomic polynomials Φ_{pq} in detail, with p and q primes. Now let $p, q > 1$ be positive coprime integers. All arguments in their paper easily generalize to this setting (instead of taking ξ to be a primitive pqth-root of unity as they do, one has to take ζ a pqth root of unity satisfying $\zeta^p \neq 1$ and $\zeta^q \neq 1$). One finds that

$$Q_{\{p,q\}}(x) = \sum_{i=0}^{\rho-1} x^{ip} \sum_{j=0}^{\sigma-1} x^{jq} - x^{-pq} \sum_{i=\rho}^{q-1} x^{ip} \sum_{j=\sigma}^{p-1} x^{jq}, \tag{13}$$

where ρ and σ are the (unique) non-negative integers for which $1 + pq = \rho p + \sigma q$. On noting that upon expanding the products in identity (13), the resulting monomials are all different, we arrive at the following result.

Lemma 1 *Let $p, q > 1$ be coprime integers. Let ρ and σ be the (unique) non-negative integers for which $1 + pq = \rho p + \sigma q$. 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 inclusion-exclusion coefficient $a_{\{p,q\}}(m)$ equals*

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

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

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

Using Lemma 1 it is easy to determine the midterm coefficient of $Q_{\{p,q\}}(x)$. This extends a result of Sister Beiter [3].

Proposition 1 *We have $a_{\{p,q\}}((p-1)(q-1)/2) = (-1)^{\rho-1}$.*

Proof. Left as an exercise to the interested reader, cf. Sister Beiter [3] or Lam and Leung [7]. □

3 Two proofs of the main (folklore) result

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

Theorem 4 *Let $p, q > 1$ be coprime integers, then $P_{S(p,q)}(x) = Q_{\{p,q\}}(x)$.*

Corollary 2 *We have*

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

Corollary 3 *The non-zero coefficients of $Q_{\{p,q\}}$ alternate between 1 and -1.*

Our first proof will make use of 'what is probably the most versatile tool in numerical semigroup theory' [13, p. 8], namely Apéry sets.

First proof of Theorem 4. The *Apéry set* of S with respect to a nonzero $m \in S$ is defined as

$$\mathrm{Ap}(S; m) = \{s \in S : s - m \notin S\}.$$

Note that

$$S = \mathrm{Ap}(S; m) + m\mathbb{Z}_{\geq 0}$$

and that $\mathrm{Ap}(S; m)$ consists of a complete set of residues modulo m. Thus we have

$$H_S(x) = \sum_{w \in \mathrm{Ap}(S;m)} x^w \sum_{i=0}^{\infty} x^{mi} = \frac{1}{1-x^m} \sum_{w \in \mathrm{Ap}(S;m)} x^w, \tag{14}$$

cf. [11, (4)]. Note that if $S = \langle a_1, \ldots, a_n \rangle$, then $\mathrm{Ap}(S; a_1) \subseteq \langle a_2, \ldots, a_n \rangle$. It follows that $\mathrm{Ap}(S(p,q); p)$ consists of multiples of q. The latter set equals the minimal set of multiples of q representing every congruence class modulo p and hence $\mathrm{Ap}(S(p,q); p) = \{0, q, \ldots, (p-1)q\}$. Hence

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

Using this identity and (10) the proof is easily completed. □

Our second proof uses the denumerant (see [10, Chapter 4] for a survey) and starting point is the observation that

$$\frac{1}{(1-x^p)(1-x^q)}=\sum_{j\ge 0} r(j)x^j, \tag{15}$$

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

Lemma 2 *Suppose that $k\ge 0$, then $r(k+pq)=r(k)+1$.*

Proof. Put $\alpha\equiv kp^{-1}(\text{mod } q)$, $0\le\alpha<q$ and $\beta\equiv kq^{-1}(\text{mod } p)$, $0\le\beta<p$ 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 $t\ge 0$ and we have $r(k)=1+t$, where we use that

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

We see that $r(k+pq)=1+t+1=r(k)+1$. □

`Remark`. It is not difficult to derive an explicit formula for $r(n)$ (see, e.g., [2, Section 1.3] or [8, pp. 213-214]). Let p^{-1},q^{-1} denote inverses of p modulo q, respectively q modulo p. Then we have

$$r(n)=\frac{n}{pq}-\{\frac{p^{-1}n}{q}\}-\{\frac{q^{-1}n}{p}\}+1,$$

where $\{x\}$ denote the fractional-part function. Note that Lemma 2 is a corollary of this formula.

Second proof of Theorem 4. From Lemma 2 we infer that

$$\begin{aligned}(1-x^{pq})\sum_{j\ge 0}r(j)x^j &= \sum_{j=0}^{pq-1}r(j)x^j+\sum_{j=pq}^{\infty}(r(j)-r(j-pq))x^j\\ &= \sum_{j=0}^{pq-1}r(j)x^j+\sum_{j\ge pq}x^j=\sum_{j\in S(p,q)}x^j,\end{aligned}$$

where we used that $r(j)\le 1$ for $j<pq$ and $r(j)\ge 1$ for $j\ge pq$. Using this identity and (15) the proof is easily completed. □

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. [10, 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., [13, Corollary 4.7]).

Theorem 5 *A numerical semigroup of embedding dimension* 2 *is symmetric.*

Proof. A numerical semigroup S of embedding dimension 2 is of the form $S = S(p,q)$ with $p, q > 1$ coprime integers. Suppose that $s \in S \cap (F(S) - S)$, 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 $F(S) - S$, it is enough to show that

$$H_{S'}(x) + x^{F(S)} H_{S'}(1/x) = 1 + x + \ldots + x^{F(S)}, \tag{16}$$

where

$$H_{S'}(x) = \sum_{0 \leq j \leq F(S),\ j \in S} x^j.$$

On noting that

$$H_{S'}(x) + \frac{x^{F(S)+1}}{1-x} = H_S(x),$$

we obtain from Theorem 4 that

$$H_{S'}(x) = \frac{Q_{\{p,q\}}(x) - x^{F(S)+1}}{1-x}. \tag{17}$$

By Theorem 4, (11) and (1) we obtain that $Q_{\{p,q\}}(1/x) x^{F(S)+1} = Q_{\{p,q\}}(x)$. From this identity and (17) we infer that

$$x^{F(S)} H_{S'}(1/x) = \frac{1 - Q_{\{p,q\}}(x)}{1-x}. \tag{18}$$

On adding (17) and (18), we see that (16) holds. □

From (18) and (16) we infer that

$$\sum_{0 \leq j \leq F(S),\ j \notin S} x^j = \frac{1 - Q_{\{p,q\}}(x)}{1-x}. \tag{19}$$

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 $G(S)$. From (1) and Theorem 1 and (10) we infer the following well-known result due to Sylvester:

$$F(S(p,q)) = pq - p - q. \tag{20}$$

For four different proofs and more background see [10, pp. 31-34], the shortest proof of (20) and (21) the author knows of is in the book by Wilf [18, p. 88]. From equation (16) we infer that $2N(S) = F(S) + 1$. Thus we obtain another well-known result of Sylvester:

$$N(S(p,q)) = (p-1)(q-1)/2. \tag{21}$$

Indeed, it is well-known that S is symmetric iff $2N(S) = F(S) + 1$; cf. [10, Lemma 7.2.3] or [13, Corollary 4.7].

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 (21) we have $\sigma_0(p,q) = (p-1)(q-1)/2$. Next we will compute $\sigma_1(p,q)$, following Brown and Shiue [4].

Theorem 6 [4]. *Let $p, q > 1$ be coprime integers. We have*

$$\sigma_1(p,q) = \frac{1}{12}(p-1)(q-1)(2pq - p - q - 1).$$

Proof. Let us denote the right hand side of (19) by $f(x)$. We have $\sigma_1(p,q) = f'(1)$. Put $y = x^p$. On rewriting $Q_{\{p,q\}}(x)$ as

$$Q_{\{p,q\}}(x) = \frac{\sum_{k=0}^{q-1} y^k}{\sum_{k=0}^{q-1} x^k},$$

we can write

$$f(x) = \frac{\sum_{k=0}^{q-1} x^k - \sum_{k=0}^{q-1} y^k}{(1-x)\sum_{k=0}^{q-1} x^k} = \frac{\sum_{k=1}^{q-1} \frac{y^k - x^k}{x-1}}{\sum_{k=0}^{q-1} x^k} = \frac{g(x)}{h(x)},$$

where

$$g(x) = \sum_{k=1}^{q-1} \frac{y^k - x^k}{x-1} = \sum_{k=1}^{q-1} (x^k + x^{k+1} + \cdots + x^{pk-1}), \ h(x) = \sum_{k=0}^{q-1} x^k.$$

Easy calculations now yield $g(1), g'(1), h(1)$ and $h'(1)$. Finally, we get

$$\sigma_1(p,q) = f'(1) = \frac{h(1)g'(1) - g(1)h'(1)}{h(1)^2} = \frac{1}{12}(p-1)(q-1)(2pq - p - q - 1),$$

completing the proof. $\square$

Using (19) it is not difficult to give a formula for $\sigma_k(p,q)$. On putting $x = e^z$ and recalling the Taylor series expansion $e^z = \sum_{k\ge 0} z^k/k!$ we obtain from (19) the identity

$$\sum_{k=0}^{\infty} \sigma_k(p,q)\frac{z^k}{k!} = \frac{e^{abz}-1}{(e^{az}-1)(e^{bz}-1)} - \frac{1}{e^z-1}. \tag{22}$$

We obtain from (22) on multiplying by z and using the Taylor series expansion (6) that

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

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

Theorem 7 [12]. *For $m \ge 1$ we have*

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

Using this formula we find e.g. that $\sigma_2(p,q) = \frac{1}{12}(p-1)(q-1)pq(pq-p-q)$. The proof we have given here of Theorem 7 is due to Rødseth [12], with the difference that we gave a different proof of the identity (22).

By using the formula (8) for power sums we obtain from Theorem 7 the identity

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

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

$$\sum_{n\notin S}(f(n+p) - f(n)) = \sum_{n=1}^{p-1}(f(nq) - f(n)),$$

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

$$\prod_{n\notin S(p,q)}(n+p) = q^{p-1}\prod_{n\notin S(p,q)} n.$$

Wang and Wang [16] obtained results similar to those of Tuenter for the *alternate Sylvester sums* $\sum_{s\notin S(p,q)}(-1)^s s^k$.

6 A reproof of Theorem 2

For $S(4,7)$ the gaps are given by $1,2,3,5,6,9,10,13$ and 17. One could try to break this down in terms of blocks of consecutive gaps ('gap blocks'): $\{1,2,3\}$, $\{5,6\}$, $\{9,10\}$, $\{13\}$ 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 3
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., $0=s_0<s_1<s_2<\ldots$. Since $s_0=0$ and $s_1=m(S)$ we have $g(G(S))\ge m(S)-1$. Since all multiples of $m(S)$ are in S, it follows that actually $g(G(S))=m(S)-1$.
2) If $g(S)\ge m(S)$, it would imply that we can find $k,k+1,\ldots,k+m(S)-1$ all in S such that furthermore $k+m(S)\notin S$, a contradiction.
3) If S is symmetric we clearly have $g(S)=g(G(S))=m(S)-1$. □
`Remark`. The second observation was made by my intern Alexandru Ciolan. It allows one to prove Theorem 10.

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

Theorem 8 *Let p,q,ρ and σ be as in Lemma 1. Put $S=S(p,q)$. There are $\rho\sigma-1$ gap blocks and $\rho\sigma-1$ element blocks.*

Proof. Let s be the number of gap blocks. We can write $G(S)$ as a union of the form

$$G(S)=\cup_{i=1}^{s}\{m_i,\ldots,p_i\},\ \text{with } m_1<m_2<\ldots<m_s. \tag{23}$$

By Theorem 4 we then find that

$$Q_{\{p,q\}}(x)=1+\sum_{i=1}^{s}(x^{p_i+1}-x^{m_i}). \tag{24}$$

It follows that s is equal to the number of negative coefficients in $Q_{\{p,q\}}(x)$, which by Corollary 1 equals $\rho\sigma-1$. On using that S is symmetric (Theorem 5) it follows that the number of element blocks equals the number of gap blocks. □

Finally, we will generalize a result of Hong et al. [6].

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

Proof. Using (23) we see 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 3 equals $m(S(p,q))-1=\min\{p,q\}-1$. □

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 3 we infer that $g(P_S(x))=\max\{g(S),g(G(S))\}=m(S)-1$. □

Problem 1 *Characterize the set of numerical semigroups for which*

$$g(S)=m(S)-1.$$

Examples show that this set is strictly contained in the set of all numerical semigroups and strictly larger than the set of symmetric numerical semigroups.

Acknowledgement. I like to thank Matthias Beck, Alexandru Ciolan, Pedro A. Garcia-Sánchez, Nathan Kaplan, Bernd Kellner, Jorge Ramírez Alfonsín and Ali Sinan Sertoz for helpful comments. Alexandru Ciolan pointed out to me that $g(S)\le m(S)-1$ 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] M. Beiter, The midterm coefficient of the cyclotomic polynomial $F_{pq}(x)$, *Amer. Math. Monthly* **71** (1964), 769–770.

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

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

[6] H. Hong, E. Lee, H.-S. Lee and C.-M. Park, Maximum gap in (inverse) cyclotomic polynomial, *J. Number Theory* **132** (2012), 2297–2315.

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

[8] 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.

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

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

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

[12] 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.

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

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

[15] 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.

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

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

[18] 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`