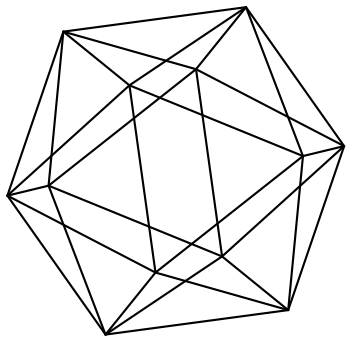
Max-Planck-Institut für Mathematik
Bonn

Cyclotomic numerical semigroup polynomials with few irreducible factors

by

Alessio Borzì
Andrés Herrera-Poyatos
Pieter Moree



Max-Planck-Institut für Mathematik
Preprint Series 2021 (6)

Date of submission: February 3, 2021

Cyclotomic numerical semigroup polynomials with few irreducible factors

by

Alessio Borzì
Andrés Herrera-Poyatos
Pieter Moree

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

Mathematics Institute
University of Warwick
Coventry CV4 7AL
UK

Department of Computer Science
University of Oxford
Wolfson Building
Parks Road
Oxford OX1 3QD
UK

MPIM 21-6

Cyclotomic numerical semigroup polynomials with few irreducible factors

Alessio Borzì, Andrés Herrera-Poyatos, Pieter Moree

February 3, 2021

Abstract

A numerical semigroup S is cyclotomic if its semigroup polynomial P_S is a product of cyclotomic polynomials. The number of irreducible factors of P_S (with multiplicity) is the polynomial length $\ell(S)$ of S. We show that a cyclotomic numerical semigroup is complete intersection if $\ell(S) \leq 2$. This establishes a particular case of a conjecture of Ciolan, García-Sánchez and Moree (2016) claiming that every cyclotomic numerical semigroup is complete intersection. In addition, we investigate the relation between $\ell(S)$ and the embedding dimension of S.

1 Introduction

The n-th cyclotomic polynomial is the minimal polynomial of any primitive n-th root of unity

$$\Phi_n(x) = \prod_{\substack{j=1 \\ (j,n)=1}}^{n} \left(x - e^{2\pi i j/n}\right) = \sum_{k=0}^{\varphi(n)} a_n(k) x^k, \tag{1}$$

where φ is Euler's totient function. Its coefficients $a_n(k)$ are integers.

Let $\mathbb{N}$ denote the non-negative integers. A *numerical semigroup* S is an additive submonoid of $\mathbb{N}$ with finite complement $\mathbb{N} \setminus S$. The *semigroup polynomial* of S is defined by $\mathrm{P}_S(x) = 1 + (x-1)\sum_{g \in \mathbb{N}\setminus S} x^g$. If $p \neq q$ are primes and $\langle p, q\rangle$ is the numerical semigroup generated by p and q, then

$$\Phi_{pq} = \mathrm{P}_{\langle p,q\rangle}, \tag{2}$$

see for instance [10]. This identity can be used to reprove various properties of cyclotomic polynomials, e.g., that $a_{pq}(k) \in \{0, 1, -1\}$, a result due to Migotti [9]. More generally, if p and q are two coprime non-negative integers, then $\mathrm{P}_{\langle p,q\rangle}$ is a product of cyclotomic polynomials. There are various other interesting infinite families of numerical semigroups such that their semigroup polynomial has only cyclotomic factors. These facts led Ciolan, García-Sánchez and Moree [10] to define *cyclotomic numerical semigroups* as numerical semigroups whose semigroup polynomial is a product of cyclotomic polynomials. For this family of numerical semigroups it is easy to see that the following implications hold:

$$\text{complete intersection} \implies \text{cyclotomic} \implies \text{symmetric} \tag{3}$$

(see Section 2.4). The converse of the second implication of (3) is far from true. In fact, for any odd integer F with $F \geq 9$, there is a numerical semigroup with Frobenius number F that

is symmetric and non-cyclotomic. This was proven independently by García-Sánchez (in the appendix of [7]), Herrera-Poyatos and Moree [7] and Sawhney and Stoner [13]. In the latter two papers it is shown (by quite different methods) that, for every $k \geq 5$, the polynomial

$$1 - x + x^k - x^{2k-1} + x^{2k},$$

which is the semigroup polynomial of the symmetric numerical semigroup $S_k = \langle k, k+1, \ldots, 2k-2 \rangle$, is not a product of cyclotomic polynomials. Therefore, S_k is symmetric, but not cyclotomic. It was conjectured by Ciolan, García-Sánchez and Moree [4] that the converse of the first implication in (3) holds true, more precisely they made the following conjecture.

Conjecture 1.1. [4, Conjecture 1]. *A numerical semigroup S is cyclotomic if and only if it is complete intersection.*

Using the GAP package [5] the authors of [4] verified that Conjecture 1.1 holds true for numerical semigroups with Frobenius number up to 70. Further, in the context of graded algebras, Borzì and D'Alì [2] prove a version of Conjecture 1.1 for Koszul algebras and for graded algebras that have an irreducible h-polynomial.

In this paper we classify all cyclotomic numerical semigroups such that their semigroup polynomial has at most two irreducible polynomial factors.

Theorem 1.2. *Let S be a cyclotomic numerical semigroup.*

1. *If P_S is irreducible, then $S = \langle p, q \rangle$ with $p \neq q$ primes and $\mathrm{P}_S = \Phi_{pq}$.*
2. *If P_S is a product of two irreducible polynomials, then either*
   (a) *$S = \langle p, q^2 \rangle$ with p, q distinct primes and $\mathrm{P}_S = \Phi_{pq}\Phi_{pq^2}$; or*
   (b) *$S = \langle p, q^2, qr \rangle$ with p, q, r distinct primes such that $p \in \langle q, r \rangle$ and $\mathrm{P}_S = \Phi_{pq}\Phi_{q^2r}$.*

As a byproduct, since the numerical semigroups obtained in Theorem 1.2 are easily seen to be complete intersections with the help of gluings (see Section 2), Conjecture 1.1 holds true in the cases studied in Theorem 1.2.

Theorem 1.3. *Suppose that the semigroup polynomial P_S has at most two irreducible factors. Then S is cyclotomic if and only if it is complete intersection.*

Theorem 1.2 motivates the following definition. We define the *polynomial length* $\ell(S)$ of S as the number of irreducible factors of P_S (with multiplicity). We study this quantity in Section 5.1.

Our paper is organised as follows. In Section 2 we gather some preliminary material that is partly expository and will be useful further on. In Section 3 we prove part 1 of Theorem 1.2, and in Section 4 we prove part 2. Finally, in Section 5 we pose some conjectures involving the polynomial length of cyclotomic numerical semigroups.

The computer algebra computations in this paper were done by using Macaulay2 [6], the GAP system [11] and, in particular, the NumericalSgps package [5].

2 Preliminaries

2.1 Numerical semigroups and Hilbert series

For an introduction to numerical semigroups, see [12].

Let S be a numerical semigroup. The *embedding dimension* $\mathrm{e}(S)$ of S is the cardinality of the (unique) minimal generating system of S. The *Frobenius number* of S is $\mathrm{F}(S) = \max(\mathbb{N} \setminus S)$. For example, if $S = \langle a, b\rangle$ with $b > a > 1$ coprime integers, then $\mathrm{F}(S)+1 = (a-1)(b-1)$ (see for instance [12, Proposition 2.13]). This fact in combination with the observation that if $T \subseteq S$ are two numerical semigroups, then clearly $\mathrm{F}(S) \leq \mathrm{F}(T)$, proves the following lemma.

Lemma 2.1. *If $a, b \in S$ with $\gcd(a, b) = 1$, then $\mathrm{F}(S) + 1 \leq (a-1)(b-1)$.*

The *Hilbert series* of S is

$$\mathrm{H}_S(x) = \sum_{s\in S} x^s \in \mathbb{Z}[[x]],$$

and the *semigroup polynomial* of S is

$$\mathrm{P}_S(x) = (1-x)\mathrm{H}_S(x) = 1 + (x-1)\sum_{g\in\mathbb{N}\setminus S} x^g. \tag{4}$$

Note that $\deg \mathrm{P}_S = \mathrm{F}(S) + 1$. The second equality in (4) easily follows from $\mathrm{H}_S(x) + \sum_{g\in\mathbb{N}\setminus S} x^g = 1/(1-x)$, where here and in the sequel we work in $\mathbb{Z}[[x]]$ and use the shorthand $1/(1-x)$ for $1 + x + x^2 + x^3 + \cdots$.

Some properties of a numerical semigroup, such as symmetry, can be captured in terms of its semigroup polynomial. We need some notation in order to characterize symmetry in this way. A numerical semigroup S is *symmetric* if for every integer n we have that $n \in S$ if and only if $\mathrm{F}(S) - n \notin S$. A polynomial $f(x) = \sum_{i=0}^{d} \alpha_i x^i \in \mathbb{Z}[x]$ is *palindromic* (or *self-reciprocal*) if $f(x) = x^d f(x^{-1})$, that is, its coefficients satisfy the relation $\alpha_{d-i} = \alpha_i$.

Theorem 2.2. [10, Theorem 5]. *A numerical semigroup S is symmetric if and only if P_S is palindromic.*

2.2 Complete intersection numerical semigroups

Let S_1, S_2 and S be numerical semigroups, and let $a_1 \in S_2$ and $a_2 \in S_1$ be coprime integers such that they are not minimal generators of their respective semigroups. We say that S is *the gluing* of S_1 and S_2 at a_1a_2 if $S = a_1S_1 + a_2S_2$ and we write $S = a_1S_1 +_{a_1a_2} a_2S_2$. We will keep this notation until the end of this section. By [12, Lemma 9.8] we have that

$$\mathrm{e}(S) = \mathrm{e}(S_1) + \mathrm{e}(S_2). \tag{5}$$

Let M be a submonoid of $\mathbb{N}$, and let $m \in M$. The *Apéry set* of M at m is the set

$$\mathrm{Ap}(M, m) = \{v \in M : v - m \notin M\}.$$

Gluings can be characterised in terms of Apéry sets as in Lemma 2.3.

Lemma 2.3. [12, Theorem 9.2]. *The numerical semigroup S is the gluing of S_1 and S_2 at $m = a_1a_2$, if and only if the map*

$$\mathrm{Ap}(a_1S_1, m) \times \mathrm{Ap}(a_2S_2, m) \to \mathrm{Ap}(S, m)$$

given by $(v, w) \mapsto v+w$ is bijective. If this is the case, then we have $\mathrm{Ap}(S, m) = \mathrm{Ap}(a_1S_1, m)+ \mathrm{Ap}(a_2S_2, m)$.

Gluings can also be characterized in terms of semigroup polynomials on using

$$\sum_{w\in \mathrm{Ap}(S,m)} x^w = (1-x^m)\,\mathrm{H}_S(x), \tag{6}$$

which follows from $S = \mathrm{Ap}(S,m) + m\mathbb{N}$.

Proposition 2.4 ([1, Corollary 4.4])**.** *The following statements are equivalent:*

1. $S = a_1S_1 +_{a_1a_2} a_2S_2$;
2. $\mathrm{H}_S(x) = (1-x^{a_1a_2})\mathrm{H}_{S_1}(x^{a_1})\mathrm{H}_{S_2}(x^{a_2})$;
3. $\mathrm{P}_S(x) = \mathrm{P}_{\langle a_1,a_2\rangle}(x)\mathrm{P}_{S_1}(x^{a_1})\mathrm{P}_{S_2}(x^{a_2})$.

Proof. The equivalence of (2) and (3) is trivial, so we just need to prove the equivalence of (1) and (2). From Lemma 2.3 we infer that $S = a_1S_1 +_{a_1a_2} a_2S_2$ if and only if

$$\sum_{w\in \mathrm{Ap}(S,a_1a_2)} x^w = \sum_{w_1\in \mathrm{Ap}(a_1S_1,a_1a_2)} \sum_{w_2\in \mathrm{Ap}(a_2S_2,a_1a_2)} x^{w_1+w_2} =$$

$$= \left(\sum_{w_1\in \mathrm{Ap}(S_1,a_2)} x^{a_1w_1}\right)\left(\sum_{w_2\in \mathrm{Ap}(S_2,a_1)} x^{a_2w_2}\right).$$

Now apply (6) and divide both sides by $1-x^{a_1a_2}$. □

Complete intersection numerical semigroups are usually introduced in the context of minimal presentations [12, Chapter 8], where a numerical semigroup S is said to be *complete intersection* if the cardinality of a minimal presentation of S is equal to $\mathrm{e}(S)-1$. In this paper we will only need the recursive characterisation of complete intersection numerical semigroups in terms of gluings.

Theorem 2.5. [12, Theorem 9.10]. *A numerical semigroup is complete intersection if and only if S is $\mathbb{N}$ or S is a gluing of two complete intersection numerical semigroups.*

Using this characterisation in terms of gluings along with Proposition 2.4 one can determine the Hilbert series of S as follows.

Corollary 2.6 ([1, Theorem 4.8])**.** *Let $S = \langle n_1,\dots,n_e\rangle$ be a complete intersection numerical semigroup. Then there are $d_1,\dots,d_{e-1} \in S\setminus\{n_1,\dots,n_e\}$ such that*

$$\mathrm{H}_S(x) = \frac{(1-x^{d_1})\dots(1-x^{d_{e-1}})}{(1-x^{n_1})\dots(1-x^{n_e})}.$$

The integers d_i in the previous result are actually the *Betti elements* of S (with multiplicity). We refer to [12, Chapter 7] for a definition of Betti element, which will not be needed in the remainder of this paper. If $\mathrm{e}(S)=2$, so $S = \langle a,b\rangle = a\mathbb{N} +_{ab} b\mathbb{N}$, then Corollary 2.6 and the fact that $\deg \mathrm{P}_S = \mathrm{F}(S) = (a-1)(b-1)$ yield

$$\mathrm{P}_{\langle a,b\rangle}(x) = \frac{(1-x)(1-x^{ab})}{(1-x^a)(1-x^b)}. \tag{7}$$

In the case when $\mathrm{e}(S)=3$, we have the following result due to Herzog.

Theorem 2.7. [8, Theorem 4.2.1]. *Let S be a numerical semigroup. If $\mathrm{e}(S)=3$, then S is complete intersection if and only if it is symmetric.*

2.3 Cyclotomic polynomials

For an introduction to cyclotomic polynomials, see [15].

From the definition (1) we have

$$x^n - 1 = \prod_{d|n} \Phi_d(x). \tag{8}$$

This in combination with (7) yields for example that

$$\mathrm{P}_{\langle a,b\rangle} = \prod_{d|ab,\ d\nmid a,\ d\nmid b} \Phi_d. \tag{9}$$

An important property of the cyclotomic polynomials is that they are irreducible over the rationals, several famous mathematicians gave different proofs of this, cf. Weintraub [16]. Hence, (8) gives the factorization of $x^n - 1$ into irreducibles.

By the so called *Möbius inversion formula* (see [14, Proposition 3.7.1]) we infer from (8) that

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}, \tag{10}$$

where the *Möbius function* μ is defined by

$$\mu(n) = \begin{cases} 1 & n = 1; \\ (-1)^k & n = p_1 \cdots p_k \text{ with the } p_i \text{ distinct primes}; \\ 0 & \text{otherwise.} \end{cases}$$

By taking degrees we obtain $\varphi(n) = \sum_{d|n} d\mu(n/d)$. If $n > 1$, then $\sum_{d|n} \mu(n/d) = 0$, so equation (10) can be rewritten as

$$\Phi_n(x) = \prod_{d|n} (1 - x^d)^{\mu(n/d)}. \tag{11}$$

Recall that a polynomial f of degree d is palindromic if $f(x) = x^d f(x^{-1})$. As, for $n > 1$,

$$x^{\varphi(n)} \Phi_n(\frac{1}{x}) = x^{\sum_{d|n} d\mu(n/d)} \prod_{d|n} \big(1 - \frac{1}{x^d}\big)^{\mu(n/d)} = \prod_{d|n} (x^d - 1)^{\mu(n/d)} = \Phi_n(x), \tag{12}$$

we see that $\Phi_n(x)$ is palindromic for $n > 1$.

It follows from (11) that for $n > 1$ we have $\Phi_n(0) = 1$ and

$$\Phi_n(x) \equiv 1 - \mu(n)x \pmod{x^2}. \tag{13}$$

Let r be any natural number. It can also be deduced from (11) that

$$\Phi_{nr^2}(x) = \Phi_{nr}(x^r). \tag{14}$$

2.4 Cyclotomic numerical semigroups

A numerical semigroup S is *cyclotomic* if P_S is a product of cyclotomic polynomials, that is, $\mathrm{P}_S = \prod_{d\in\mathcal{D}} \Phi_d^{f_d}$, for some finite set $\mathcal{D}$, with $f_d \geq 1$. As $\mathrm{P}_S(1) = 1$, Φ_1 does not appear in this product.

Corollary 2.6 gives rise to the following result of Ciolan et al. [4].

Corollary 2.8. *Every complete intersection numerical semigroup is cyclotomic.*

Proof. By Corollary 2.6 and (8) we have $\mathrm{P}_S = (1-x)H_S(x) = \prod \Phi_n^{f_n}$, with possibly $f_n < 0$. However, this would imply that $\mathrm{P}_S(x)$ has a pole at $x = e^{2\pi i/n}$, contradicting the fact that P_S is a polynomial. □

Observe that the product of two palindromic polynomials is palindromic. Hence, by applying Theorem 2.2 and recalling that Φ_n is palindromic for $n > 1$ (see Section 2.3), we reach the following conclusions.

Corollary 2.9 ([4, Theorem 1])**.** *Every cyclotomic numerical semigroup is symmetric.*

Corollary 2.10 ([4, Lemma 7])**.** *Conjecture 1.1 holds true for those S with $\mathrm{e}(S) \leq 3$.*

Proof. This follows from Corollary 2.9 and Theorem 2.7. □

To conclude this section, we note that the cyclotomicity of numerical semigroups is preserved under gluing.

Corollary 2.11. *If S is the gluing of S_1 and S_2 at a_1a_2, then S is cyclotomic if and only if both S_1 and S_2 are cyclotomic.*

Proof. This follows from Proposition 2.4. □

3 Cyclotomic numerical semigroups of polynomial length 1

In this section we classify cyclotomic numerical semigroups having irreducible semigroup polynomial. They are given in Corollary 3.3.

Lemma 3.1. *Let S be a numerical semigroup such that Φ_n divides P_S for some n. If $p, q \in S$ are two different primes dividing n, then $S = \langle p, q\rangle$ and $\mathrm{P}_S = \Phi_{pq}$.*

Proof. Recall that $\deg \Phi_n = \varphi(n)$, see (1), and $\deg \mathrm{P}_S = \mathrm{F}(S) + 1$. Hence,

$$(p-1)(q-1) \leq \varphi(n) \leq \deg \mathrm{P}_S = \mathrm{F}(S) + 1.$$

By Lemma 2.1 with $a = p$ and $b = q$ it follows that

$$(p-1)(q-1) \leq \varphi(n) \leq \mathrm{F}(S) + 1 \leq (p-1)(q-1),$$

and we conclude that $\mathrm{P}_S = \Phi_n$ and $\varphi(n) = \varphi(pq)$. Writing $n = kpq$ we have $\varphi(pq) = \varphi(n) = \varphi(kpq) \geq \varphi(k)\varphi(pq)$ and hence $\varphi(k) = 1$, implying $k = 1$ or $k = 2$. Consequently, $n = pq$ or $n = 2pq$. From (13) and the equality $\mathrm{P}_S(x) \equiv \Phi_n(x) \pmod{x^2}$, we obtain $\mu(n) = 1$ and so $n = pq$ and hence $S = \langle p, q\rangle$. □

Theorem 3.2. *Let S be a numerical semigroup such that $\mathrm{P}_S(x) = \Phi_n(x^j)^h$. Then $S = \langle p, q\rangle$ with $p \neq q$ primes, $n = pq$ and $j = h = 1$.*

Proof. On the one hand we have $\mathrm{P}_S(x) \equiv 1 - x \pmod{x^2}$, and on the other $\Phi_n(x^j)^k \equiv 1 - \mu(n)hx^j \pmod{x^{2j}}$. We conclude that $\mu(n) = j = h = 1$, so $\mathrm{P}_S(x) = \Phi_n(x)$. From $1 = \mathrm{P}_S(1) = \Phi_n(1)$ we infer $n \geq 2$. Thus n is a product of an even number of distinct primes $p_1 < p_2 < \ldots < p_{2k}$, that is $n = p_1 \cdots p_{2k}$. From (11) and the fact that if $d|n$, then $\mu(n/d) = \mu(d)$, we obtain

$$\Phi_n(x) \prod_{\substack{d|n \\ \mu(d)=-1}} (1 - x^d) = \prod_{\substack{d|n \\ \mu(d)=1}} (1 - x^d). \tag{15}$$

Recall that $\Phi_n(x) = \mathrm{P}_S(x) = (1 - x)\mathrm{H}_S(x)$. On dividing both sides of (15) by $1 - x$ and reducing the resulting identity modulo x^{p_2+1}, we find that

$$(1 - x^{p_1})(1 - x^{p_2})\mathrm{H}_S(x) \equiv 1 \pmod{x^{p_2+1}},$$

which can be rewritten as

$$\mathrm{H}_S(x) \equiv 1 + x^{p_1}\mathrm{H}_S(x) + x^{p_2}\mathrm{H}_S(x) \pmod{x^{p_2+1}}.$$

We deduce that both p_1 and p_2 are in S. Consequently, we obtain $S = \langle p_1, p_2 \rangle$ by Lemma 3.1. □

Corollary 3.3 (Part 1 of Theorem 1.2)**.** *A cyclotomic numerical semigroup S has irreducible semigroup polynomial if and only if $S = \langle p, q \rangle$ for some distinct primes p and q. If this is the case, then $P_S = \Phi_{pq}$.*

4 Cyclotomic numerical semigroups of polynomial length 2

In this section we classify the cyclotomic numerical semigroups with polynomial length 2, as it was announced in part 2 of Theorem 1.2. As a consequence of this result, it follows that every cyclotomic numerical semigroup with polynomial length 2 is complete intersection. Our proof of part 2 of Theorem 1.2 uses the following three lemmas.

Lemma 4.1. *Let S be a cyclotomic numerical semigroup. Hence*

$$\mathrm{P}_S(x) = \prod_{d \in \mathcal{D}} \Phi_d(x)^{f_d}$$

for some finite set of positive integers $\mathcal{D}$ and positive integers f_d. Then we have

$$\sum_{d \in \mathcal{D}} f_d \mu(d) = 1.$$

In particular, there exists an integer $d > 1$ such that $\mu(d) = 1$ and $\Phi_d \mid \mathrm{P}_S$.

Proof. Since $\mathrm{P}_S(1) = 1$, we have $1 \notin \mathcal{D}$. In view of (13), we obtain

$$\mathrm{P}_S(x) \equiv 1 - x \sum_{d \in \mathcal{D}} f_d \mu(d) \pmod{x^2}.$$

Recalling that $\mathrm{P}_S(x) \equiv 1 - x \pmod{x^2}$, it follows that $1 = \sum_{d \in \mathcal{D}} f_d \mu(d)$, and also that there must be some integer $d > 1$ in $\mathcal{D}$ with $\mu(d) = 1$. □

Lemma 4.2. *Let S be a numerical semigroup such that*

$$\mathrm{P}_S(x) = \Phi_n(x) f(x^q) \tag{16}$$

for some integers $n, q > 1$ such that $\mu(n) = 1$ and $f(x) \in \mathbb{Z}[x]$ is of positive degree. Then q is a prime number and $n = pq$ for some other prime $p \in S$.

Proof. Since $\mu(n) = 1$ by assumption, we can write $n = p_1 \cdots p_{2k}$ with $p_1 < p_2 < \ldots < p_{2k}$ primes. Using (11) and reducing the resulting expression modulo x^{p_2+1} we obtain from (16)

$$\mathrm{H}_S(x)(1 - x^{p_1})(1 - x^{p_2}) \equiv f(x^q) \pmod{x^{p_2+1}},$$

which can be rewritten as

$$\mathrm{H}_S(x) \equiv f(x^q) + x^{p_1}\mathrm{H}_S(x) + x^{p_2}\mathrm{H}_S(x) \pmod{x^{p_2+1}}. \tag{17}$$

Since p_1 and p_2 can not belong to S at the same time by Lemma 3.1, we see that $f(x^q)$ contains a monomial with exponent p_1 or p_2. Consequently, q divides p_1 or p_2, that is, $q \in \{p_1, p_2\}$. Furthermore, if $p \in \{p_1, p_2\} \setminus \{q\}$, then q does not divide p and we find that $p \in S$ by (17). Note that $\{p_1, p_2\} = \{p, q\}$.

It remains to show that $n = p_1 p_2 = pq$. In order to obtain a contradiction we assume that $k > 1$. Using (11) and reducing the resulting expression modulo x^{p_3+1}, we obtain from (16)

$$\mathrm{H}_S(x)(1 - x^{p})(1 - x^{q})(1 - x^{p_3}) \equiv f(x^q)(1 - x^{pq}) \pmod{x^{p_3+1}},$$

which can be simplified to

$$\mathrm{H}_S(x) \equiv x^{p}\mathrm{H}_S(x) + x^{p_3}\mathrm{H}_S(x) + f(x^q)\frac{(1 - x^{pq})}{(1 - x^q)} \pmod{x^{p_3+1}}. \tag{18}$$

Note that

$$f(x^q)\frac{(1 - x^{pq})}{(1 - x^q)} = g(x^q),$$

for some $g(x) \in \mathbb{Z}[x]$. Since q does not divide p_3, we must have $p_3 \in S$ in view of (18). Since $p \in S$, we conclude by Lemma 3.1 with $a = p$ and $b = p_3$ that $S = \langle p, p_3 \rangle$ and hence $P_S = \Phi_{pp_3}$ is irreducible, whereas by assumption it has at least two irreducible factors. □

Lemma 4.3. *Let S be a numerical semigroup such that*

$$\mathrm{P}_S(x) = \Phi_{pq}(x)\Phi_l(x^q)$$

for some distinct prime numbers p and q, and l a multiple of q. Then either

1. *$S = \langle p, q^2 \rangle$ and $l = pq$; or*
2. *$S = \langle p, q^2, qr \rangle$ for some prime number r such that $r \notin \{p, q\}$ and $p \in \langle q, r \rangle$, and $l = qr$.*

Proof. We can write

$$\mathrm{H}_S(x) = \Phi_l(x^q)\frac{1 - x^{pq}}{(1 - x^q)(1 - x^p)} = \frac{\Phi_l(x^q)}{1 - x^q}\sum_{i=0}^{q-1} x^{ip}. \tag{19}$$

Note that $\Phi_l(x)/(1-x) \in \mathbb{Z}[[x]]$. We write it as $\sum_{j=0}^{\infty} a_j x^j$. We consider $S' = \{j \in \mathbb{N} : a_j \neq 0\}$. Since $\Phi_l(0) = 1$, it follows that $a_0 = 1$ and hence $0 \in S'$. We are going to prove that S' is a numerical semigroup with $\mathrm{P}_{S'} = \Phi_l$. Equation (19) can be rewritten in $\mathbb{Z}[[x]]$ as

$$\mathrm{H}_S(x) = \left(\sum_{j=0}^{\infty} a_j x^{jq}\right)\left(\sum_{i=0}^{q-1} x^{ip}\right) = \sum_{j=0}^{\infty} a_j \sum_{i=0}^{q-1} x^{jq+ip}. \tag{20}$$

Since p and q are prime numbers, if $jq+ip = j'q+i'p$ with $j, j' \in \mathbb{N}$ and $i, i' \in \{0, 1, \ldots, q-1\}$, then $i = i'$ and $j = j'$. Consequently, a_j is the qj-th coefficient of H_S and hence $a_j \in \{0, 1\}$. Note that $j \in S'$ if and only if $qj \in S$. Since S is a numerical semigroup, we see that S' is closed under addition. Furthermore, we have $(1-x)\mathrm{H}_{S'}(x) = \Phi_l(x)$. As a consequence, S' is a numerical semigroup with polynomial Φ_l. By Theorem 3.2 and the assumption $q \mid l$, we obtain $l = qr$, where r is a prime number different from q, and $S' = \langle q, r\rangle$. Summarizing, we have $\mathrm{P}_S(x) = \Phi_{pq}(x)\Phi_{qr}(x^q) = \Phi_{pq}(x)\Phi_{q^2r}(x)$, where we used (14), and $\mathrm{H}_S(x) = \mathrm{H}_{S'}(x^q)\sum_{i=0}^{q-1} x^{ip}$. From the latter equality, we obtain $S = qS' + p\mathbb{N}$. There are two possibilities:

- $r = p$. Then $\mathrm{P}_S = \Phi_{pq}\Phi_{pq^2} = \mathrm{P}_{\langle p, q^2\rangle}$, where in the latter equality we used (9). That is, $S = \langle p, q^2\rangle$.
- $r \neq p$. Then $S = q\langle r, q\rangle +_{qp} p\mathbb{N}$ is a gluing and, thus, $S = \langle p, q^2, qr\rangle$. □

Proof of part 2 of Theorem 1.2. By Lemma 4.1, our assumption $\ell(S) = 2$ implies that we can write $\mathrm{P}_S = \Phi_n\Phi_m$ with $\mu(n) = 1$ and $\mu(m) = 0$. Let q be the smallest prime such that $q^2 \mid m$ and put $l = m/q$. On applying (14) we find

$$\mathrm{P}_S(x) = \Phi_n(x)\Phi_l(x^q). \tag{21}$$

Note that $n, l > 1$. By Lemma 4.2 it now follows that $\mathrm{P}_S(x) = \Phi_{pq}(x)\Phi_l(x^q)$ for some prime $p \neq q$. The proof is completed on invoking Lemma 4.3 (note that $q \mid l$). □

5 Some interconnected conjectures

5.1 Polynomial length of cyclotomic numerical semigroups

Let S be a numerical semigroup. Recall that we define the *polynomial length* $\ell(S)$ of S as the number of irreducible factors of P_S (with multiplicity). If $q > p$ are two primes we have $\mathrm{P}_{\langle p,q\rangle}(x) = \Phi_{pq}(x)$ by (2) and hence the polynomial length of $\langle p, q\rangle$ is 1. This observation is generalized in Example 5.1. This example involves some more notation that we now introduce. Let $d(n) = \sum_{d|n} 1$ denote the number of positive divisors of n. We have $d(ab) \leq d(a)d(b)$ with equality if a and b are coprime. By $\mathrm{ir}(f)$ we denote the number of irreducible prime factors of f, and so $\ell(S) = \mathrm{ir}(P_S)$. A fundamental observation we will use is that

$$\mathrm{ir}(x^n - 1) = d(n) \tag{22}$$

(this is a consequence of (8) and the irreducibility of cyclotomic polynomials). Using this and (10) we obtain the (known) identity

$$\mathrm{ir}(\Phi_n) = 1 = \sum_{\delta|n} d(\delta)\mu(n/\delta).$$

If S is complete intersection with minimal generators $n_1, \ldots, n_e$, and Betti elements $b_1, \ldots, b_{e-1}$ (with multiplicity), then from Corollary 2.6 and (22) we have

$$\ell(S) = \sum_{j=1}^{e-1} d(b_j) - \sum_{j=1}^{e} d(n_j) + 1. \tag{23}$$

Example 5.1. Let $b > a > 1$ be coprime integers. The only Betti element of $\langle a, b\rangle$ is ab, see (7), so we have

$$\mathrm{ir}(P_{\langle a,b\rangle}(x)) = d(ab) - d(a) - d(b) + 1.$$

From (7) and the multiplicativity of the sum of divisors function d we find that

$$l(\langle a, b\rangle) = (d(a) - 1)(d(b) - 1).$$

If $S = a_1 S_1 +_{a_1 a_2} a_2 S_2$, then from Proposition 2.4 and the latter example, we obtain the inequality

$$\ell(S) \geq \ell(S_1) + \ell(S_2) + (d(a_1) - 1)(d(a_2) - 1). \tag{24}$$

Remark 5.2. This lower bound is sharp. Let $S_1 = \langle 2, 3\rangle$ and $S_2 = \langle 5, 7\rangle$. Recall that S_1 and S_2 have length 1 (Corollary 3.3). We consider the following gluing of S_1 and S_2, $S = 12\,\langle 2, 3\rangle + 5\,\langle 5, 7\rangle$. Then the polynomial of S is

$$\mathrm{P}_S(x) = \mathrm{P}_{\langle 12,5\rangle}(x)\Phi_6(x^{12})\Phi_{35}(x^5) = \mathrm{P}_{\langle 12,5\rangle}(x)\Phi_{72}(x)\Phi_{175}(x),$$

and $\ell(S) = (d(12) - 1)(d(5) - 1) + \ell(S_1) + \ell(S_2) = 7$.

Proposition 5.3. *If S is a complete intersection numerical semigroup, then we have* $\mathrm{e}(S) \leq \ell(S) + 1$.

Proof. We proceed by induction on $\mathrm{e}(S)$. If $\mathrm{e}(S) = 2$, then the result is trivial. Now let us assume that the result is true for every numerical semigroup with embedding dimension smaller than $\mathrm{e}(S) > 2$. The numerical semigroup S is a gluing of two complete intersection numerical semigroups S_1 and S_2 by Theorem 2.5. From (5), our induction hypothesis, and (24) we have

$$\mathrm{e}(S) = \mathrm{e}(S_1) + \mathrm{e}(S_2) \leq \ell(S_1) + \ell(S_2) + 2 \leq \ell(S) + 1. \qquad \square$$

The next result shows that the inequality in Proposition 5.3 is sharp.

Proposition 5.4. *Let $e \geq 2$ be an integer. For every $l \geq e - 1$ there exists a complete intersection numerical semigroup S such that $\ell(S) = l$ and* $\mathrm{e}(S) = e$.

Proof. For every $k \geq 1$, we inductively construct a family of numerical semigroups $S_k^{(e)}$, such that $e(S_k^{(e)}) = e$ and $\ell(S_k^{(e)}) = e + k - 2$, as follows:

- $S_k^{(2)} = \langle p_1^k, p_2\rangle$ for some distinct primes p_1 and p_2;
- $S_k^{(e+1)} = p_1 S_k^{(e)} +_{p_{e+1} p_1} p_{e+1}\mathbb{N}$ for some prime $p_{e+1} \in S_k^{(e)}$ that is not a minimal generator.

By (5) we conclude that

$$e(S_k^{(e)}) = e(S_k^{(e-1)}) + 1 = \cdots = e(S_k^{(2)}) + e - 2 = e.$$

From Proposition 2.4 we have $P_{S_k^{(e)}}(x) = P_{S_k^{(e-1)}}(x^{p_1})\Phi_{p_1p_e}(x)$. Applying this formula recursively we obtain

$$P_{S_k^{(e)}}(x) = P_{S_k^{(2)}}(x^{p_1^{e-2}}) \prod_{i=3}^{e} \Phi_{p_1p_i}(x^{p_1^{e-i}}).$$

Now, inserting $P_{S_k^{(2)}}(x) = \prod_{j=1}^{k} \Phi_{p_1^j p_2}(x)$, which follows by (9), and applying (14), we infer that

$$P_{S_k^{(e)}}(x) = \prod_{i=3}^{e} \Phi_{p_1^{e-i+1}p_i}(x) \prod_{j=1}^{k} \Phi_{p_1^{e+j-2}p_2}(x),$$

and hence $\ell(S_k^{(e)}) = e + k - 2$. □

Conjecture 5.5. *Let S be a cyclotomic numerical semigroup. Then*

$$\mathrm{e}(S) \leq \ell(S) + 1.$$

Using Proposition 5.3 we see that

$$\text{Conjecture 1.1} \implies \text{Conjecture 5.5}.$$

Assuming Conjecture 5.5 holds true, the proof of Theorem 1.2 can be greatly simplified. Namely, by assumption $\ell(S) \leq 2$, so we would have $\mathrm{e}(S) \leq \ell(S) + 1 \leq 3$ and hence S would be complete intersection by Corollary 2.10.

To conclude this section, we have computed all the cyclotomic numerical semigroups with Frobenius number at most 70, and classified them in terms of their polynomial length. These cyclotomic numerical semigroups are complete intersections, as it was computationally checked in [4], and there are 835 of them. The results are displayed in Table 1. The largest polynomial length found among these semigroups is 8. Recall that Sections 3 and 4 of the present paper study cyclotomic numerical semigroups of polynomial length at most 2, which add up to 138 semigroups out of the 835 found.

Table 1: Number of cyclotomic numerical semigroups with Frobenius number at most 70, grouped by their polynomial length.

Length	1	2	3	4	5	6	7	8
Number of semigroups	33	105	224	196	165	74	34	4

5.2 Cyclotomic exponent sequence

Let S be a numerical semigroup. Since $\mathrm{P}_S(0) = 1$, there exist unique integers e_j such that the formal identity

$$\mathrm{P}_S(x) = \prod_{j=1}^{\infty} (1 - x^j)^{e_j} \tag{25}$$

holds [3, Lemma 3.1]. The sequence $\mathbf{e} = \{e_j\}_{j\in\mathbb{N}}$ is known as the *cyclotomic exponent sequence* of S. This sequence was introduced in [4, Section 6] and later studied in [3]. From (25) and the uniqueness of the exponents $\mathbf{e}$, one can show that S is a cyclotomic numerical semigroup

if and only if $\mathbf{e}$ has only a finite number of non-zero elements, see [3, Proposition 2.4] for details. If this is the case, then, by (22), we obtain

$$\ell(S) = \sum_{j=1}^{\infty} e_j d(j).$$

This equality generalizes equation (23), which gives the length of a complete intersection numerical semigroup.

One of the main results of [3] is the following.

Theorem 5.6 ([3, Theorem 1.1])**.** *Let $S \neq \mathbb{N}$ be a numerical semigroup and let $\mathbf{e}$ be its cyclotomic exponent sequence. Then*

1. $e_1 = 1$;
2. $e_j = 0$ *for every* $j \geq 2$ *not in* S;
3. $e_j = -1$ *for every minimal generator* j *of* S;
4. $e_j = 0$ *for every* j *in* S *that has only one factorization and is not a minimal generator.*

As a consequence of this theorem, the set $\{n \in \mathbb{N} : e_n < 0\}$ is a system of generators of S. In the case of cyclotomic numerical semigroups, the authors of [3] made the following conjecture.

Conjecture 5.7 ([3, Conjecture 7.1])**.** *Let S be a cyclotomic numerical semigroup and let $\mathbf{e}$ be its cyclotomic exponent sequence. Then $n \in \mathbb{N}$ is a minimal generator of S if and only if $e_n < 0$.*

The cyclotomic exponent sequence of a complete intersection numerical semigroup can be easily obtained from Corollary 2.6. Note that for these semigroups the only integers with $e_n < 0$ are the minimal generators. Hence, as already noted in [3, Proposition 7.3], we have

$$\text{Conjecture 1.1} \implies \text{Conjecture 5.7}.$$

In the rest of this section we relate Conjectures 5.5 and 5.7. In order to do so, we formulate a further conjecture.

Conjecture 5.8. *Let S be a cyclotomic numerical semigroup. Hence*

$$\mathrm{P}_S(x) = \prod_{d \in \mathcal{D}} \Phi_d(x)^{f_d}$$

for some finite set of positive integers $\mathcal{D}$ and positive integers f_d. Let $\mathbf{e}$ the cyclotomic exponent sequence of S. Then

$$\{d \geq 2 : e_d > 0\} \subseteq \mathcal{D},$$

and $e_d \leq f_d$ for every $d \geq 2$ with $e_d > 0$.

In addition, we will need the following proposition, the proof of which we include for completeness.

Proposition 5.9 ([3, Proposition 2.3])**.** *Let S be a numerical semigroup and let $\mathbf{e}$ be its cyclotomic exponent sequence. If S is cyclotomic, then $\sum_{j \geq 1} e_j = 0$.*

Proof. Let N be the largest index j such that $e_j \neq 0$. Then we have

$$\mathrm{P}_S(x) = (1-x)^{\sum_{j\leq N} e_j} G_S(x),$$

for some rational function $G_S(x)$ satisfying $G_S(1) \notin \{0, \infty\}$ (in fact $G_S(1) = \prod_{j\leq N} j^{e_j}$). Since $\mathrm{P}_S(1) = 1$, it follows that $\sum_{j\geq 1} e_j = 0$. □

Proposition 5.10. *The following implications hold:*

$$\textit{Conjecture 1.1} \Longrightarrow \textit{Conjecture 5.7} \Longrightarrow \textit{Conjecture 5.8} \Longrightarrow \textit{Conjecture 5.5}.$$

Proof. The first implication follow from Corollary 2.6. Let S be a cyclotomic numerical semigroup and let $n_1, \ldots, n_e$ be its minimal generators. Let us assume that S satisfies Conjecture 5.7. Then we have

$$\prod_{i=1}^{e}(1-x^{n_i})\mathrm{P}_S(x) = \prod_{d\in\mathbb{N};\, e_d>0}(1-x^d)^{e_d}$$

Let $d \in \mathbb{N}$ with $e_d > 0$ and $d \geq 2$. We are going to prove that $\Phi_d^{e_d}$ divides P_S. Recall that $\Phi_d^{e_d}$ divides $(1-x^d)^{e_d}$ exactly. Now we argue that Φ_d does not divide $\prod_{i=1}^{e}(1-x^{n_i})$. Note that Φ_d divides $\prod_{i=1}^{e}(1-x^{n_i})$ if and only if there exists $i \in \{1, 2, \ldots, e\}$ such that d divides n_i. By Theorem 5.6 it follows that $d \neq n_i$ and $d \in S$. Since by assumption n_i is a minimal generator of S, we conclude that d does not divide n_i. This along with the fact that Φ_d is irreducible allows us to conclude that $\Phi_d^{e_d}$ divides P_S and, hence, $e_d \leq f_d$.

Now let us assume that S satisfies Conjecture 5.8. Since $\{d \in \mathbb{N} : e_d < 0\}$ is a (finite) system of generators of S by Theorem 5.6, we find that

$$\mathrm{e}(S) \leq \sum_{d\in\mathbb{N};\, e_d<0}(-e_d).$$

From Proposition 5.9, we obtain

$$\sum_{d\in\mathbb{N};\, e_d<0}(-e_d) = \sum_{d\in\mathbb{N};\, e_d>0} e_d.$$

Finally, because we are assuming that S satisfies Conjecture 5.8, we have

$$\sum_{d\in\mathbb{N};\, e_d>0} e_d \leq e_1 + \sum_{d\in\mathcal{D}} f_d = \ell(S) + 1.$$

We conclude that $\mathrm{e}(S) \leq \ell(S) + 1$. □

Acknowledgement. The authors thank Pedro A. García-Sánchez for putting the authors in contact with each other and for helpful conversations on this work.

References

[1] A. Assi, P. A. García-Sánchez, and I. Ojeda. Frobenius vectors, Hilbert series and gluings of affine semigroups. *J. Commut. Algebra*, 7(3):317–335, 2015.

[2] A. Borzì and A. D'Alì. Graded algebras with cyclotomic Hilbert series. *arXiv preprint arXiv:2005.09708*, 2020.

[3] A. Ciolan, P. García-Sánchez, A. Herrera-Poyatos, and P. Moree. Cyclotomic exponent sequences of numerical semigroups. *arXiv, to appear*, 2021.

[4] E.-A. Ciolan, P. A. García-Sánchez, and P. Moree. Cyclotomic numerical semigroups. *SIAM J. Discrete Math.*, 30(2):650–668, 2016.

[5] M. Delgado, P. A. García-Sánchez, and J. Morais. NumericalSgps. A package for numerical semigroups, Version 1.0.1. Available at http://www.gap-system.org/Packages/numericalsgps.html, 2015.

[6] D. R. Grayson and M. E. Stillman. Macaulay2, a software system for research in algebraic geometry. Available at http://www.math.uiuc.edu/Macaulay2/.

[7] A. Herrera-Poyatos and P. Moree. Coefficients and higher order derivatives of cyclotomic polynomials: old and new. *Expos. Math.*, 2020. https://doi.org/10.1016/j.exmath.2019.07.003.

[8] J. Herzog. Generators and relations of abelian semigroups and semigroup rings. *Manuscripta Math.*, 3:175–193, 1970.

[9] A. Migotti. Zur Theorie der Kreisteilungsgleichung. *S.-B. der Math.-Naturwiss. Class der Kaiser. Akad. der Wiss., Wien*, 87:7–14, 1883.

[10] P. Moree. Numerical semigroups, cyclotomic polynomials, and Bernoulli numbers. *Amer. Math. Monthly*, 121(10):890–902, 2014.

[11] The GAP Group. Gap–groups, algorithms, and programming, version 4.7.9. Available at http://www.gap-system.org, 2015.

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

[13] M. Sawhney and D. Stoner. On symmetric but not cyclotomic numerical semigroups. *SIAM J. Discrete Math.*, 32(2):1296–1304, 2018.

[14] R. P. Stanley. *Enumerative combinatorics. Volume 1*, volume 49 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 2012.

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

[16] S. H. Weintraub. Several proofs of the irreducibility of the cyclotomic polynomials. *Amer. Math. Monthly*, 120(6):537–545, 2013.

Alessio Borzì Alessio.Borzi@warwick.ac.uk
Mathematics Institute, University of Warwick, Coventry CV4 7AL, United Kingdom.

Andrés Herrera-Poyatos andres.herrerapoyatos@cs.ox.ac.uk
Department of Computer Science, University of Oxford, Wolfson Building, Parks Road, Oxford, OX1 3QD, United Kingdom.

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