NUMERICAL SEMIGROUPS AND APPLICATIONS

Abdallah Assi, Pedro A. García-Sánchez

NUMERICAL SEMIGROUPS AND APPLICATIONS

ABDALLAH ASSI AND PEDRO A. GARCÍA-SÁNCHEZ

Contents

Introduction

Numerical semigroups arise in a natural way in the study of nonnegative integer solutions to Diophantine equations of the form $a_1x_1 + \cdots + a_nx_n = b$, where $a_1, \ldots, a_n, b \in \mathbb{N}$ (here $\mathbb{N}$ denotes the set of nonnegative integers; we can reduce to the case $\gcd(a_1, \ldots, a_n) = 1$). Frobenius in his lectures asked what is the largest integer b such that this equation has no solution over the nonnegative integers, for the case $n = 2$. Sylvester and others solved this problem, and since then this has been known as the Frobenius problem (see [17] for an extensive exposure of this and related problems).

Other focus of interest comes from commutative algebra and algebraic geometry. Let $\mathbb{K}$ be a field and let $\mathbf{A} = \mathbb{K}[t^{a_1}, \ldots, t^{a_n}]$ be the $\mathbb{K}$-algebra of polynomials in $t^{a_1}, \ldots, t^{a_n}$. The ring $\mathbf{A}$ is the coordinate ring of the curve parametrized by $t^{a_1}, \ldots, t^{a_n}$, and information from $\mathbf{A}$ can be derived from the properties of the numerical semigroup generated by the exponents $a_1, \ldots, a_n$. Thus in many cases the names of invariants in numerical semigroups

The first author is partially supported by the project GDR CNRS 2945 and a GENIL-SSV 2014 grant.
The second author is supported by the projects MTM2010-15595, FQM-343, FQM-5849, Géanpyl (FR n°2963 du CNRS), and FEDER funds.
The authors would like to thank M. Delgado, D. Llena and V. Micale for their comments.

are inherited from Algebraic Geometry. Along this line Bertin and Carbonne ([8]), Delorme ([12]), Watanabe ([19]) and others found several families of numerical semigroups yielding complete intersections and thus Gorenstein semigroup rings. In the monograph [7] one can find a good dictionary Algebraic Theory-Numerical semigroups.

Numerical semigroups are also useful in the study of singularities of plane algebraic curves. Let $\mathbb{K}$ be an algebraically closed field of characteristic zero and let $f(x,y)$ be an element of $\mathbb{K}[[x,y]]$. Given another element $g \in \mathbb{K}[[x,y]]$, we define the local intersection multiplicity of f with g to be the rank of the $\mathbb{K}$-vector space $\mathbb{K}[[x,y]]/(f,g)$. When g runs over the set of elements of $\mathbb{K}[[x,y]] \setminus (f)$, these numbers define a semigroup. If furthermore f is irreducible, then this semigroup is a numerical semigroup. This leads to a classification of irreducible formal power series in terms of their associated numerical semigroups. This classification can be generalized to polynomials with one place at infinity. The arithmetic properties of numerical semigroups have been in this case the main tool in the proof of Abhyankar-Moh lemma which says that a coordinate has a unique embedding in the plane.

Recently, due to use of algebraic codes and Weierstrass numerical semigroups, some applications to coding theory and cryptography have arise. The idea is finding properties of the codes in terms of the associated numerical semigroup. See for instance [10] and the references therein.

Another focus of recent interest has been the study of factorizations in monoids. If we consider again the equation $a_1x_1 + \cdots + a_nx_n = b$, then we can think of the set of nonnegative integer solutions as the set of factorizations of b in terms of $a_1, \ldots, a_n$. It can be easily shown that no numerical semigroup other than $\mathbb{N}$ is half-factorial, or in other words, there are elements with factorizations of different lengths. Several invariants measure how far are monoids from being half-factorial, and how wild are the sets of factorizations. For numerical semigroups several algorithms have been developed in the last decade, and this is why studying these invariants over numerical semigroups offer a good chance to test conjectures and obtain families of examples.

The aim of this manuscript is to give some basic notions related to numerical semigroups, and from these on the one hand describe a classical application to the study of singularities of plane algebraic curves, and on the other, show how numerical semigroups can be used to obtain handy examples of nonunique factorization invariants.

1. Notable elements

Most of the results appearing in this section are taken from [18, Chapter 1].

Let S be a subset of $\mathbb{N}$. The set S is a submonoid of $\mathbb{N}$ if the following holds:

(i) $0 \in S$,
(ii) If $a, b \in S$ then $a + b \in S$.

Clearly, $\{0\}$ and $\mathbb{N}$ are submonoids of $\mathbb{N}$. Also, if S contains a nonzero element a, then $da \in S$ for all $d \in \mathbb{N}$, and in particular, S is an infinite set.

Let S be a submonoid of $\mathbb{N}$ and let G be the subgroup of $\mathbb{Z}$ generated by S (that is, $G = \{\sum_{i=1}^{s} \lambda_i a_i \mid s \in \mathbb{N}, \lambda_i \in \mathbb{Z}, a_i \in S\}$). If $1 \in G$, then we say that S is a *numerical semigroup*.

We set $\mathrm{G}(S) = \mathbb{N} \setminus S$ and we call it the set of *gaps* of S. We denote by $\mathrm{g}(S)$ the cardinality of $\mathrm{G}(S)$, and we call $\mathrm{g}(S)$ the *genus* of S. Next proposition in particular shows that the genus of any numerical semigroup is a nonnegative integer.

Proposition 1. *Let S be a submonoid of $\mathbb{N}$. Then S is a numerical semigroup if and only if $\mathbb{N} \setminus S$ is a finite set.*

Proof. Let S be a numerical semigroup and let G be the group generated by S in $\mathbb{Z}$. Since $1 \in G$, we can find an expression $1 = \sum_{i=1}^{k} \lambda_i a_i$ for some $\lambda_i \in \mathbb{Z}$ and $a_i \in S$. Assume, without loss of generality, that $\lambda_1, \ldots, \lambda_l < 0$ (respectively $\lambda_{l+1}, \ldots, \lambda_k > 0$). If $s = \sum_{i=l}^{l} -\lambda_i a_i$, then $s \in S$ and $\sum_{i=1+l}^{k} \lambda_i a_i = 1 + s \in S$. We claim that for all $n \geq (s-1)(s+1)$, $n \in S$. Let $n \geq (s-1)(s+1)$ and write $n = qs + r$, $0 \leq r < s$. Since $n = qs + r \geq (s-1)s + (s-1)$, we have $q \geq s - 1 \geq r$, whence $n = qs + r = (rs + r) + (q - r)s = r(s+1) + (q-r)s \in S$.

Conversely, assume that $\mathbb{N} \setminus S$ has finitely many elements. Then there exist $s \in S$ such that $s + 1 \in S$. Hence $1 = s + 1 - s \in G$. □

The idea of focusing on numerical semigroups instead of submonoids of $\mathbb{N}$ in general is the following.

Proposition 2. *Let S be a submonoid of $\mathbb{N}$. Then S is isomorphic to a numerical semigroup.*

Proof. Let d be $\gcd(S)$, that is, d is the generator of the group generated by S in $\mathbb{Z}$. Let $S_1 = \{s/d \mid s \in S\}$ is a numerical semigroup. The map $\phi : S \to S_1$, $\phi(s) = s/d$ is a homomorphism of monoids that is clearly bijective. □

Even though any numerical semigroup has infinitely many elements, it can be described by means of finitely many of them. The rest can be obtained as linear combinations with nonnegative integer coefficients from these finitely many.

Let S be a numerical semigroup and let $A \subseteq S$. We say that S is generated by A and we write $S = \langle A \rangle$ if for all $s \in S$, there exist $a_1, \ldots, a_r \in A$ and $\lambda_1, \ldots, \lambda_r \in \mathbb{N}$ such that $a = \sum_{i=1}^{r} \lambda_i a_i$. Every numerical semigroup S is finitely generated, that is, $S = \langle A \rangle$ with $A \subseteq S$ and A is a finite set.

Let $S^* = S \setminus \{0\}$. The smallest nonzero element of S is called the *multiplicity* of S, $\mathrm{m}(S) = \min S^*$.

Proposition 3. *Every numerical semigroup is finitely generated.*

Proof. Let A be a system of generators of S (S itself is a system of generators). Let m be the multiplicity of S. Clearly $m \in A$. Assume that $a < a'$ are two elements in A such that $a \equiv a' \bmod m$. Then $a' = km + a$ for some positive integer k. So we can remove a' from A and we still have a generating system for S. Observe that at the end of this process we have at most one element in A in each congruence class modulo m, and we conclude that we can choose A to have finitely many elements. □

The underlying idea in the last proof motivates the following definition.

Let $n \in S^*$. We define the *Apéry set* of S with respect to n, denoted $\mathrm{Ap}(S, n)$, to be the set

$$\mathrm{Ap}(S, n) = \{s \in S \mid s - n \notin S\}.$$

This is why some authors call $\{n\} \cup (\mathrm{Ap}(S, n) \setminus \{0\})$ a standard basis of S, when n is chosen to be the least positive integer in S.

As we see next, $\mathrm{Ap}(S, n)$ has precisely n elements.

Lemma 4. *Let S be a numerical semigroup and let $n \in S^*$. For all $i \in \{1, \ldots, n\}$, let $w(i)$ be the smallest element of S such that $w(i) \equiv i \bmod n$. Then*

$$\mathrm{Ap}(S, n) = \{0, w(1), \ldots, w(n-1)\}.$$

Proof. Let $0 \leq i \leq n-1$. By definition, $w(i) \in S$ and clearly $w(i) - n \equiv i \bmod(n)$, hence $w(i) - n \notin S$, in particular $w(i) \in \mathrm{Ap}(S,n)$. This proves one inclusion. Observe that there are no elements $a, b \in \mathrm{Ap}(S,n)$ such that $a \equiv b \bmod n$. Hence we get an equality, because we are ranging all possible congruence classes modulo n. □

Next we give an example using the `numericalsgps GAP` package ([11] and [13], respectively). We will do this several times along the manuscript, since it is also our intention to show how calculations can easily be accomplished using this package.

`GAP` **example 5.** Let us start defining a numerical semigroup.

```
gap> s:=NumericalSemigroup(5,9,21);;
gap> SmallElementsOfNumericalSemigroup(s);
[ 0, 5, 9, 10, 14, 15, 18, 19, 20, 21, 23 ]
```

This means that our semigroup is $\{0, 5, 9, 10, 14, 15, 18, 19, 20, 21, 23, \rightarrow\}$, where the arrow means that every integer larger than 23 is in the set. If we take a nonzero element n in the semigroup, its Apéry set has exactly n elements.

```
gap> AperyListOfNumericalSemigroupWRTElement(s,5);
[ 0, 21, 27, 18, 9 ]
```

We can define the Apéry set for other integers as well, but the above feature no longer holds.

```
gap> AperyListOfNumericalSemigroupWRTInteger(s,6);
[ 0, 5, 9, 10, 14, 18, 19, 23, 28 ]
```

Apéry sets are one of the most important tools when dealing with numerical semigroups. Next we see that they can be used to represent elements in a numerical semigroup in a unique way (actually the proof extends easily to any integer).

Proposition 6. *Let S be a numerical semigroup and let $n \in S^*$. For all $s \in S$, there exists a unique $(k, w) \in \mathbb{N} \times \mathrm{Ap}(S,n)$ such that $s = kn + w$.*

Proof. Let $s \in S$. If $s \in \mathrm{Ap}(S,n)$, then we set $k = 0, w = s$. If $s \notin \mathrm{Ap}(S,n)$, then $s_1 = s - n \in S$. We restart with s_1. Clearly there exists k such that $s_k = s - kn \in \mathrm{Ap}(S,n)$.

Let $s = k_1 n + w_1$ with $k_1 \in \mathbb{N}, w_1 \in \mathrm{Ap}(S,n)$. Suppose that $k_1 \neq k$. Hence $0 \neq (k_1 - k)n = w - w_1$. In particular $w \equiv w_1 \bmod(n)$. This is a contradiction. □

This gives an alternative proof that S is finitely generated.

Corollary 7. *Let S be a numerical semigroup. Then S is finitely generated.*

Proof. Let $n \in S^*$. By the proposition above, $S = \langle \{n\} \cup \mathrm{Ap}(S,n) \setminus \{0\} \rangle$. But the cardinality of $\mathrm{Ap}(S,n) = n$. This proves the result. □

Let S be a numerical semigroup and let $A \subseteq S$. We say that A is a *minimal set of generators* of S if $S = \langle A \rangle$ and no proper subset of A has this property.

Corollary 8. *Let S be a numerical semigroup. Then S has a minimal set of generators. This set is finite and unique: it is actually $S^* \setminus (S^* + S^*)$.*

Proof. Notice that by using the argument in the proof of Proposition 3, every generating set can be refined to a minimal generating set.

Let $A = S^* \setminus (S^* + S^*)$ and let B be another minimal generating set. If B is not included in A, there exists $a, b, c \in B$ such that $a = b + c$. But this contradicts the minimality of B, since in this setting $B \setminus \{a\}$ is a generating system for S. This proves $B \subseteq A$.

Now take $a \in A \subseteq S = \langle B \rangle$. Then $a = \sum_{b \in B} \lambda_b b$. But $a \in S^* \setminus (S^* + S^*)$, and so $\sum_{b \in B} \lambda_b = 1$. This means that there exists $b \in B$ with $\lambda_b = 1$ and $\lambda_{b'} = 0$ for the rest of $b' \in B$. We conclude that $a = b \in B$, which proves the other inclusion. □

Let S be a numerical semigroup. The cardinality of a minimal set of generators of S is called the *embedding dimension* of S. We denote it by $\mathrm{e}(S)$.

Lemma 9. *Let S be a numerical semigroup. We have $\mathrm{e}(S) \leq \mathrm{m}(S)$.*

Proof. The proof easily follows from the proof of Corollary 7 or from that of Proposition 3. □

Examples 10. i) $S = \mathbb{N}$ if and only if $\mathrm{e}(S) = 1$.
ii) Let $m \in \mathbb{N}^*$ and let $S = \langle m, m+1, \ldots, 2m-1 \rangle$. We have $\mathrm{Ap}(S, m) = \{0, m+1, \ldots, 2m-1\}$ and $\{m, m+1, \ldots, 2m-1\}$ is a minimal set of generators of S. In particular $\mathrm{e}(S) = \mathrm{m}(S) = m$.
iii) Let $S = \{0, 4, 6, 9, 10, \ldots\}$. We have $\mathrm{Ap}(S, 4) = \{0, 9, 6, 12\}$. In particular $\mathrm{m}(S) = 4$ and $S = \langle 4, 6, 9, 12 \rangle = \langle 4, 6, 9 \rangle$. Hence $\mathrm{e}(S) = 3$.

GAP example 11. We can easily generate "random" numerical semigroups with the following command. The first argument is an upper bound for the number of minimal generators, while the second says the range where the generators must be taken from.

```
gap> s:=RandomNumericalSemigroup(5,100);
<Numerical semigroup with 5 generators>
gap> MinimalGeneratingSystemOfNumericalSemigroup(s);
[ 6, 7 ]
```

Let S be a numerical semigroup. We set $\mathrm{F}(S) = \max(\mathbb{N} \setminus S)$ and we call it the *Frobenius number* of S. We set $\mathrm{C}(S) = \mathrm{F}(S) + 1$ and we call it the *conductor* of S. Recall that we denoted $\mathrm{G}(S) = \mathbb{N} \setminus S$ and we called it the set of *gaps* of S. Also we used $\mathrm{g}(S)$ to denote the cardinality of $\mathrm{G}(S)$ and we call $\mathrm{g}(S)$ the *genus* of S. We denote by $\mathrm{n}(S)$ the cardinality of $\{s \in S : s \leq \mathrm{F}(S)\}$.

Proposition 12 (Selmer's formulas)**.** *Let S be a numerical semigroup and let $n \in S^*$. We have the following:*

(i) $\mathrm{F}(S) = \max(\mathrm{Ap}(S, n)) - n$,
(ii) $\mathrm{g}(S) = \frac{1}{n}\left(\sum_{w \in \mathrm{Ap}(S,n)} w\right) - \frac{n-1}{2}$.

Proof. (i) Clearly $\max(\mathrm{Ap}(S, n)) - n \notin S$. If $x > \max(\mathrm{Ap}(S, n)) - n$ then $x + n > \max(\mathrm{Ap}(S, n))$. Write $x + n = qn + i$, $q \in \mathbb{N}$, $i \in \{0, \ldots, n-1\}$ and let $w(i) \in \mathrm{Ap}(S, n)$ be the smallest element of S which is congruent to i modulo n. Since $x + n > w(i)$, we have $x + n = kn + w(i)$ with $k > 0$. Hence $x = (k-1)n + w(i) \in S$.
(ii) For all $w \in \mathrm{Ap}(S, n)$, write $w = k_i n + i$, $k_i \in \mathbb{N}$, $i \in \{0, \ldots, n-1\}$. We have:

$$\mathrm{Ap}(S, n) = \{0, k_1 n + 1, \ldots, k_{n-1} n + n - 1\}.$$

Let $x \in \mathbb{N}$ and suppose that $x \equiv i \bmod(n)$. We claim that $x \in S$ if and only if $w(i) \leq x$. In fact, if $x = q_i n + i$, then $x - w(i) = (q_i - k_i)n$. Hence $w(i) \leq x$ if and only if $k_i \leq q_i$ if and only if $x = (q_i - k_i)n + w(i) \in S$. It follows that $x \notin S$ if and only if

$x = q_i n + i, q_i < k_i$. Consequently

$$\mathrm{g}(S) = \sum_{i=1}^{n-1} k_i = \frac{1}{n}\left(\sum_{i=1}^{n-1}(k_i n + i)\right) - \frac{n-1}{2} = \frac{1}{n}\left(\sum_{w\in \mathrm{Ap}(S,n)} w\right) - \frac{n-1}{2}. \qquad \square$$

Example 13. Let $S = \langle a, b\rangle$ be a numerical semigroup. We have

$$\mathrm{Ap}(S, a) = \{0, b, 2b, \ldots, (a-1)b\}.$$

Hence

(i) $\mathrm{F}(S) = (a-1)b - a = ab - a - b$.
(ii) $\mathrm{g}(S) = \frac{1}{a}(a + 2a + \cdots + (b-1)a) - \frac{a-1}{2} = \frac{(a-1)(b-1)}{2} = \frac{\mathrm{F}(S)+1}{2}$.

Lemma 14. *Let S be a numerical semigroup. We have* $\mathrm{g}(S) \geq \frac{\mathrm{F}(S)+1}{2}$.

Proof. Let $s \in \mathbb{N}$. If $s \in S$, then $\mathrm{F}(S) - s \notin S$. Thus $\mathrm{g}(S)$ is greater than or equal to $\mathrm{n}(S)$. But $\mathrm{n}(S) + \mathrm{g}(S) = \mathrm{F}(S) + 1$. This proves the result. $\square$

GAP **example 15.** Let $S = \langle 5, 7, 9\rangle$.

```
gap> s:=NumericalSemigroup(5,7,9);
<Numerical semigroup with 3 generators>
gap> FrobeniusNumber(s);
13
gap> ConductorOfNumericalSemigroup(s);
14
gap> ap:=AperyListOfNumericalSemigroupWRTElement(s,5);
[ 0, 16, 7, 18, 9 ]
gap> Maximum(ap)-5;
13
gap> Sum(ap)/5 -2;
8
gap> GenusOfNumericalSemigroup(s);
8
gap> GapsOfNumericalSemigroup(s);
[ 1, 2, 3, 4, 6, 8, 11, 13 ]
```

Conjecture 16. Let g be positive integer and let n_g be the number of numerical semigroups S with $\mathrm{g}(S) = g$. Is $n_g \leq n_{g+1}$? This conjecture is known to be true for $g \leq 67$ but it is still open in general (J. Fromentin, personal communication; see also Manuel Delgado's web page).

GAP **example 17.**

```
gap> List([1..20],i->Length(NumericalSemigroupsWithGenus(i)));
[ 1, 2, 4, 7, 12, 23, 39, 67, 118, 204, 343, 592, 1001, 1693, 2857, 4806, 8045,
13467, 22464, 37396 ]
```

The following result allows to prove Johnson's formulas (see Corollary 19 below).

Proposition 18. *Let S be a numerical semigroup minimally generated by $n_1, \ldots, n_p$. Let $d = \gcd(n_1, \ldots, n_{p-1})$ and let $T = \langle n_1/d, \ldots, n_{p-1}/d, n_p\rangle$. We have* $\mathrm{Ap}(S, n_p) = d\mathrm{Ap}(T, n_p)$.

Proof. Let $w \in \mathrm{Ap}(S, n_p)$. Since $w - n_p \notin S$ then $w \in \langle n_1, \ldots, n_{p-1}\rangle$, hence $\frac{w}{d} \in \left\langle \frac{n_1}{d}, \ldots, \frac{n_{p-1}}{d}\right\rangle$. If $\frac{w}{d} - n_p \in T$, then $w - dn_p \in S$, which is a contradiction. Hence $\frac{w}{d} \in \mathrm{Ap}(T, n_p)$, in particular $w \in d\mathrm{Ap}(T, n_p)$.

Conversely, if $w \in \mathrm{Ap}(T, n_p)$, then $w \in \left\langle \frac{n_1}{d}, \ldots, \frac{n_{p-1}}{d}\right\rangle$, hence $dw \in \langle n_1, \ldots, n_{p-1}\rangle \in S$. Suppose that $dw - n_p \subseteq S$. We have:

$$dw - n_p = \sum_{i=1}^{p} \lambda_i n_i \text{ implies } dw = \sum_{i=1}^{p-1} \lambda_i n_i + (\lambda_p + 1)n_p.$$

In particular d divides $\lambda_p + 1$. Write $w = \sum_{i=1}^{p-1} \lambda_i \frac{n_i}{d} + \left(\frac{\lambda_p+1}{d}\right) n_p$, whence $w - n_p \in T$, which is a contradiction. Finally $dw \in \mathrm{Ap}(S, n_p)$. This implies our assertion. □

Corollary 19. *Let S be a numerical semigroup minimally generated by $\{n_1, \ldots, n_p\}$. Let $d = \gcd(n_1, \ldots, n_{p-1})$ and let $T = \langle \frac{n_1}{d}, \ldots, \frac{n_{p-1}}{d}, n_p\rangle$. We have the following:*

(i) $\mathrm{F}(S) = dF(T) + (d-1)n_p$,

(ii) $\mathrm{g}(S) = dg(T) + \frac{(d-1)(d-2)}{2}$.

Proof. (i) $\mathrm{F}(S) = \max \mathrm{Ap}(S, n_p) - n_p = d \max \mathrm{Ap}(T, n_p) - n_p = d(\max \mathrm{Ap}(T, n_p) - n_p) + (d-1)n_p = d\mathrm{F}(T) + (d-1)n_p$.

(ii) $\mathrm{g}(S) = \frac{1}{n_p}\left(\sum_{w \in \mathrm{Ap}(S,n_p)} w\right) - \frac{n_p-1}{2} = \frac{d}{n_p}\left(\sum_{w \in \mathrm{Ap}(T,n_p)} w\right) - \frac{n_p-1}{2}$
$= d\left(\frac{1}{n_p}\sum_{w \in \mathrm{Ap}(T,n_p)} w - \frac{n_p-1}{2}\right) + \frac{(d-1)(n_p-1)}{2}$. □

Example 20. Let $S = \langle 20, 30, 17\rangle$, $T = \langle 2, 3, 17\rangle = \langle 2, 3\rangle$; $\mathrm{F}(S) = 10\mathrm{F}(T) + 9 \times 17 = 163$ and $\mathrm{g}(S) = 10 + 916/2 = 82$.

Let S be a numerical semigroup. We say that $x \in \mathbb{N}$ is a *pseudo-Frobenius number* if $x \notin S$ and $x + s \in S$ for all $s \in S^*$. We denote by $\mathrm{PF}(S)$ the set of pseudo Frobenius numbers. The cardinality of $\mathrm{PF}(S)$ is denoted by $\mathrm{t}(S)$ and we call it the *type* of S. Note that $\mathrm{F}(S) = \max(\mathrm{PF}(S))$.

Let $a, b \in \mathbb{N}$. We define $\leq_S$ as follows: $a \leq_S b$ if $b - a \in S$. Clearly $\leq_S$ is a (partial) order relation. With this order relation $\mathbb{Z}$ becomes a poset. We see next that $\mathrm{PF}(S)$ are precisely the maximal gaps of S with respect to $\leq_S$.

Proposition 21. *Let S be a numerical semigroup. We have*

$$\mathrm{PF}(S) = \max_{\leq_S}(\mathbb{N} \setminus S).$$

Proof. Let $x \in \mathrm{PF}(S)$: $x \notin S$ and $x + S^* \subseteq S$. Let $y \in \mathbb{N} \setminus S$ and assume that $x \leq_S y$. If $x \neq y$, then $y - x = s \in S^*$, hence $y = x + s \in x + S^* \subseteq S$. This is a contradiction.
Conversely, let $x \in \mathrm{Max}_{\leq_S}\mathbb{N} \setminus S$. If $x + s \notin S$ for some $s \in S^*$, then $x \leq_S x + s$. This is a contradiction. □

We can also recover the pseudo-Frobenius elements by using, once more, the Apéry sets.

Proposition 22. *Let S be a numerical semigroup and let $n \in S^*$. Then*

$$\mathrm{PF}(S) = \{w - n \mid w \in \max_{\leq_S} \mathrm{Ap}(S, n)\}.$$

Proof. Let $x \in \mathrm{PF}(S) : x + n \in S$ and $x \notin S$. Hence $x + n \in \mathrm{Ap}(S, n)$. Let us prove that $x + n$ is maximal with respect to $\leq_S$. Let $w \in \mathrm{Ap}(S, n)$ such that $x + n \leq_S w$. Let $s \in S$

such that $w-x-n=s$. We have $w-n=x+s$. If $s\in S^*$, then $x+s\in S$. But $w-n\notin S$, a contradiction.
Conversely let $w\in \mathrm{Max}_{\leq_S}\mathrm{Ap}(S,n)$ and let $s\in S^*$. If $w-n+s\notin S$, then $w+s\in \mathrm{Ap}(S,n)$. This contradicts the maximality of w. □

Examples 23. (i) Let $S=\langle 5,6,8\rangle$; $\mathrm{Ap}(S,5)=\{0,6,12,8,14\}$. Hence $\mathrm{PF}(S)=\{12-5,14-5\}=\{7,9\}$. In particular, $\mathrm{t}(S)=2$.
(ii) Let $S=\langle a,b\rangle$ where $a,b\in\mathbb{N}\setminus\{0,1\}$ and $\gcd(a,b)=1$. We have $\mathrm{Ap}(S,a)=\{0,b,2b,\ldots,(a-1)b\}$. Thus $\mathrm{PF}(S)=\{\mathrm{F}(S)=(a-1)b-a\}$ and $\mathrm{t}(S)=1$.

In particular, we get the following consequence, which gives an upper bound for the type of a numerical semigroup.

Corollary 24. *Let S be a numerical semigroup other than $\mathbb{N}$. We have $\mathrm{t}(S)\leq \mathrm{m}(S)-1$.*

Proof. The type S is nothing but the cardinality of the set of maximal elements of $\mathrm{Ap}(S,\mathrm{m}(S))$ with respect to $\leq_S$. Since 0 is not a maximal element, the result follows. □

Remark 25. Let S be a numerical semigroup. In the above inequality, one cannot replace $\mathrm{m}(S)-1$ by $\mathrm{e}(S)$ as it is shown in the following example: let $S=\langle s,s+3,s+3n+1,5+3n+2\rangle$, $n\geq 2$, $r\geq 3n+2$, $s=r(3n+2)+3$; then $\mathrm{t}(S)=2n+3$.

Type, the number of sporadic elements (elements below the Frobenius number) and the genus of a numerical semigroup are related in the following way.

Proposition 26. *Let S be a numerical semigroup and recall that $\mathrm{n}(S)$ is the cardinality of $\mathrm{N}(S)=\{s\in S\mid s<\mathrm{F}(S)\}$. With these notations we have $\mathrm{g}(S)\leq \mathrm{t}(S)\mathrm{n}(S)$.*

Proof. Let $x\in\mathbb{N}$ and let $f_x=\min\{f\in \mathrm{PF}(S)\mid f-x\in S\}$. Let

$$\phi:\mathrm{G}(S)\to \mathrm{PF}(S)\times N(S),\ \phi(x)=(f_x,f_x-x).$$

The map ϕ is clearly injective. In particular $\mathrm{g}(s)$ is less than or equal than the cardinality of $\mathrm{PF}(S)\times N(S)$, which is $\mathrm{t}(S)\mathrm{n}(S)$. □

In particular, if we use the fact that $\mathrm{g}(s)+\mathrm{n}(s)=\mathrm{F}(S)+1$, then we obtain the following easy consequence.

Corollary 27. *Let S be a numerical semigroup. We have $\mathrm{F}(S)+1\leq(\mathrm{t}(S)+1)\mathrm{n}(S)$.*

GAP **example 28.** We go back to $S=\langle 5,7,9\rangle$.

```
gap> PseudoFrobeniusOfNumericalSemigroup(s);
[ 11, 13 ]
gap> TypeOfNumericalSemigroup(s);
2
gap> MultiplicityOfNumericalSemigroup(s);
5
gap> SmallElementsOfNumericalSemigroup(s);
[ 0, 5, 7, 9, 10, 12, 14 ]
gap> Length(last-1);
7
```

Conjecture 29 (Wilf)**.** $\mathrm{F}(S)+1\leq \mathrm{e}(S)\mathrm{n}(S)$.

1.1. **Numerical semigroups with maximal embedding dimension.** Let S be a numerical semigroup and recall that $\mathrm{e}(S) \leq \mathrm{m}(S)$. In the following we shall consider the case where $\mathrm{e}(S) = \mathrm{m}(S)$. We are going to see that if this is the case, then the type is also maximal.

Let S be a numerical semigroup. We say that S has *maximal embedding dimension* if $\mathrm{e}(S) = \mathrm{m}(S)$.

Trivially, any minimal generator is in the Apéry set of any nonzero element different from it. We write the short proof for this.

Lemma 30. *Let x be a minimal generator of S and let $n \in S^*$, $n \neq x$. We have $x - n \notin S$. In particular $x \in \mathrm{Ap}(S, n)$.*

Proof. If $x - n \in S$, since $x = n + (x - n)$, this contradicts the the fact that x is a minimal generator. □

As a consequence, we get that the Apéry set of the multiplicity consists of 0 plus the rest of minimal generators.

Proposition 31. *Let $n_1 < n_2 < \cdots < n_e$ be a minimal set of generators of S. Then S has maximal embedding dimension if and only if $\mathrm{Ap}(S, n_1) = \{0, n_2, \ldots, n_e\}$.*

Proof. Assume that S has maximal embedding dimension. By Lemma 30, $n_2, \ldots, n_e \in \mathrm{Ap}(S, n_1)$. But $n_1 = \mathrm{m}(S) = e$, whence $\mathrm{Ap}(S, n_1) = \{0, n_2, \ldots, n_e\}$.

Conversely, $S = \langle (\mathrm{Ap}(S, n_1) \setminus \{0\}) \cup \{n_1\} \rangle = \langle n_1, n_2, \ldots, n_e \rangle$. Hence $e = \mathrm{e}(S) = \mathrm{m}(S)$. □

As we already mentioned above, the type is also maximal in this kind of numerical semigroup. Actually this also characterizes maximal embedding dimension.

Proposition 32. *Let $n_1 < n_2 < \cdots < n_e$ be a minimal set of generators of S. The following are equivalent.*

(i) S has maximal embedding dimension.
(ii) $\mathrm{g}(S) = \frac{1}{n_1} \sum_{i=2}^{e} n_i - \frac{n_1 - 1}{2}$.
(iii) $\mathrm{t}(S) = n_1 - 1 = \mathrm{m}(S) - 1$.

Proof. If S has maximal embedding dimension, then $\mathrm{Ap}(S, n_1) = \{0, n_2, \ldots, n_e\}$. By Selmer's formulas (Proposition 12), $\mathrm{g}(S) = \frac{1}{n_1} \sum_{w \in \mathrm{Ap}(S, n_1)} w - \frac{n_1 - 1}{2} = \frac{1}{n_1} \sum_{i=2}^{e} n_i - \frac{n_1 - 1}{2}$. Conversely, we have $\{n_2, \ldots, n_e\} \subseteq \mathrm{Ap}(S, n_1)$ and $\frac{1}{n_1} \sum_{w \in \mathrm{Ap}(S, n_1)} w = \frac{1}{n_1} \sum_{i=2}^{e} n_i$. Hence $\mathrm{Ap}(S, n_1) = \{0, n_2, \ldots, n_e\}$. In particular, S has maximal embedding dimension. This proves that (i) and (ii) are equivalent.

Finally we prove that (i) is equivalent to (iii). If S has maximal embedding dimension, then $\mathrm{Ap}(S, n_1) = \{0, n_2, \ldots, n_e\}$. It easily follows that $\mathrm{Max}_{\leq_S} \mathrm{Ap}(S, n_1) = \{n_2, \ldots, n_e\}$, whence $\mathrm{t}(S) = n_1 - 1 = \mathrm{m}(S) - 1$. Now assume that $\mathrm{t}(S) = n_1 - 1$. Then the cardinality of $\mathrm{PF}(S)$ is $n_1 - 1 = \mathrm{m}(S) - 1$. According to Proposition 22, this means that all the elements in $\mathrm{Ap}(S, n_1)$ with the exception of 0 are maximal with respect to $\leq_S$. We also know that $\{n_2, \ldots, n_e\} \subseteq \mathrm{Ap}(S, n_1)$ (Lemma 30). Hence all minimal generators (other than n_1) are maximal in $\mathrm{Ap}(S, n_1)$ with respect to $\leq_S$. Assume that there exists $x \in \mathrm{Ap}(S, n_1) \setminus \{0, n_2, \ldots, n_e\}$. Then $x = \sum_{i=1}^{e} \lambda_i n_i, \lambda_i \geq 0$, and since $x - n_1 \notin S$, we deduce that $\lambda_1 = 0$. Since $x \neq 0$, $\lambda_k \neq 0$ for some k. Thus $x - n_k \in S$, and consequently n_k is not maximal with respect to $\leq_S$. This is a contradiction. Hence $\mathrm{Ap}(S, n_1) = \{0, n_2, \ldots, n_e\}$, and this yields $n_1 = \mathrm{m}(S) = \mathrm{e}(S)$. □

As another consequence of Selmer's formulas, we get an easy expression of the Frobenius number of a maximal embedding dimension numerical semigroup.

Proposition 33. *Let $n_1 < n_2 < \cdots < n_e$ be a minimal set of generators of S with $e = n_1$. Then $\mathrm{F}(S) = n_e - n_1$.*

Proof. This follows from the fact that $\mathrm{F}(S) = \max \mathrm{Ap}(S, n_1) - n_1$ (Proposition 12). □

The converse to this proposition is not true. Just take $S = \langle 4, 5, 11\rangle$.

GAP **example 34.** One can always construct maximal embedding dimension numerical semigroups from any numercal semigroup in the following way (see [18, Chapter 2]).

```
gap> s:=NumericalSemigroup(4,7,9);
<Numerical semigroup with 3 generators>
gap> AperyListOfNumericalSemigroup(s);
[ 0, 9, 14, 7 ]
gap> t:=NumericalSemigroup(4+last);
<Numerical semigroup with 4 generators>
gap> MinimalGeneratingSystemOfNumericalSemigroup(t);
[ 4, 11, 13, 18 ]
```

1.2. **Special gaps and unitary extensions of a numerical semigroup.** We introduce in this section another set of notable elements of numerical semigroups, that is, in some sense dual to the concept of minimal generating system. Let S be a numerical semigroup. Notice that an element $s \in S$ is a minimal generator if and only if $S \setminus \{s\}$ is a numerical semigroup. We define the set of *special gaps* of S as

$$\mathrm{SG}(S) = \{x \in \mathrm{PF}(S) \mid 2x \in S\}.$$

The duality we mentioned above comes in terms of the following result.

Lemma 35. *Let $x \in \mathbb{Z}$. Then $x \in \mathrm{SG}(S)$ if and only if $S \cup \{x\}$ is a numerical semigroup.*

Proof. Easy exercise. □

If S and T are numerical semigroups, with $S \subset T$, we can construct a chain of numerical semigroups $S = S_1 \subset S_2 \subset \cdots \subset S_k = T$ such that for every i, S_{i+1} is obtained from S_i by adjoining a special gap. This can be done thanks to the following result.

Lemma 36. *Let T be a numerical semigroup and assume that $S \subset T$. Then $\max(T \setminus S) \in \mathrm{SG}(S)$. In particular, $S \cup \{\max(T \setminus S)\}$ is a numerical semigroup.*

Proof. Let $x = \max(T \setminus S)$. Clearly $2x \in S$. Take $s \in S^*$. Then $x + s \in T$ and $x < x + s$. Hence $x + s \in S$. □

Remark 37. Let $\mathcal{O}(S)$ be the set of *oversemigroups* of S, that is, the set of numerical semigroups T such that $S \subseteq T$. Since $\mathbb{N} \setminus S$ is a finite set, we deduce that $\mathcal{O}(S)$ is a finite set.

GAP **example 38.**

```
gap> s:=NumericalSemigroup(7,9,11,17);;
gap> GenusOfNumericalSemigroup(s);
12
gap> o:=OverSemigroupsNumericalSemigroup(s);;
gap> Length(o)
```

```
51
gap> s:=NumericalSemigroup(3,5,7);;
gap> o:=OverSemigroupsNumericalSemigroup(s);;
gap> List(last,MinimalGeneratingSystemOfNumericalSemigroup);
[ [ 1 ], [ 2, 3 ], [ 3 .. 5 ], [ 3, 5, 7 ] ]
```

2. Irreducible numerical semigroups

A numerical semigroup S is *irreducible* if it cannot be expressed as the intersection of two proper oversemigroups. In the following we will show that irreducible semigroups decompose into two classes: symmetric and pseudo-symmetric. We will also give characterizations of these two classes. Usually in the literature the concepts of symmetric and pseudo-symmetric have been studied separately; the second a sort of generalization of first. Irreducible numerical semigroups gathered these two families together, and since then many papers devoted to them have been published.

The following lemma is just a particular case of Lemma 36, taking $T = \mathbb{N}$.

Lemma 39. *Let S be a numerical semigroup other than $\mathbb{N}$. Then $S \cup \{\mathrm{F}(S)\}$ is a numerical semigroup.*

The following result is just one of the many characterizations that one can find for irreducible numerical semigroups.

Theorem 40. *Let S be a numerical semigroup. The following are equivalent.*

(i) S is irreducible.
(ii) S is maximal (with respect to set inclusion) in the set of numerical semigroups T such that $\mathrm{F}(S) = \mathrm{F}(T)$.
(iii) S is maximal (with respect to set inclusion) in the set of numerical semigroups T such that $\mathrm{F}(S) \notin T$.

Proof. (i) implies (ii) Let T be a numerical semigroup such that $\mathrm{F}(S) = \mathrm{F}(T)$. If $S \subseteq T$, then $S = T \cap (S \cup \{\mathrm{F}(S)\})$. Since $S \neq S \cup \{\mathrm{F}(S)\}$, we deduce $S = T$.

(ii) implies (iii) Let T be a numerical semigroup such that $\mathrm{F}(S) \notin T$ and assume that $S \subseteq T$. The set $T_1 = T \cup \{\mathrm{F}(S)+1, \mathrm{F}(S)+2, \dots\}$ is a numerical semigroup with $\mathrm{F}(T_1) = \mathrm{F}(S)$. But $S \subseteq T_1$, whence $S = T_1$. Since $\mathrm{F}(S) + k \in S$ for all $k \geq 1$, it follows that $S = T$.

(iii) implies (i) Let S_1, S_2 be two numerical semigroups such that $S \subseteq S_1$, $S \subseteq S_2$ and $S = S_1 \cap S_2$. Since $\mathrm{F}(S) \notin S$, $\mathrm{F}(S) \notin S_i$ for some $i \in \{1, 2\}$. By (iii), $S_i = S$. □

Let S be a numerical semigroup. We say that S is *symmetric* if

(i) S is irreducible,
(ii) $\mathrm{F}(S)$ is odd.

We say that S is *pseudo-symmetric* if

(i) S is irreducible,
(ii) $\mathrm{F}(S)$ is even.

Next we show some characterizations of symmetric and pseudo-symmetric numerical semigroups. We first prove the following.

Proposition 41. *Let S be a numerical semigroup and suppose that*

$$H = \left\{ x \in \mathbb{Z} \setminus S \mid \mathrm{F}(S) - x \notin S, x \neq \frac{\mathrm{F}(S)}{2} \right\}$$

is not empty. If $h = \max H$, then $S \cup \{h\}$ is a numerical semigroup.

Proof. Since $S \subseteq S \cup \{h\}$, the set $\mathbb{N} \setminus (S \cup \{h\})$ has finitely many elements. Let $a, b \in S \cup \{h\}$.

- If $a, b \in S$, then $a + b \in S$.
- Let $a \in S^*$. Assume that $a + h \notin S$, by the maximality of h, we deduce $\mathrm{F}(S) - a - h = \mathrm{F}(S) - (a + h) \in S$. Hence $\mathrm{F}(s) - h = a + \mathrm{F}(S) - a - h \in S$. This contradicts the definition of h.
- If $2h \notin S$, then $\mathrm{F}(S) - 2h = s \in S^*$. This implies that $\mathrm{F}(S) - h = h + s \in S$ (by the preceding paragraph). This is a contradiction. □

GAP **example 42.** In light of Proposition 41 and Lemma 35, if for a numerical semigroup, there exists a maximum of $\{x \in \mathbb{Z} \setminus (S \cup \{\mathrm{F}(S)/2\}) \mid \mathrm{F}(S) - x \notin S\}$, then it is a special gap.

```
gap> s:=NumericalSemigroup(7,9,11,17);
<Numerical semigroup with 4 generators>
gap> g:=GapsOfNumericalSemigroup(s);
[ 1, 2, 3, 4, 5, 6, 8, 10, 12, 13, 15, 19 ]
gap> Filtered(g, x-> (x<>19/2) and not(19-x in s));
[ 4, 6, 13, 15 ]
gap> SpecialGapsOfNumericalSemigroup(s);
[ 13, 15, 19 ]
```

We have introduced the concepts of symmetric and pseudo-symmetric as subclasses of the set of irreducible numerical semigroups. However, these two concepts existed before that of irreducible numerical semigroup, and thus the definitions were different than the ones we have given above. Next we recover the classical definitions of these two classical concepts. Needless to say that as in the case of irreducible numerical semigroups, there are many different characterizations of these properties. We will show some below.

Proposition 43. *Let S be a numerical semigroup.*

(i) S is symmetric if and only if for all $x \in \mathbb{Z} \setminus S$, we have $\mathrm{F}(S) - x \in S$.

(ii) S is pseudo-symmetric if and only if for all $x \in \mathbb{Z} \setminus S$, $\mathrm{F}(S) - x \in S$ or $x = \frac{\mathrm{F}(S)}{2}$.

Proof. (i) Assume that S is symmetric. Then $\mathrm{F}(S)$ is odd, and thus $H = \{x \in \mathbb{Z} \setminus S \mid \mathrm{F}(S) - x \notin S\} = \{x \in \mathbb{Z} \setminus S \mid \mathrm{F}(S) - x \notin S, x \neq \mathrm{F}(S)/2\}$. If H is not the emptyset, then $T = S \cup \{h = \max H\}$ is a numerical semigroup with Frobenius number $\mathrm{F}(S)$ containing properly S, which is impossible in light of Theorem 40.

For the converse note that $\mathrm{F}(S)$ cannot be even, since otherwise as $\mathrm{F}(S)/2 \notin S$, we would have $\mathrm{F}(S) - \mathrm{F}(S)/2 = \mathrm{F}(S)/2 \in S$; a contradiction. So, we only need to prove that S is irreducible. Let to this end T be a numerical semigroup such that $\mathrm{F}(S) \notin T$ and suppose that $S \subset T$. Let $x \in T \setminus S$. By hypothesis $\mathrm{F}(S) - x \in S$. This implies that $\mathrm{F}(S) = (\mathrm{F}(S) - x) + x \in T$. This is a contradiction (we are using here Theorem 40 once more).

(ii) The proof is the same as the proof of (i). □

The maximality of irreducible numerical semigroups, in the set of numerical semigroups with the same Frobenius number, translates to minimality in terms of gaps. This is highlighted in the next result.

Corollary 44. *Let S be a numerical semigroup.*

(i) S is symmetric if and only if $\mathrm{g}(S) = \frac{\mathrm{F}(S)+1}{2}$.

(ii) S is pseudo-symmetric if and only if $\mathrm{g}(S) = \frac{\mathrm{F}(S)+2}{2}$.
Hence irreducible numerical semigroups are those with the least possible genus.

Recall that the Frobenius number and genus for every embedding dimension two numerical semigroup are known; as a consequence, we get the following.

Corollary 45. *Let S be a numerical semigroup. If $\mathrm{e}(S) = 2$, then S is symmetric.*

The rest of the section is devoted to characterizations in terms of the Apéry sets (showing in this way their ubiquity). First we show that Apéry sets are closed under summands.

Lemma 46. *Let S be a numerical semigroup and let $n \in S^*$. If $x, y \in S$ and $x+y \in \mathrm{Ap}(S,n)$, then $x, y \in \mathrm{Ap}(S,n)$.*

Proof. Assume to the contrary, and without loss of generality, that $y-n \in S$. Then $x+y-n \in S$, and consequently $x + y \notin \mathrm{Ap}(S,n)$. □

Proposition 47. *Let S be a numerical semigroup and let $n \in S^*$. Let $\mathrm{Ap}(S,n) = \{0 = a_0 < a_1 < \cdots < a_{n-1}\}$. Then S is symmetric if and only if $a_i + a_{n-1-i} = a_{n-1}$ for all $i \in \{0, \ldots, n-1\}$.*

Proof. Suppose that S is symmetric. From Proposition 12, we know that $\mathrm{F}(S) = a_{n-1} - n$. Let $0 \leq i \leq n-1$. Since $a_i - n \notin S$, we get $\mathrm{F}(S) - a_i + n = a_{n-1} - a_i \in S$. Let $s \in S$ be such that $a_{n-1} - a_i = s$. Since $a_{n-1} = a_i + s \in \mathrm{Ap}(S,n)$, by Lemma 46, $s \in \mathrm{Ap}(S,n)$. Hence $s = a_j$ for some $0 \leq j \leq n-1$. As this is true for any i, we deduce that $j = n-1-i$.

Conversely, the hypothesis implies that $\mathrm{Max}_{\leq_S}\mathrm{Ap}(S,n) = a_{n-1}$. Hence $\mathrm{PF}(S) = \{\mathrm{F}(S)\}$ (Proposition 22). Also, by Proposition 21, $\{\mathrm{F}(S)\} = \mathrm{Max}_{\leq_S}(\mathbb{N}\backslash S)$. If $x \notin S$, then $x \leq_S \mathrm{F}(S)$, whence $\mathrm{F}(S) - x \in S$. To prove that $\mathrm{F}(S)$ is odd, just use the same argument of the proof of Proposition 43. □

As a consequence of the many invariants that can be computed using Apéry sets, we get the following characterizations of the symmetric property.

Corollary 48. *Let S be a numerical semigroup. The following conditions are equivalent.*

(i) S is symmetric.
(ii) $\mathrm{PF}(S) = \{\mathrm{F}(S)\}$.
(iii) If $n \in S$, then $\mathrm{Max}_{\leq S}(\mathrm{Ap}(S,n) = \{\mathrm{F}(S) + n\}$.
(iv) $\mathrm{t}(S) = 1$.

Now, we are going to obtain the analogue for pseudo-symmetric numerical semigroups. The first step is to deal with one half of the Frobenius number.

Lemma 49. *Let S be a numerical semigroup and let $n \in S^*$. If S is pseudo-symmetric, then $\frac{\mathrm{F}(S)}{2} + n \in \mathrm{Ap}(S,n)$.*

Proof. Clearly $\frac{\mathrm{F}(S)}{2} \notin S$. If $\frac{\mathrm{F}(S)}{2} + n \notin S$, then $\mathrm{F}(S) - \frac{\mathrm{F}(S)}{2} - n \in S$. This implies that $\frac{\mathrm{F}(S)}{2} \in S$, which is a contradiction. □

Proposition 50. *Let S be a numerical semigroup and let $n \in S^*$. Let $\mathrm{Ap}(S,n) = \{0 = a_0 < a_1, \cdots < a_{n-2}\} \cup \left\{\frac{\mathrm{F}(S)}{2} + n\right\}$. Then S is pseudo-symmetric if and only if $a_i + a_{n-2-i} = a_{n-2}$ for all $0 \leq i \leq n-2$.*

Proof. Suppose that S is pseudo-symmetric and let $w \in \mathrm{Ap}(S,n)$. If $w \neq \frac{\mathrm{F}(S)}{2}+n$, then $w-n \notin S$ and $w-n \neq \frac{\mathrm{F}(S)}{2}$. Hence $\mathrm{F}(S)-(w-n)=\mathrm{F}(S)+n-w=\max \mathrm{Ap}(S,n)-w \in S$. Since $\mathrm{F}(S)-w \notin S$, then $\mathrm{F}(S)+n-w=\max \mathrm{Ap}(S,n)-w \in \mathrm{Ap}(S,n)$. But $\max(S,n)-w \neq \frac{\mathrm{F}(S)}{2}+n$ (otherwise $w=\frac{\mathrm{F}(S)}{2}$, a contradiction). Now we use the same argument as in the symmetric case (Proposition 47).

Conversely, let $x \neq \frac{\mathrm{F}(S)}{2}$, $x \notin S$. Take $w \in \mathrm{Ap}(S,n)$ such that $w \equiv x \pmod n$. There exists $k \in \mathbb{N}^*$ such that $x=w-kn$ (compare with Proposition 6).

(1) If $w=\frac{\mathrm{F}(S)}{2}+n$, then $\mathrm{F}(S)-x=\frac{\mathrm{F}(S)}{2}+(k-1)n$. But $x \neq \frac{\mathrm{F}(S)}{2}$. Hence $k \geq 2$, and consequently $\mathrm{F}(S)-x=w+(k-2)n \in S$.
(2) If $w \neq \frac{\mathrm{F}(S)}{2}+n$, then $\mathrm{F}(S)-x=\mathrm{F}(S)+n-w+(k-1)n=a_{n-2}-w+(k-1)n \in S$, because $a_{n-2}-w \in S$. □

Again, by using the properties of the Apéry sets, we get several characterizations for pseudo-symmetric numerical semigroups.

Corollary 51. *Let S be a numerical semigroup. The following conditions are equivalent.*

(i) S is pseudo-symmetric.
(ii) $\mathrm{PF}(S)=\left\{\mathrm{F}(S), \frac{\mathrm{F}(S)}{2}\right\}$.
(iii) If $n \in S$, then $\mathrm{Max}_{\leq S}(\mathrm{Ap}(S,n))=\left\{\frac{\mathrm{F}(S)}{2}+n, \mathrm{F}(S)+n\right\}$.

Example 52. Let S be a numerical semigroup. If S is pseudo-symmetric, then $\mathrm{t}(S)=2$. The converse is not true in general. Let $S=\langle 5,6,8\rangle$. We have $\mathrm{Ap}(S,5)=\{0,6,12,8,14\}$. Thus, $\mathrm{PF}(S)=\{7,9\}$, and $\mathrm{t}(S)=2$. However S is not pseudo-symmetric.

GAP **example 53.** Let us see how many numerical semigroups with Frobenius number 15 and type 2 are not pseudo-symmetric.

```
gap> l:=NumericalSemigroupsWithFrobeniusNumber(16);;
gap> Length(l);
205
gap> Filtered(l, s->TypeOfNumericalSemigroup(s)=2);
[ <Numerical semigroup>, <Numerical semigroup>, <Numerical semigroup>,
  <Numerical semigroup>, <Numerical semigroup>, <Numerical semigroup>,
  <Numerical semigroup>, <Numerical semigroup>, <Numerical semigroup>,
  <Numerical semigroup>, <Numerical semigroup>, <Numerical semigroup>,
  <Numerical semigroup>, <Numerical semigroup> ]
gap> Filtered(last,IsPseudoSymmetricNumericalSemigroup);
[ <Numerical semigroup>, <Numerical semigroup>, <Numerical semigroup>,
  <Numerical semigroup>, <Numerical semigroup>, <Numerical semigroup>,
  <Numerical semigroup> ]
gap> Difference(last2,last);
[ <Numerical semigroup with 3 generators>, <Numerical semigroup with 3 generators>,
  <Numerical semigroup with 3 generators>, <Numerical semigroup with 3 generators>,
  <Numerical semigroup with 3 generators>, <Numerical semigroup with 4 generators>,
  <Numerical semigroup with 5 generators> ]
gap> List(last, MinimalGeneratingSystemOfNumericalSemigroup);
[ [ 3, 14, 19 ], [ 3, 17, 19 ], [ 5, 7, 18 ], [ 5, 9, 12 ], [ 6, 7, 11 ],
```

```
[ 6, 9, 11, 13 ], [ 7, 10, 11, 12, 13 ] ]
```

2.1. **Decomposition of a numerical semigroup into irreducible semigroups.** Recall that a numerical semigroup S is irreducible if it cannot be expressed as the intersection of two numerical semigroups properly containing it. We show in this section that every numerical semigroup can be expressed as a finite intersection of irreducible numerical semigroups.

Theorem 54. *Let S be a numerical semigroup. There exists a finite set of irreducible numerical semigroups $\{S_1, \dots, S_r\}$ such that $S = S_1 \cap \cdots \cap S_r$.*

Proof. If S is not irreducible, then there exist two numerical semigroups S^1 and S^2 such $S = S^1 \cap S^2$ and $S \subset S^1$ and $S \subset S^2$. If S^1 is not irreducible, then we restart with S^1, and so on. We construct this way a sequence of oversemigroups of S. This process will stop, because $\mathcal{O}(S)$ has finitely many elements. □

The next step is to find a way to compute an "irredundant" decomposition into irreducible numerical semigroups. The key result to accomplish this task is the following proposition.

Proposition 55. *Let S be a numerical semigroup and let $S_1, \dots, S_r \in \mathcal{O}(S)$. The following conditions are equivalent.*

(i) $S = S_1 \cap \cdots \cap S_r$.
(ii) For all $h \in \mathrm{SG}(S)$, there is $i \in \{1, \dots, r\}$ such that $h \notin S_i$.

Proof. (i) implies (ii) Let $h \in \mathrm{SG}(S)$. Then $h \notin S$, which implies that $h \notin S_i$ for some $i \in \{1, \dots, r\}$.

(ii) implies (i) Suppose that $S \subset S_1 \cap \cdots \cap S_r$, and let $h = \max(S_1 \cap \cdots \cap S_r \setminus S)$. In light of Lemma 36, $h \in \mathrm{SG}(S)$, and for all $i \in \{1, \dots, r\}$, $h \in S_i$, contradicting the hypothesis. □

Remark 56. Let $\mathcal{I}(S)$ be the set of irreducible numerical semigroups of $\mathcal{O}(S)$, and let $\mathrm{Min}_{\subseteq}(I(S))$ be the set of minimal elements of $\mathcal{I}(S)$ with respect to set inclusion. Assume that $\mathrm{Min}_{\subseteq}(I(S)) = \{S_1, \dots, S_r\}$. Define $\mathrm{C}(S_i) = \{h \in \mathrm{SG}(S) : h \notin S_i\}$. We have $S = S_1 \cap \cdots \cap S_r$ if and only if $\mathrm{SG}(S) = \mathrm{C}(S_1) \cup \cdots \cup \mathrm{C}(S_r)$. This gives a procedure to compute a (nonredundant) decomposition of S into irreducibles. This decomposition might not be unique, and not all might have the same number of irreducibles involved.

GAP example 57.
```
gap> s:=NumericalSemigroup(7,9,11,17);;
gap> DecomposeIntoIrreducibles(s);
[ <Numerical semigroup>, <Numerical semigroup>, <Numerical semigroup> ]
gap> List(last,MinimalGeneratingSystemOfNumericalSemigroup);
[ [ 7, 8, 9, 10, 11, 12 ], [ 7, 9, 10, 11, 12, 13 ], [ 7, 9, 11, 13, 15, 17 ] ]
```

There exists some (inefficient) bound on the number of irreducible numerical semigroups appearing in a minimal decomposition of a numerical semigroup into irreducibles. Actually, there might be different minimal decompositions (in the sense that they cannot be refined to other decompositions) with different cardinalities. So it is an open problem to know the minimal cardinality among all possible minimal decompositions.

2.2. **Free numerical semigroups.** We present in this section a way to construct easily symmetric numerical semigroups. This idea was originally exploited by Bertin, Carbonne and Watanabe among others (see [8, 12, 19]) and goes back to the 70's.

Let S be a numerical semigroup and let $\{a_0, \dots, a_h\}$ be its minimal set of generators. Let $d_1 = a_0$ and for all $k \geq 2$, set $d_k = \gcd(d_{k-1}, a_k)$. Define $e_k = \frac{d_k}{d_{k+1}}$, $1 \leq k \leq h$.

We say that S is *free* for the arrangement $(a_0, \ldots, a_h)$ if for all $k \in \{1, \ldots, h\}$:

(i) $e_k > 1$,
(ii) $e_k a_k$ belongs to the semigroup generated by $\{a_0, \ldots, a_{k-1}\}$.

We say that S is *telescopic* if $a_0 < a_1 < \cdots < a_h$ and S is free for the arrangement $(a_0, \ldots, a_h)$.

There is an alternative way of introducing free semigroups with the use of gluings (more modern notation), see for instance [18, Chapter 8].

One of the advantages of dealing with free numerical semigroups is that every integer admits a unique representation in terms of its minimal generators if we impose some bounds on the coefficients.

Lemma 58. *Assume that S is free for the arrangement $(a_0, \ldots, a_h)$, and let $x \in \mathbb{Z}$. There exist unique $\lambda_0, \ldots, \lambda_h \in \mathbb{Z}$ such that the following holds:*

(i) $x = \sum_{k=1}^{h} \lambda_k a_k$,
(ii) for all $h \in \{1, \ldots, h\}$, $0 \leq \lambda_k < e_k$.

Proof. Existence. The group generated by S is $\mathbb{Z}$, and so there exist $\alpha_0, \ldots, \alpha_h \in \mathbb{Z}$ such that $x = \sum_{k=1}^{h} \alpha_k a_k$. Write $\alpha_h = q_h e_h + \lambda_h$, with $0 \leq \lambda_h < e_h$. But $e_h a_h = \sum_{i=0}^{h-1} \beta_i a_i$, with $\beta_i \in \mathbb{N}$ for all $i \in \{1, \ldots, h-1\}$. Hence

$$x = \sum_{k=0}^{h-1} (\lambda_k + q_h \beta_k) + \lambda_h a_h,$$

and $0 \leq \lambda_h < e_h$. Now the result follows by an easy induction on h.

Uniqueness. Let $x = \sum_{k=0}^{h} \alpha_k a_k = \sum_{k=0}^{h} \beta_k a_k$ be two distinct such representations, and let $j \geq 1$ be the greatest integer such that $\alpha_j \neq \beta_j$. We have

$$(\alpha_j - \beta_j) a_j = \sum_{k=1}^{j-1} (\beta_k - \alpha_k) a_k.$$

In particular, d_j divides $(\alpha_j - \beta_j) a_j$. But $\gcd(d_j, a_j) = d_{j+1}$, , whence $\frac{d_j}{d_{j+1}}$ divides $(\alpha_j - \beta_j) \frac{a_j}{d_{j+1}}$. As $\gcd(d_j/d_{j+1}, a_j/d_{j+1}) = 1$, this implies that $\frac{d_j}{d_{j+1}}$ divides $\alpha_j - \beta_j$. However $|\alpha_j - \beta_j| < e_j = \frac{d_j}{d_{j+1}}$, yielding a contradiction. □

An expression of x like in the preceding lemma is called a *standard representation*. As a consequence of this representation we obtain the following characterization for membership to a free numerical semigroup.

Lemma 59. *Suppose that S is free for the arrangement $(a_0, \ldots, a_h)$ and let $x \in \mathbb{N}$. Let $x = \sum_{k=0}^{h} \lambda_k a_k$ be the standard representation of x. We have $x \in S$ if and only if $\lambda_0 \geq 0$.*

Proof. If $\lambda_0 \geq 0$ then clearly $x \in S$. Suppose that $x \in S$ and write $x = \sum_{k=0}^{h} \alpha_k a_k$ with $\alpha_0, \ldots, \alpha_h \in \mathbb{N}$. Imitating the construction of a standard representation made in the above Lemma, we easily obtain the result. □

With this it is easy to describe the Apéry set of the first generator in the arrangement that makes the semigroup free.

Corollary 60. *Suppose that S is free for the arrangement $(a_0, \dots, a_h)$. Then*

$$\mathrm{Ap}(S, a_0) = \left\{ \sum_{k=1}^{h} \lambda_k a_k \mid 0 \leq \lambda_k < e_k \text{ for all } k \in \{1, \dots, h\} \right\}.$$

Proof. Let $x \in S$ and let $x = \sum_{k=0}^{h} \lambda_k a_k$ be the standard representation of x. Clearly $x - a_0 = (\lambda_0 - 1)a_0 + \sum_{k=1}^{h} \lambda_k a_k$ is the standard representation of $x - \lambda_0$. Hence $x - a_0 \notin S$ if and only if $\lambda_0 = 0$. This proves our assertion. □

As usual, once we know an Apéry set, we can derive many properties of the semigroup.

Proposition 61. *Let S be free for the arrangement $(a_0, \dots, a_h)$.*

(i) $\mathrm{F}(S) = \sum_{k=1}^{h}(e_k - 1) - r_0$.
(ii) S is symmetric.
(iii) $\mathrm{g}(S) = \frac{\mathrm{F}(S)+1}{2}$.

Proof. We have $\mathrm{F}(S) = \max \mathrm{Ap}(S, a_0) - a_0$, by Proposition 12. As $\max \mathrm{Ap}(S, a_0) = \sum_{k=1}^{h}(e_k - 1)a_k$, (i) follows easily.

Assertion (ii) is a consequence of Corollary 60 and Proposition 47.

Finally (iii) is a consequence of (ii) and Corollary 44. □

GAP **example 62.** The proportion of free numerical semigroup compared with symmetric numerical semigroups with fixed Frobenius number (or genus) is small.

```
gap> List([1,3..51], i ->
> [Length(FreeNumericalSemigroupsWithFrobeniusNumber(i)),
> Length(IrreducibleNumericalSemigroupsWithFrobeniusNumber(i))]);
[ [ 1, 1 ], [ 1, 1 ], [ 2, 2 ], [ 3, 3 ], [ 2, 3 ], [ 4, 6 ], [ 5, 8 ], [ 3, 7 ],
  [ 7, 15 ], [ 8, 20 ], [ 5, 18 ], [ 11, 36 ], [ 11, 44 ], [ 9, 45 ], [ 14, 83 ],
  [ 17, 109 ], [ 12, 101 ], [ 18, 174 ], [ 24, 246 ], [ 16, 227 ], [ 27, 420 ],
  [ 31, 546 ], [ 21, 498 ], [ 35, 926 ], [ 38, 1182 ], [ 27, 1121 ] ]
```

3. Semigroup of an irreducible meromorphic curve

Let $\mathbb{K}$ be an algebraically closed field of characteristic zero and let $f(x, y) = y^n + a_1(x)y^{n-1} + \cdots + a_n(x)$ be a nonzero polynomial of $\mathbb{K}((x))[y]$ where $\mathbb{K}((x))$ denotes the field of meromorphic series in x. The aim of this section is to associate with f, when f is irreducible, a subsemigroup of $\mathbb{Z}$. The construction of this subsemigroup is based on the notion of Newton-Puiseux exponents. These exponents appear when we solve f as a polynomial in y, and it turns out that the roots are elements of $\mathbb{K}((x^{\frac{1}{n}}))$. Two cases are of intereset: the local case, that is, the case when $f \in \mathbb{K}[[x]][y]$, and the case when $f \in \mathbb{K}[x^{-1}][y]$ with the condition that $F(x, y) = f(x^{-1}, y)$ has one place at infinity. In the first case, the subsemigroup associated with f is a numerical semigroup. In the second case, this subsemigroup is a subset of $-\mathbb{N}$, and some of its numerical properties have some interesting applications in the study of the embedding of special curves with one place at infinity in the affine plane.

3.1. Newton-Puiseux theorem.

Theorem 63 (Hensel's Lemma)**.** *Let f be as above and assume that $f \in \mathbb{K}[\![x]\!][y]$. Assume that there exist two nonconstant polynomials $\tilde{g}, \tilde{h} \in \mathbb{K}[y]$ such that:*

(i) $\tilde{g}, \tilde{h}$ *are monic in* y,
(ii) $\gcd(\tilde{g}, \tilde{h}) = 1$,
(iii) $f(0, y) = \tilde{g}\tilde{h}$.

Then there exist $g, h \in \mathbb{K}[\![x]\!][y]$ *such that:*

(i) g, h *are monic in* y,
(ii) $\mathrm{g}(0, y) = \tilde{g}, h(0, y) = \tilde{h}$,
(iii) $\deg_y g = \deg \tilde{g}$, $\deg_y h = \deg \tilde{h}$,
(iv) $f = gh$.

Proof. Let r (respectively s) be the degree of $\tilde{g}$ (respectively $\tilde{h}$) and write $f(x, y) = \sum_{q \geq 0} f_q(y)x^q$. Clearly $f(0, y) = f_0$ is monic of degree n in y. Furthermore, we can assume that $\deg_y f_q < n$ for all $q \geq 1$. For all $i \geq 0$, we construct $f_i, g_i \in \mathbb{K}[y]$ such that:

(1) $g_0 = \tilde{g}, h_0 = \tilde{h}$,
(2) For all $i \geq 1$, $\deg_y g_i < r$ and $\deg_y h_i < s$,
(3) for all $q \geq 1$, $f_q = \sum_{i=1}^{q} g_i h_{q-i}$.

If $i = 0$, then we set $g_0 = \tilde{g}, h_0 = \tilde{h}$. Suppose that we have $g_0, \ldots, g_{q-1}, h_0, \ldots, h_{q-1}$. Let $e_q = f_q - \sum_{i=0}^{q-1} g_i h_{q-i}$. Note that $\deg_y e_q < n$. We need to prove the existence of two monic polynomials g_q, h_q such that $e_q = h_0 g_q + g_0 h_q$, $\deg_y g_q < r$ and $\deg_y h_q < s$. To this end, we use Euclid's extended algorithm for polynomials with coefficients in a field. By hypothesis, $\gcd(g_0, h_0) = 1$. Let $\alpha, \beta \in \mathbb{K}[y]$ be such that $\alpha g_0 + \beta h_0 = 1$. We have $e_q = (e_q\alpha)g_0 + (e_q\beta)h_0$. Let $G_q = e_q\beta$, $H_q = e_q\alpha$ and write $G_q = Qg_0 + R$ with $\deg_y R < r$. We have

$$e_q = (e_q\alpha)g_0 + (Qg_0 + R)h_0 = (e_q\alpha + Qh_0)g_0 + Rh_0.$$

Let $g_q = R, h_q = e_q\alpha + Qh_0$. Since $\deg_y g_q < r$, it follows that $\deg_y h_q < s$. Hence g_q, h_q fulfill the above conditions. □

Proposition 64. *Let* $f(x, y) \in \mathbb{K}((x))[y]$ *be as above. There exist* $m \in \mathbb{N}$ *and* $y(t) \in \mathbb{K}((t))$ *such that* $f(t^m, y(t)) = 0$.

Proof. We shall prove the result by induction on the degree in y of f. If $n = 1$, then $f = y - a_1(x)$. Hence $f(t, a_1(t)) = 0$. Suppose that $n \geq 2$. We shall assume the following.

(1) $a_1(x) = 0$.
(2) $a_k(x) \in \mathbb{K}[\![x]\!]$ for all $k \in \{2, \ldots, n\}$ and $a_k(0) \neq 0$ for some $k \in \{2, \ldots, n\}$.

It follows that $f(0, y) = y^n + a_2(0)y^{n-2} + \cdots + a_n(0)$ is not a power in $\mathbb{K}[y]$. Hence there exist nonconstant monic polynomials $\tilde{g}(y), \tilde{h}(y) \in \mathbb{K}[y]$ such that $\gcd(\tilde{g}(y), \tilde{h}(y)) = 1$ and $f(0, y) = \tilde{g}(y)\tilde{h}(y)$. By Hensel's lemma, there exist monic polynomials $g, h \in \mathbb{K}[\![x]\!][y]$ such that $\deg_y g, \deg_y h < n$ and $f = gh$. By induction hypothesis there exist $n \in \mathbb{N}$ and $y(t) \in \mathbb{K}((t))$ such that $\mathrm{g}(t^n, y(t)) = 0$. In particular, $f(t^n, y(t)) = 0$.

(1) Assume that $a_1(x) \neq 0$. Let $z = y + \frac{a_1}{n}$ and let $\mathrm{F}(x, z) = f(x, z - \frac{a_1}{n})$. Let $m \in \mathbb{N}$ and $z(t) \in \mathbb{K}((t))$ such that $\mathrm{F}(t^n, z(t)) = 0$. We have $f\left(t^n, z(t) - \frac{a_1}{n}\right) = 0$.
(2) Let $f = y^n + \sum_{k=2}^{n} a_k(x)y^{n-k}$ with $a_k(x) \neq 0$ for some $k \in \{2, \ldots, n\}$ (if $f(x, y) = y^n$, then $f(t, 0) = 0$, and so it suffices to take $m = 1$ and $y(t) = 0$). For all $k \in \{2, \ldots, n\}$ such that $a_k \neq 0$, let $u_k = \mathrm{ord}_x(a_k)$. Set $u = \min\left\{\frac{u_k}{k} \mid a_k \neq 0\right\}$. There exists an index r such that $u = \frac{u_r}{r}$. Let $x = w^r$ and $z = w^{-u_r}y$, and let $g(w, z) = w^{-nu_r}f(w^r, y)$. We

have

$$g(w,z) = w^{-nu_r}\left(w^{nu_r}z^n + \sum_{k=2}^{n} a_k(w^r)w^{u_r(n-k)}z^{n-k}\right)$$
$$= z^n + \sum_{k=2}^{n} a_k(w^r)w^{u_r(n-k)}z^{n-k}.$$

Let $b_k(w) = a_k(w^r)w^{u_r(n-k)}$. We have $\mathrm{ord}_w b_k = ru_k - ku_r \geq 0$, hence $b_k \in \mathbb{K}[[w]]$. Furthermore, $\mathrm{ord}_w b_r(w) = 0$, that is, $b_r(0) \neq 0$. Finally, if $m \in \mathbb{N}$ and $w(t) \in \mathbb{K}((t))$ are such that $\mathrm{g}(t^m, w(t)) = 0$, then $f(t^{mr}, t^{mu_r}z(t)) = 0$. □

Lemma 65. *Let $m \in \mathbb{N}^*$. The extension $\mathbb{K}((t^m)) \to \mathbb{K}((t))$ is an algebraic extension of degree m.*

Proof. The field $\mathbb{K}((t))$ is a $\mathbb{K}((t^m))$-vector space with basis $\{1, t, \ldots, t^{m-1}\}$. □

Let $y(t) \in \mathbb{K}((t))$ and let $F(t^m, y) \in \mathbb{K}((t^m))[y]$ be the minimal polynomial of y over $\mathbb{K}((t^m))$. By abuse of notation we write $F(x,y) \in \mathbb{K}((x))[y]$ for $F(t^m, y)$. Then

(1) $F(x,y)$ is a monic irreducible polynomial of $\mathbb{K}((x))[y]$,
(2) $F(t^m, y(t)) = 0$,
(3) for all $g(x,y) \in \mathbb{K}((x))[y]$, if $g(t^m, y(t)) = 0$, then $F(x,y)$ divides $g(x,y)$,
(4) $\deg_y F(x,y) = [\mathbb{K}((t^m))(y(t)) : \mathbb{K}((t^m))]$,
(5) $\deg_y F(x,y)$ divides m.

Write $y(t) = \sum_p c_p t^p$. Define the *support* of $y(t)$ to be $\mathrm{Supp}(y(t)) = \{p \mid c_p \neq 0\}$.

Proposition 66. *Let the notations be as above. If $\gcd(m, \mathrm{Supp}(y(t))) = 1$, then the following holds.*

(i) $F(t^m, y) = \prod_{w, w^m=1}(y - y(wt))$, and if $w_1 \neq w_2$, $w_1^n = w_2^n = 1$, then $y(w_1 t) \neq y(w_2 t)$.
(ii) $\deg_y F(x,y) = m$.

Proof. Clearly (i) implies (ii).

To prove (i), note that if $w^m = 1$, then $F((wt)^m, y(wt)) = 0$. Let $w_1 \neq w_2$ be such that $w_1^m = w_2^m = 1$. We have $y(w_1 t) - y(w_2 t) = \sum_p (w_1^p - w_2^p)c_p t^p$. If $y(w_1 t) = y(w_2 t)$, then $w_1^p = w_2^p$ for all $p \in \mathrm{Supp}(y(t))$. But $w_1^m = w_2^m$, and $\gcd(m, \mathrm{Supp}(y(t))) = 1$, which yields $w_1 = w_2$; a contradiction. □

Proposition 67. *Suppose that $f(x,y)$ is irreducible. There exists $y(t) \in \mathbb{K}((t))$ such that $f(t^n, y(t)) = 0$. Furthermore,*

(1) $f(t^n, y) = \prod_{w^n=1}(y - y(wt))$,
(2) if $w_1 \neq w_2$, $w_1^n = w_2^n = 1$, then $y(w_1 t) \neq y(w_2 t)$,
(3) $\gcd(n, \mathrm{Supp}(y(t))) = 1$.

Proof. We know that there exist $m \in \mathbb{N}$ and $y(t) \in \mathbb{K}((t))$ such that $f(t^m, y(t)) = 0$. Let m be the smallest integer with this property and let $d = \gcd(m, \mathrm{Supp}(y(t)))$. If $d > 1$, then $y(t) = z(t^d)$ for some $z(t) \in \mathbb{K}((t))$, hence $f\left((t^{m/d})^d, z(t^d)\right) = 0 = f\left(t^{m/d}, z(t)\right)$, which is a contradiction. The polynomial f is monic and irreducible. Thus f is consequently the minimal polynomial of $y(t)$ over $\mathbb{K}((t^m))$. In particular $m = n$. This with Proposition 66 completes the proof of the assertion. □

Suppose that f is irreducible and let $y(t) = \sum_p c_p t^p$ as above. Let $d_1 = n = \deg_y f$ and let $m_1 = \inf\{p \in \mathrm{Supp}(y(t)) \mid d_1 \nmid p\}$, $d_2 = \gcd(d_1, m_1)$. Then for all $i \geq 2$, let $m_i = \inf\{p \in \mathrm{Supp}(y(t)) \mid d_i \nmid p\}$ and $d_{i+1} = \gcd(d_i, m_i)$. By hypothesis, there exists $h \geq 1$ such that $d_{h+1} = 1$. We set $\underline{m} = (m_1, \ldots, m_h)$ and $\underline{d} = (d_1, \ldots, d_{h+1})$. We also set $e_i = \frac{d_i}{d_{i+1}}$ for all $i \in \{1, \ldots, h\}$. We finally define the sequence $\underline{r} = (r_0, \ldots, r_h)$ as follows: $r_0 = n, r_1 = m_1$ and for all $i \in \{2, \ldots, h\}$,

$$r_i = r_{i-1}e_{i-1} + m_i - m_{i-1}.$$

The sequence $\underline{m}$ is called the set of *Newton-Puiseux exponents* of f. The sequences $\underline{m}, \underline{d}, \underline{r}$ are called the *characteristic sequences associated* with f. Note that $d_k = \gcd(r_0, \ldots, r_{k-1})$ for all $1 \leq k \leq h+1$.

Lemma 68. *Let $k \in \{1, \ldots, h\}$ and let $i \in \{1, \ldots, e_k - 1\}$. Then ir_k is not in the group generated by $\{r_0, \ldots, r_{k-1}\}$.*

Proof. Assume we can write $ir_k = \sum_{j=1}^{k-1} \theta_j r_j$, for some $\theta_0, \cdots, \theta_{k-1} \in \mathbb{Z}$. Since $\gcd(r_0, \cdots, r_{k-1}) = d_k$, we get that d_k divides ir_k. Hence $e_k = \frac{d_k}{d_{k+1}}$ divides $i\frac{r_k}{d_{k+1}}$. But $\gcd\left(e_k, \frac{r_k}{d_{k+1}}\right) = 1$ and $i < e_k$. This is a contradiction. □

Lemma 69. *Let the notations be as above, in particular f is irreducible and $y(t) \in \mathbb{K}((t))$ is a root of $f(t^n, y) = 0$.*

(i) $\mathrm{ord}_t(y(t) - y(wt)) \in \{m_1, \ldots, m_h\}$.
(ii) The cardinality of $\{y(wt) \mid \mathrm{ord}_t(y(t) - y(wt)) > m_k\}$ *is* d_{k+1}.
(iii) The cardinality of $\{y(wt) \mid \mathrm{ord}_t(y(t) - y(wt)) = m_k\}$ *is* $d_k - d_{k+1}$.

Proof. (i) From the expression of $y(t)$, we get $y(t) - y(wt) = \sum_p (1 - w^p)c_p t^p$. Let $M = \mathrm{ord}_t(y(t) - y(wt))$. It follows that for all $p < M$, $w^p = 1$. Hence, if $d = \gcd(n, \{p \in \mathrm{Supp}(y(t)) \mid p < M\})$, then $w^d = 1$. But $d = d_k$ for some $1 \leq k \leq h$, whence $M = m_{k-1}$.
(ii) In fact, $\mathrm{ord}_t(y(t) - y(wt)) > m_k$ if and only if $w^{d_{k+1}} = 1$.
(iii) Observe that $\mathrm{ord}_t(y(t) - y(wt)) = m_k$ if and only if $\mathrm{ord}_t(y(t) - y(wt)) > m_{k-1}$ and $\mathrm{ord}_t(y(t) - y(wt)) \leq m_k$. Hence the result follows from (ii). □

Let the notations be as above and let $1 \leq k \leq h$. Let $\bar{y}(t) = \sum_{p<m_k} c_p t^p$ and let $G_k(x, y)$ be the minimal polynomial of $\bar{y}(t)$ over $\mathbb{K}((t^n))$. Since $\gcd(n, \mathrm{Supp}(\bar{y}(t))) = d_k$, the polynomial G_k is a monic irreducible polynomial of degree $\frac{n}{d_k}$ in y. Furthermore, if $Y(t) = \bar{y}(t^{\frac{1}{d_k}})$, then

$$G_k(t^{\frac{n}{d_k}}, y) = \prod_{v, v^{\frac{n}{d_k}}=1} (y - Y(vt)).$$

We call G_k a *d_kth pseudo root* of f.

Proposition 70. *Under the standing hypothesis.*

(i) The sequence of Newton-Puiseux exponents of G_k is given by $\left(\frac{m_1}{d_k}, \cdots, \frac{m_{k-1}}{d_k}\right)$.
(ii) The $\underline{r}$-sequence and $\underline{d}$-sequence of G_k are given by $\left(\frac{r_0}{d_k}, \cdots, \frac{r_{k-1}}{d_k}\right)$ *and* $\left(\frac{d_0}{d_k}, \cdots, \frac{d_{k-1}}{d_k}, 1\right)$, *respectively.*

Proof. (i) This follows from the expression of $Y(t)$, using the fact that $\gcd(\frac{n}{d_k}, \cdots, \frac{m_{k-1}}{d_k}) = 1$.

(ii) Let $\underline{R}$, $\underline{D}$, $\underline{E}$ be the characteristic sequences associated with G_k. We have $D_1 = R_0 = \deg_y G_k = \frac{n}{d_k} = \frac{r_0}{d_k} = \frac{d_1}{d_k}$, $R_1 = \frac{m_1}{d_k} = \frac{r_1}{d_k}$ and $D_2 = \gcd(\frac{r_0}{d_k}, \frac{r_1}{d_k}) = \frac{d_2}{d_k}$. Hence $E_1 = e_1$. Now $R_2 = R_1E_1 + \frac{m_2}{d_k} - \frac{m_1}{d_k}$, hence $R_2 = \frac{r_2}{d_k}$. The assertion now follows by an easy induction on $i \leq k-1$. □

Let g be a nonzero polynomial of $\mathbb{K}((x))[y]$. We define the *intersection multiplicity* of f with g, denoted $\mathrm{int}(f,g)$, to be $\mathrm{int}(f,g) = \mathrm{ord}_t g(t^n, y(t))$. Note that this definition does not depend on the root $y(t)$, that is, $\mathrm{int}(f,g) = \mathrm{ord}_t g(t^n, y(wt))$ for all $w \in \mathbb{K}$ such that $w^n = 1$.

Proposition 71. *Let the notations be as above. We have* $\mathrm{int}(f, G_k) = r_k$.

Proof. From Proposition 67, we can write

$$f(t^n, \bar{y}(t^{d_k})) = \prod_{w^n=1} (\bar{y}(t^{d_k}) - y(wt)).$$

As in the proof of Lemma 69, we deduce

$$\mathrm{ord}_t(\bar{y}(t^{d_k}) - y(wt)) = \begin{cases} m_i & \text{if } \mathrm{ord}_t(y(t) - y(wt)) = m_i < m_k, \\ m_k & \text{if } \mathrm{ord}_t(y(t) - y(wt)) \geq m_k. \end{cases}$$

Hence $\mathrm{ord}_t f(t^n, \bar{y}(t^{d_k})) = \sum_{i=1}^{k-1}(d_i - d_{i+1})m_i + m_k d_k$. Now

$$\begin{aligned} r_k d_k &= r_{k-1}d_{k-1} + (m_k - m_{k-1})d_k \\ &= r_{k-2}d_{k-2} + (m_{k-1} - m_{k-2})d_{k-1} + (m_k - m_{k-1})d_k \\ &\cdots \\ &= r_1 d_1 - m_1 d_2 + \sum_{i=2}^{k-1}(d_i - d_{i+1})m_i + m_k d_k \\ &= \sum_{i=1}^{k-1}(d_i - d_{i+1})m_i + m_k d_k. \end{aligned}$$

Hence $\mathrm{ord}_t f(t^n, \bar{y}(t^{d_k})) = r_k d_k$. In particular $\mathrm{int}(f, G_k) = \mathrm{ord}_t f\left(t^{n/d_k}, \bar{y}(t^{1/d_k})\right) = r_k$. □

Let $G_1, \ldots, G_h$ be the set of pseudo-roots of f constructed above and recall that for all $k \in \{1, \ldots, h\}$, G_k is a monic irreducible polynomial of degree $\frac{n}{d_k}$ in y. Recall also that the set of characteristic sequences associated with G_k are given by $\left(\frac{m_1}{d_k}, \ldots, \frac{m_{k-1}}{d_k}\right)$, $\left(\frac{d_1}{d_k}, \ldots, \frac{d_{k-1}}{d_k}, 1\right)$ and $\left(\frac{r_0}{d_k}, \ldots, \frac{r_{k-1}}{d_k}\right)$.

Proposition 72. *Let* $g \in \mathbb{K}((x))[y]$. *Then*

$$g = \sum_{\theta} c_\theta(x) G_1^{\theta_1} \ldots G_h^{\theta_h} f^{\theta_{h+1}}$$

for some $\theta = (\theta_1, \ldots, \theta_{h+1}) \in \mathbb{N}^{h+1}$, *with* $0 \leq \theta_k < e_k$ *for all* $k \in \{1, \ldots, h\}$, *and some* $c_\theta(x) \in \mathbb{K}((x))$. *We call this expression the* expansion of g with respect to $(G_1, \ldots, G_h, f)$.

Proof. Write $g = Qf + R$ where $\deg_y R < n$. If $\deg_y Q \geq n$, then write $Q = Q^1 f + R^1$ with $\deg_y R^1 < n$. We have $g = Q^1 f^2 + R^1 f + R$, then we restart with Q^1. This process will stop giving the following expression of g in terms of the powers of f:

$$g = \sum_{k=0}^{l} \alpha_k(x,y) f^k,$$

where $\deg_y \alpha_k(x,y) < n$ for all $k \in \{0,\dots,l\}$. Fix $k \in \{0,\dots,l\}$ and write the expression of α_k in terms of the powers of G_h:

$$\alpha_k = \sum_{i=0}^{l_k} \alpha_i^k G_h^i,$$

with $\deg_y \alpha_i^k < \frac{n}{d_h}$ for all $i \in \{0,\dots,l_k\}$. Note that, since $\deg_y \alpha_k < n$, we have $i < e_h = d_h$. Finally we get

$$g = \sum_{\theta} c_\theta(x,y) G_h^{\theta_h} f^{\theta_{h+1}},$$

with $\theta_h < e_h$ for all $\theta = (\theta_h, \theta_{h+1}) \in \mathbb{N}^2$ such that $c_\theta \neq 0$. Now we restart with the set of polynomials $c_\theta(x,y)$ and G_{h-1}. We get the result by induction on $k \leq h$. □

Proposition 73. *Let $g \in \mathbb{K}((x))[y]$. If $f \nmid g$, then there exist unique $\lambda_0 \in \mathbb{Z}, \lambda_1, \dots, \lambda_h \in \mathbb{N}$ such that $\operatorname{int}(f,g) = \sum_{k=0}^{h} \lambda_k r_k$ and for all $k \in \{1,\dots,h\}$, $\lambda_k < e_k$.*

Proof. Let $g = \sum_\theta c_\theta(x) G_1^{\theta_1} \cdots G_h^{\theta_h} f^{\theta_{h+1}}$ be the expansion of g with respect to $(G_1,\dots,G_h,f)$. Notice that $\theta_k < e_k$ for all $k \in \{1,\dots,h\}$ (Proposition 72). Given a monomial $c_\theta(x) G_1^{\theta_1} \cdots G_h^{\theta_h} f^{\theta_{h+1}}$ of g, if $\theta_{h+1} = 0$ and $\theta_0 = \operatorname{ord}_x c_\theta(x)$, then

$$\operatorname{int}(f, c_\theta(x) G_1^{\theta_1} \cdots G_h^{\theta_h}) = \sum_{k=0}^{h} \theta_k r_k.$$

Let $c_\alpha(x) G_1^{\alpha_1} \cdots G_h^{\alpha_h}$ and $c_\beta(x) G_1^{\beta_1} \cdots G_h^{\beta_h}$ be two monomials of g, and let α_0 and β_0 be the orders in x of $c_\alpha(x)$ and $c_\beta(x)$, respectively. Assume that $\sum_{k=0}^{h} \alpha_k r_k = \sum_{k=0}^{h} \beta_k r_k$ and let j be the greatest integer such that $\alpha_j \neq \beta_j$. Suppose that $j \geq 0$ and that $\alpha_j > \beta_j$. We have

$$(\alpha_j - \beta_j) r_j = \sum_{k=0}^{j-1} (\beta_k - \alpha_k) r_k$$

with $0 < \alpha_j - \beta_j < e_j$. This contradicts Lemma 68. Finally either $f \mid g$ or there is a unique monomial $c_{\theta^0}(x) G_1^{\theta_1^0} \cdots G_h^{\theta_h^0}$ such that

$$\operatorname{int}(f,g) = \sum_{k=0}^{h} \theta_k^0 r_k = \inf\{\operatorname{int}(f, c_\theta(x) G_1^{\theta_1} \cdots G_h^{\theta_h}), c_\theta \neq 0\}.$$ □

Corollary 74. *Let $g \in \mathbb{K}((x))[y]$. If $\deg_y g < \frac{n}{d_{k+1}}$ for some $k \in \{1,\dots,h\}$, then there exist $\lambda_0 \in \mathbb{Z}, \lambda_1, \dots, \lambda_k \in \mathbb{N}$ such that $\operatorname{int}(f,g) = \sum_{i=0}^{k} \lambda_i r_i$.*

Proof. Let $g = \sum_\theta c_\theta(x) G_1^{\theta_1} \dots G_h^{\theta_h} f^{\theta_{h+1}}$ be the expansion of g with respect to $(G_1,\dots,G_h,f)$. Since $\deg_y g < \frac{n}{d_{k+1}}$, we deduce that for all nonzero monomial $c_\theta(x) G_1^{\theta_1} \dots G_h^{\theta_h} f^{\theta_{h+1}}$, $\theta_{k+1} = \cdots = \theta_{h+1} = 0$. This implies the result. □

More generally, let $k \in \{1, \dots, h\}$ and define a *d_kth pseudo root* of f to be any monic polynomial G_k of degree $\frac{n}{d_k}$ in y such that $\mathrm{int}(f, G_k) = r_k$. The following proposition shows that such a polynomial is necessarily irreducible.

Proposition 75. *Let $k \in \{1, \dots, h\}$ and let H be a monic polynomial of $\mathbb{K}((x))[y]$, of degree $\frac{n}{d_k}$ in y. If $\mathrm{int}(f, H) = r_k$, then H is irreducible.*

Proof. Let $H = H_1 \cdots H_s$ be the decomposition of G into irreducible components in $\mathbb{K}((x))[y]$. Suppose that $s > 1$ and let $i \in \{1, \dots, s\}$. Since $\deg_y H_i < \frac{n}{d_k}$, by Corollary 74, there exist $\lambda_0^i \in \mathbb{Z}, \lambda_1^i, \dots, \lambda_{k-1}^i$ such that $\mathrm{int}(f, H_i) = \lambda_0^i r_0 + \cdots + \lambda_{k-1}^i r_{k-1}$. Hence $r_k = (\sum_{i=1}^s \lambda_0^i) r_0 + \cdots + (\sum_{i=1}^s \lambda_{k-1}^i) r_{k-1}$. This contradicts Lemma 68. □

Lemma 76. *Let the notations be as above. For all $1 \leq k \leq h$, there exist $\lambda_0^k, \dots, \lambda_{k-1}^k \in \mathbb{N}$ such that $e_k r_k = \sum_{i=1}^{k-1} \lambda_i^k r_i$.*

Proof. Let G_h be a d_hth pseudo root of f. Write $f = G_h^{d_h} + \alpha_1(x,y) G_h^{d_h - 1} + \cdots + \alpha_{d_h}(x,y)$. For all $k \in \{0, \dots, d_h\}$, $\mathrm{int}(f, \alpha_k(x,y) G_h^{d_h - k}) = \mathrm{int}(f, \alpha_k(x,y)) + (d_h - k) r_h$ (where $\alpha_0(x,y) = 1$). But $f(t^n, y(t)) = 0$, and by Corollary 74, for all $k \in \{1, \dots, d_h\}$, there exist $\alpha_0^k, \dots, \alpha_{h-1}^k$ such that $\mathrm{int}(f, \alpha_k(x,y)) = \sum_{i=1}^{h-1} \alpha_i^k r_i$. Now a similar argument as in Proposition 73 shows that if $0 \leq k_1 \neq k_2 \leq d_h - 1$, then $\mathrm{int}(f, \alpha_{k_1} G_h^{d_h - k_1}) \neq \mathrm{int}(f, \alpha_{k_2} G_h^{d_h - k_2})$. The same argument shows also that for all $i \in \{1, \dots, d_h - 1\}$, if $\alpha_i(x,y) \neq 0$, then $\mathrm{int}(f, \alpha_i(x,y) G_h^{d_h - i}) \neq \mathrm{int}(f, \alpha_{d_h}(x,y))$. Let $E = \{\mathrm{int}(f, \alpha_k(x,y)) + (d_h - k) r_h \mid k \in \{0, \dots, d_h\}\}$ and let $k_0 \in \{0, \dots, d_h\}$ be such that $\mathrm{int}(f, \alpha_{k_0}(x,y)) + (d_h - k_0) r_h = \inf(E)$. If k_0 is unique with this property, then $\mathrm{ord}_t f(t^n, y(t)) = \mathrm{int}(f, \alpha_{k_0}(x,y)) + (d_h - k_0) r_h$, which is a contradiction because $f(t^n, y(t)) = 0$. Hence there is at least one $k_1 \neq k_0$ such that $\mathrm{int}(f, \alpha_{k_0}(x,y)) + (d_h - k_0) r_h = \mathrm{int}(f, \alpha_{k_1}(x,y)) + (d_h - k_1) r_h$. This is possible only for $\{k_0, k_1\} = \{0, d_h\}$, in particular $\mathrm{int}(f, G_h^{d_h}) = \mathrm{int}(f, \alpha_{d_h}(x,y))$. This proves the result for $k = h$. Now we use an induction on $1 \leq k \leq h$. □

Proposition 77. *Let the notations be as above. Let g be a nonzero polynomial of $\mathbb{K}((x))[y]$ and let $G_1, \dots, G_h$ be a set of $d_1, \dots, d_h$th pseudo roots of f. If $\deg_y g < \frac{n}{d_{k+1}}$ for some $k \in \{0, \dots, h-1\}$, then $\mathrm{int}(f, g) = d_{k+1} \mathrm{int}(G_{k+1}, g)$.*

Proof. Let $g = \sum_{\underline{\theta}} c_{\underline{\theta}}(x) G_1^{\theta_1} \cdots G_k^{\theta_k}$ be the expansion of g with respect to $(G_1, \dots, G_h, f)$. By Proposition 73, there is a unique monomial $c_{\underline{\theta^0}}(x) G_1^{\theta_1^0} \cdots G_k^{\theta_k^0}$ such that

$$\mathrm{int}(f, g) = \mathrm{int}(f, c_{\underline{\theta^0}}(x) G_1^{\theta_1^0} \cdots G_k^{\theta_k^0}) = \inf\{\mathrm{int}(f, c_{\underline{\theta}}(x) G_1^{\theta_1} \cdots G_k^{\theta_k}, c_{\underline{\theta}} \neq 0\}.$$

Now clearly, the expansion of g above is also that of g with respect to $(G_1, \dots, G_{k+1})$. Furthermore, if $c_{\underline{\theta}}(x) \neq 0$ and if $\theta_0 = \mathrm{ord}_x c_{\underline{\theta}}(x)$, then $\mathrm{int}(G_{k+1}, c_{\underline{\theta}}(x) G_1^{\theta_1} \dots G_k^{\theta_k}) = \sum_{i=0}^k \theta_i \frac{r_i}{d_{k+1}} = \frac{1}{d_{k+1}} \mathrm{int}(f, c_{\underline{\theta}}(x) G_1^{\theta_1} \cdots G_k^{\theta_k})$. This implies the result. □

Proposition 78. *Let $(G_1, \dots, G_h)$ be a set of pseudo-roots of f. For all $k \in \{1, \dots, h-1\}$, $(G_1, \dots, G_k)$ is a set of pseudo roots of G_{k+1}.*

Proof. Fix $k \in \{1, \dots, h-1\}$ and let $i \in \{1, \dots, k\}$. By Proposition 77,

$$\mathrm{int}(G_{k+1}, G_i) = \frac{1}{d_{k+1}} \mathrm{int}(f, G_i) = \frac{r_i}{d_{k+1}}.$$

Furthermore, G_i is irreducible by Proposition 75. This proves the result. □

Let $(G_1, \cdots, G_h)$ be a set of pseudo-roots of f. Let $k \in \{1, \ldots, h\}$ and write

$$f = G_k^{d_k} + \alpha_1(x,y)G_k^{d_k-1} + \cdots + \alpha_{d_k}(x,y),$$

where $\deg_y \alpha_i(x,y) < \frac{n}{d_k}$ for all $i \in \{1, \ldots, d_k\}$. Let $G_k' = G_k + \frac{\alpha_1}{d_k}$. We call G_k' the *Tchirnhausen transform* of G_k and denote it by $\mathrm{T}(G_k)$. With these notations we have the following.

Proposition 79. $\mathrm{int}(f, \mathrm{T}(G_k)) = r_k$.

Proof. Let $k = h$ and let

$$f = G_h^{d_h} + \alpha_1(x,y)G_h^{d_h-1} + \cdots + \alpha_{d_h}(x,y)$$

be the G_h-adic expansion of f. Hence $\mathrm{int}(f, G_h^{d_h}) = r_h d_h$ and $\mathrm{int}(f, \alpha_i(x,y)G_h^{d_h-i} = \mathrm{int}(f, \alpha_i(x,y) + (d_h - i)r_h$ for all i such that $\alpha_i(x,y) \neq 0$. Let $i, j \in \{0, \ldots, d_h - 1\}$, $i \neq j$, and assume that $\alpha_i(x,y) \neq 0 \neq \alpha_j(x,y)$. By a similar argument as in Lemma 76, we have $\mathrm{int}(f, \alpha_i(x,y)) + (d_h - i)r_h \neq \mathrm{int}(f, \alpha_j(x,y)) + (d_h - j)r_h$. Also if $\alpha_i(x,y) \neq 0$ for some $i \in \{1, \ldots, d_h - 1\}$, then $\mathrm{int}(f, \alpha_i(x,y)G_h^{d_h-i}) \neq \mathrm{int}(f, \alpha_{d_h}(x,y)$. Now $f(t^n, y(t)) = 0$. This implies

(1) $\mathrm{int}(f, \alpha_{d_h}) = r_h d_h = \mathrm{int}(f, G_h^{d_h})$,
(2) $\mathrm{int}(f, \alpha_i(x,y)) > ir_h$ for all $1 \leq i \leq d_h - 1$ such that $\alpha_i(x,y) \neq 0$.

It follows that $\mathrm{int}(f, \alpha_1(x,y) > r_h$, hence $\mathrm{int}(f, T(G_h)) = \mathrm{int}(f, G_h + \frac{\alpha_1(x,y)}{d_h}) = \mathrm{int}(f, G_h) = r_h$.

Let $k < h$ and let

$$f = G_{k+1}^{d_{k+1}} + \alpha_1(x,y)G_{k+1}^{d_{k+1}-1} + \cdots + \alpha_{d_{k+1}}(x,y)$$

be the G_{k+1}-adic expansion of f. Let also

$$G_{k+1} = G_k^{e_k} + \beta_1(x,y)G_k^{e_k-1} + \cdots + \beta_{e_k}(x,y)$$

be the G_k-adic expansion of G_{k+1}. Easy calculations show that $\alpha_1(x,y) = d_{h+1}\beta_1(x,y)$. Repeating the argument above for (G_{k+1}, G_k) instead of (f, G_h), we prove that $\mathrm{int}(G_{k+1}, \beta_1(x,y)) > \mathrm{int}(G_{k+1}, G_k) = \frac{r_k}{d_{k+1}}$, hence, by Proposition 77,

$$\mathrm{int}(f, \alpha_1(x,y)) = \mathrm{int}(f, \beta_1(x,y)) = d_{k+1}\mathrm{int}(G_{k+1}, \beta_1(x,y)) > r_k$$

In particular $\mathrm{int}(f, T(G_k)) = \mathrm{int}(f, G_k + \frac{\alpha_1(x,y)}{d_k}) = \mathrm{int}(f, G_k) = r_k$. □

Corollary 80. *Let $k \in \{1, \ldots, h\}$ and let G_k be a d_kth pseudo root of f. Then $T(G_k)$ is a d_kth pseudo root of f.*

Proof. Clearly $T(G_k)$ is a monic polynomial of degree $\frac{n}{d_k}$ in y. By Proposition 79, $\mathrm{int}(f, T(G_k)) = r_k$, and by Proposition 75, $T(G_k)$ is irreducible. This proves the result. □

Let d be a divisor of n and let g be a monic polynomial of f of degree $\frac{n}{d}$ in y. Let

$$f = g^d + \alpha_1(x,y)g^{d-1} + \cdots + \alpha_d(x,y)$$

be the g-adic expansion of f. We say that g is a *dth approximate root* of f if $\alpha_1(x,y) = 0$.

Lemma 81. *Let the notations be as above. A dth approximate root of f exists and it is unique.*

Proof. Let $G = y^{\frac{n}{d}}$ and let $f = G^d + \alpha_1(x,y)G^{d-1} + \cdots + \alpha_d(x,y)$ be the G-adic expansion of f. If $\alpha_1(x,y) = 0$, then G is a dth approximate root of f. If $\alpha_1(x,y) \neq 0$, then we set $G_1 = T(G) = G + \frac{\alpha_1(x,y)}{d}$. Let $f = G_1^d + \alpha_1^1(x,y)G_1^{d-1} + \cdots + \alpha_d^1(x,y)$ be the G_1-adic expansion of f. Easy calculations show that if $\alpha_1^1(x,y) \neq 0$, then $\deg_y \alpha_1^1(x,y) < \deg_y \alpha_1(x,y)$. In this case we restart with f and $G_2 = T(G_1)$. Clearly there exists k such that if $f = G_k^d + \alpha_1^k(x,y)G_k^{d-1} + \cdots + \alpha_d^k(x,y)$ is the G_k-adic expansion of f, then $\alpha_1^k(x,y) = 0$. Hence G_k is a d-th approximate root of f.

Let G, H be two dth approximate roots, and let $f = G^d + \alpha_2(x,y)G^{d-2} + \cdots + \alpha_d(x,y)$ and $f = H^d + \beta_2(x,y)H^{d-2} + \cdots + \beta_d(x,y))$ be the G-adic and H-adic expansion of f, respectively. We have $G^d - H^d = (G-H)(G^{d-1} + HG^{d-2} + \cdots + H^{d-1}) = \beta_2(x,y)H^{d-2} + \cdots + \beta_d(x,y) - (\alpha_2(x,y)G^{d-2} + \cdots + \alpha_d(x,y))$. If $G \neq H$, then $\deg_y(G-H) \geq 0$, but $\deg_y(G^{d-1} + HG^{d-2} + \cdots + H^{d-1}) = (d-1)\frac{n}{d} > \deg_y(\beta_2(x,y)H^{d-2} + \cdots + \beta_d(x,y) - (\alpha_2(x,y)G^{d-2} + \cdots + \alpha_d(x,y)))$. This is a contradiction. □

It results from Lemma 81 that, given a divisor d of n, a dth approximate root exists and it is unique. We denote it by $\mathrm{App}(f;d)$.

Proposition 82. *Let the notations be as above. For all $k \in \{1,\ldots,h\}$, $\mathrm{int}(f, \mathrm{App}(f;d_k)) = r_k$.*

Proof. Let $1 \leq k \leq h$ and let G_k be a d_kth pseudo root of f. By Proposition 77, $\mathrm{int}(f,G_k) = \mathrm{int}(f,T(G_k))$. But $\mathrm{App}(f,d_k)$ is obtained by applying the operation T finitely many times to G_k. Hence the result is a consequence of Proposition 78 and Corollary 80. □

Corollary 83. *For all $k \in \{1,\ldots,h\}$, $\mathrm{App}(f,d_k)$ is irreducible. In particular $\mathrm{App}(f,d_k)$ is a d_kth pseudo root of f.*

Proof. This results from Propositions 75 and 82. □

Next we shall introduce the notion of contact between two irreducible polynomials of $\mathbb{K}((x))[y]$. The notion tells us how far the parametrizations of these two polynomials are close.

Let g be a monic irreducible polynomial of $\mathbb{K}((x))[y]$, of degree p in y and let $z_1(t), \cdots, z_p(t)$ be the set of roots of $g(t^p, y) = 0$. We define the *contact* of f with g, denoted $c(f,g)$, to be:

$$\mathrm{c}(f,g) = \frac{1}{np} \max_{i,j} \mathrm{ord}_t(y_i(t^p) - z_j(t^n))$$

Note that $\mathrm{c}(f,g) = \frac{1}{np}\max_i \mathrm{ord}_t(y_i(t^p) - z(t^n)) = \frac{1}{np}\max_j \mathrm{ord}_t(y(t^p) - z_j(t^n))$ where $y(t)$ and $z(t)$ are roots of $f(t^n,y) = 0$ and $g(t^p,y) = 0$, respectively.

Proposition 84. *Let g be an irreducible monic polynomial of $\mathbb{K}((x))[y]$ and let $p = \deg_y g$. We have the following.*

(1) $\mathrm{c}(f,g) < \frac{m_1}{n}$ if and only if $\mathrm{int}(f,g) = np\mathrm{c}(f,g)$.
(2) $\frac{m_k}{n} < c = \mathrm{c}(f,g) \leq \frac{m_{k+1}}{n}$ for some $k \in \{1,\ldots,h\}$ (with the assumption that $m_{h+1} = +\infty$) if and only if $\mathrm{int}(f,g) = (r_k d_k + nc - m_k)\frac{p}{n}$

Proof. Let $z(t)$ be a root of $g(t^p,y) = 0$. We have $\mathrm{int}(f,g) = \mathrm{ord}_t f(t^p, z(t))$. Note that $f(t^p, z(t)) = f((t^{\frac{p}{n}})^n, z(t))$. Also, $f(t^n,y) = \prod_{i=1}^n (y - y_i(t))$. Hence $f((t^{\frac{p}{n}})^n, y) = \prod_{i=1}^n (y -$

$y_i(t^{\frac{p}{n}})$), which implies that $f(t^p, z(t)) = \prod_{i=1}^{n}(z(t) - y_i(t^{\frac{p}{n}}))$, and it follows that

$$\operatorname{int}(f,g) = \operatorname{ord}_t f(t^p, z(t)) = \frac{1}{n}\operatorname{ord}_t\left(\prod_{i=1}^{n}(z(t^n) - y_i(t^p))\right) = \frac{1}{n}\sum_{i=1}^{n}\operatorname{ord}_t(z(t^n) - y_i(t^p)).$$

Suppose, without loss of generality, that $\mathrm{c}(f,g) = \frac{1}{np}\operatorname{ord}_t(y_1(t^p) - z(t^n))$. It follows that $\operatorname{int}(f,g) \leq \operatorname{ord}_t(y_1(t^p) - z(t^n)) \leq npc(f,g)$.

If $c(f,g) < \frac{m_1}{n}$, then $\operatorname{ord}_t(y_1(t^p) - z(t^n)) < m_1 p$. Let $2 \leq i \leq n$. We have $z(t^n) - y_i(t^p) = z(t^n) - y_1(t^p) + y_1(t^p) - y_i(t^p)$ and by Lemma 69, $\operatorname{ord}_t(y_1(t^p) - y_i(t^p)) \geq pm_1$, hence $\operatorname{ord}_t(z(t^n) - y_i(t^p)) = \operatorname{ord}_t(z(t^n) - y_1(t^p))$. Finally $\operatorname{ord}_t f(t^p, z(t)) = \operatorname{ord}_t(z(t^n) - y_1(t^p)) = npc(f,g)$. Conversely, if $\operatorname{int}(f,g) = npc(f,g)$, then $\operatorname{ord}_t(y_i(t) - z(t)) = \operatorname{ord}_t(y_1(t) - z(t))$ for all $i \in \{2, \ldots, n\}$. This is true only if $\mathrm{c}(f,g) < \frac{m_1}{n}$. This proves (1).

Suppose that $c(f,g) \geq \frac{m_1}{n}$ and let k be the greatest element such that $\frac{m_k}{n} \leq c(f,g) < \frac{m_{k+1}}{n}$. Let $2 \leq i \leq n$. We have $z(t^n) - y_i(t^p) = z(t^n) - y_1(t^p) + y_1(t^p) - y_i(t^p)$. Hence

$$\operatorname{ord}_t(z(t^n) - y_i(t^p)) = \begin{cases} \operatorname{ord}_t(z(t^n) - y_1(t^p)) & \text{if } \operatorname{ord}_t(y_i(t) - y_1(t)) > m_k, \\ \operatorname{ord}_t(y_1(t^p) - y_i(t^p)) & \text{if } \operatorname{ord}_t(y_i(t) - y_1(t)) \leq m_k. \end{cases}$$

By Lemma 69, $\operatorname{ord}_t f(t^p, z(t)) = \frac{1}{n}\sum_{i=1}^{n}\operatorname{ord}_t(z(t^n) - y_i(t^p)) = \frac{1}{n}(d_{k+1}\operatorname{ord}_t(z(t^n) - y_1(t^p)) + p\sum_{i=1}^{k}(d_i - d_{i+1})m_i) = \frac{1}{n}(d_{k+1}npc(f,g) + p(r_k d_k - m_k d_{k+1})) = \frac{p}{n}(d_{k+1}nc(f,g)) + \frac{p}{n}(r_k d_k - m_k d_{k+1}) = \frac{p}{n}(r_k d_k + (nc(f,g) - m_k)d_{k+1})$.

Conversely, suppose that $\operatorname{int}(f,g) = (r_k d_k + nc - m_k)\frac{p}{n}$ for some $k \geq 1$. If $c < \frac{m_1}{n}$, then $\operatorname{int}(f,g) = npc < np\frac{m_1}{n} = pm_1 = pr_1 = (r_1 d_1)\frac{p}{n} \leq (r_k d_k + nc - m_k)\frac{p}{n}$, which is a contradiction. Hence $c(f,g) \geq \frac{m_1}{n}$, and a similar argument shows that $c = \mathrm{c}(f,g)$. This proves (2). □

Corollary 85. *Let $k \in \{1, \ldots, h\}$ and let G_k be a pseudo-root of f. We have $\mathrm{c}(f, G_k) = \frac{m_k}{n}$. In particular $\mathrm{c}(f, \operatorname{App}_{d_k}(f)) = \frac{m_k}{n}$.*

Proof. By Proposition 71, $\operatorname{int}(f, G_k) = r_k = (r_k d_k + (n\frac{m_k}{n} - m_k)d_{k+1})\frac{n/d_k}{n}$. Hence $\mathrm{c}(f, G_k) = m_k$ by Proposition 84. □

Proposition 86. *Let g be a monic irreducible polynomial of $\mathbb{K}((x))[y]$ of degree p in y. If $\mathrm{c}(f,g) > \frac{m_k}{n}$, for some $k \in \{1, \ldots, h\}$, then $\frac{n}{d_{k+1}}$ divides p. In particular, if $\mathrm{c}(f,g) > \frac{m_h}{n}$, then n divides p.*

Proof. Let $z(t)$ be a root of $g(t^p, y) = 0$ and assume, without loss of generality, that $\mathrm{c}(f,g) = \frac{1}{np}\operatorname{ord}_t(z(t^n) - y_1(t^p))$. Write $y_1(t) = \sum_i a_i t^i$ and $z(t) = \sum_j b_j t^j$. The hypothesis implies that for all i in $\operatorname{Supp}(y_1(t))$ with $i \leq m_k$, there exist $j \in \operatorname{Supp}(z(t))$ such that $jn = ip$, that is, $j = i\frac{p}{n} \in \mathbb{N}$. But $\gcd(i \in \operatorname{Supp}(y_1(t)), i \leq m_k) = d_{k+1}$, whence $d_{k+1}\frac{p}{n} \in \mathbb{N}$, which implies that $\frac{n}{d_{k+1}}$ divides n. □

Proposition 87. *Let g be a monic polynomial of $\mathbb{K}((x))[y]$ and assume that $\deg_y g = n$. If $\operatorname{int}(f,g) > r_h d_h$, then g is irreducible.*

Proof. Let $g = g_1 \cdots g_r$ be the decomposition of g into irreducible components in $\mathbb{K}((x))[y]$. If $r > 1$ then, by Proposition 86, $\deg_y g_i < n$ for all $1 \leq i \leq r$. Thus $\mathrm{c}(f, g_i) < m_h$ for all $1 \leq i \leq r$. By Proposition 84, $\operatorname{int}(f, g_i) < r_h d_h \frac{\deg_y g_i}{n}$, hence $\operatorname{int}(f, g_i) = \sum_{i=1}^{r}\operatorname{int}(f, g_i) < r_h d_h$, which is a contradiction. This proves our assertion. □

3.2. **The local case.** In the following we shall assume that $f(x,y)$ is an irreducible polynomial of $\mathbb{K}[\![x]\!][y]$. Note that in this case, for all $k \in \{1\dots,h\}$, $m_k > 0$ and $G_k \in \mathbb{K}[\![x]\!][y]$ for every d_kth pseudo root G_k of f.

Let $\mathrm{g}(x,y)$ be a nonzero element of $\mathbb{K}[\![x]\!][y]$ and recall that the intersection multiplicity of f with g, denoted $\mathrm{int}(f,g)$, is defined to be the order in t of $\mathrm{g}(t^n, y(t))$. Note that this definition does not depend on the choice of the root $y(t)$ of $f(t^n,y)=0$ and also that $\mathrm{int}(f,g) \geq 0$.

The set $\{\mathrm{int}(f,g) : g \in \mathbb{K}[\![x]\!][y]\}$ is a semigroup of $\mathbb{N}$. We call it the *semigroup of* f and denote it by $\Gamma(f)$.

Let $g_k = \mathrm{App}(f, d_k)$ for all $1 \leq k \leq h$. Recall that $\mathrm{int}(f, g_k) = r_k$.

Proposition 88. *Under the standing hypothesis.*

(i) The semigroup $\Gamma(f)$ is generated by $r_0, \dots, r_h$.
(ii) $\Gamma(f)$ is a numerical semigroup.
(iii) $\Gamma(f)$ is free for the arrangement $(r_0, \dots, r_h)$.
(iv) For all $k \in \{1, \dots, h\}$, $r_k d_k < r_{k+1} d_{k+1}$.

Proof. (i) Follows from Proposition 73.
(ii) Follows from the fact that $d_{h+1} = \gcd(r_0, \cdots, r_h) = 1$.
(iii) Is a consequence of Lemma 68 and Lemma 76.
(iv) For all $k \in \{1, \dots, h\}$, we have $r_{k+1}d_{k+1} = r_k d_k + (m_{k+1} - m_k)d_{k+1}$ and $m_k < m_{k+1}$, whence $r_k d_k < r_{k+1} d_{k+1}$. □

Conversely we have the following.

Proposition 89. *Let $r_0 < r_1 < \cdots < r_h$ be a sequence of nonzero elements of $\mathbb{N}$ and let $d_1 = r_0$ and $d_{k+1} = \gcd(r_k, d_k)$ for all $1 \leq k \leq h$. Assume that the following conditions hold:*

(1) $d_{h+1} = 1$,
(2) for all $k \in \{1, \dots, h\}$, $r_k d_k < r_{k+1} d_{k+1}$,
(3) the semigroup $\Gamma = \langle r_0, \dots, r_h \rangle$ is free for the arrangement $(r_0, \dots, r_h)$.

Then there exists a monic irreducible polynomial $f(x,y) \in \mathbb{K}[\![x]\!][y]$ of degree r_0 in y such that $\Gamma(f) = \Gamma$.

Proof. Let $r_0 = n$ and $m_1 = r_1$, and for all $1 \leq k \leq h$ let $m_{k+1} = r_{k+1} - r_k \frac{d_k}{d_{k+1}} + m_k$. Finally let $y(t) = t^{m_1} + t^{m_2} + \cdots + t^{m_h} \in \mathbb{K}[\![t]\!]$. Let $f(x,y)$ is the minimal polynomial of $y(t)$ over $\mathbb{K}((t^n))$. We have

$$f(x,y) = \prod_{w^n=1} (y - y(wt)).$$

Now $\mathrm{Supp}(y(t)) = \{m_1, \dots, m_h\}$, hence $\underline{m} = (m_1, \dots, m_h)$ is nothing but the sequence of Newton-Puiseux exponents of f, and consequently $\Gamma(f) = \langle r_0, \dots, r_h \rangle$. □

Let f_x, f_y denote the partial derivatives of f. Let H be an irreducible component of f_y. Let $\deg_y H = n_H$ and write $H(t^{n_H}, y) = \prod_{i=1}^{n_H} (y - z_i(t))$. By the chain rule of derivatives we have:

$$\frac{d}{dt} f(t^{n_H}, z_1(t)) = \frac{df}{dx}(t^{n_H}, z_1(t))(n_H t^{n_H - 1}) + \frac{df}{dy}(t^{n_H}, z_1(t))(z_1'(t)) = \frac{df}{dx}(t^{n_H}, z_1(t))(n_H t^{n_H - 1}).$$

It follows that $\mathrm{int}(f, H) - 1 = \mathrm{int}(f_x, H) + n_H - 1$. Adding this equality over the set of irreducible components of f_y, we get that

$$\mathrm{int}(f, f_y) = \mathrm{int}(f_x, f_y) + n - 1.$$

Write $f(t^n,y)=\prod_{i=1}^n(y-y_i(t))$. We have $f_y(t^n,y)=\sum_{i=1}^n\prod_{k\neq i}(y-y_k(t))$. Hence $f_y(t^n,y_1(t))=\prod_{k=2}^n(y_1(t)-y_k(t))$, and $\mathrm{int}(f,f_y)=\sum_{k=2}^n\mathrm{ord}_t(y_1(t)-y_k(t))=\sum_{k=1}^h(d_k-d_{k+1})m_k$ (see Lemma 69). But $\sum_{k=1}^h(d_k-d_{k+1})m_k=r_hd_h-m_h=\sum_{k=1}^h(e_k-1)r_k$. Finally

$$\mathrm{int}(f,f_y)=\sum_{k=1}^h(e_k-1)r_k=\mathrm{int}(f_x,f_y)+n-1.$$

Note that the conductor $\mathrm{C}(\Gamma(f))=\sum_{k=1}^h(e_k-1)r_k-n+1$. Hence

$$\mathrm{C}(\Gamma(f))=\mathrm{int}(f_x,f_y).$$

3.3. **The case of curves with one place at infinity.** Let the notations be as above and assume that $f(x,y)\in\mathbb{K}[x^{-1}][y]$ and also that $f(x,y)$ is irreducible in $\mathbb{K}((x))[y]$.

Let $\mathrm{g}(x,y)$ be a nonzero element of $\mathbb{K}[x^{-1}][y]$. As above, we define the intersection multiplicity of f with g, denoted $\mathrm{int}(f,g)$, to be the order in t of $\mathrm{g}(t^n,y(t))$. Note that this definition does not depend on the choice of the root $y(t)$ of $f(t^n,y)=0$.

The set $\{\mathrm{int}(f,g):g\in\mathbb{K}[x^{-1}][y]\}$ is a semigroup of $-\mathbb{N}$. We call it the *semigroup of* f and we denote it by $\Gamma(f)$. For all $k\in\{1,\dots,h\}$, let $g_k=\mathrm{App}_{d_k}(f)$, and let $-r_k=\mathrm{int}(f,g_k)$.

Proposition 90. *Under the standing hypothesis.*

(i) The semigroup $\Gamma(f)$ is generated by $-r_0,\dots,-r_h$.
(ii) $-\Gamma(f)=\{-r\mid r\in\Gamma(f)\}$ is a numerical semigroup.
(iii) $-\Gamma(f)$ is free for the arrangement $(r_0,\dots,r_h)$.
(iv) For all $1\leq k\leq h$, $-r_kd_k<-r_{k+1}d_{k+1}$.

Proof. (i) follows from Proposition 73, while (ii) holds because $d_{h+1}=1$.

(iii) is a consequence of Lemma 76.

Finally, for all $k\in\{1,\dots,h\}$, $-r_{k+1}d_{k+1}=-r_kd_k+(m_{k+1}-m_k)d_{k+1}$ and $m_k<m_{k+1}$. Hence $-r_kd_k<-r_{k+1}d_{k+1}$ and (iv) follows. □

Let f_x,f_y denote the partial derivatives of f. Let H be an irreducible component of f_y. Let $\deg_y H=n_H$ and write $H(t^{n_H},y)=\prod_{i=1}^{n_H}(y-z_i(t))$. Arguing as above, by the chain rule of derivatives we have:

$$\frac{d}{dt}f(t^{n_H},z_1(t))=\frac{df}{dx}(t^{n_H},z_1(t))(n_Ht^{n_H-1})+\frac{df}{dy}(t^{n_H},z_1(t))(z_1'(t))=\frac{df}{dx}(t^{n_H},z_1(t))(n_Ht^{n_H-1}).$$

It follows that $\mathrm{int}(f,H)-1=\mathrm{int}(f_x,H)+n_H-1$. Adding this equality over the set of irreducible components of f_y, we get that

$$\mathrm{int}(f,f_y)=\mathrm{int}(f_x,f_y)+n-1.$$

Now write $f(t^n,y)=\prod_{i=1}^n(y-y_i(t))$. We have $f_y(t^n,y)=\sum_{i=1}^n\prod_{k\neq i}(y-y_k(t))$. Hence $f_y(t^n,y_1(t))=\prod_{k=2}^n(y_1(t)-y_k(t))$, and $\mathrm{int}(f,f_y)=\sum_{k=2}^n\mathrm{ord}_t(y_1(t)-y_k(t))=\sum_{k=1}^h(d_k-d_{k+1})m_k$ (see Lemma 69). But $\sum_{k=1}^h(d_k-d_{k+1})m_k=(-r_h)d_h-m_h=\sum_{k=1}^h(e_k-1)(-r_k)$. Finally

$$\mathrm{int}(f,f_y)=\sum_{k=1}^h(e_k-1)(-r_k)=\mathrm{int}(f_x,f_y)+n-1.$$

Let $F=y^n+a_1(x)y^{n-1}+\cdots+a_n(x)$ be a nonzero polynomial of $\mathbb{K}[x][y]$ and assume, possibly after a change of variables, that $\deg_x a_i(x)<i$ for all $i\in\{1,\dots,n\}$ such that $a_i(x)\neq 0$.

Let $C = \mathrm{V}(F)$ be the algebraic curve $F = 0$ and let $h_F(u, x, y) = u^n F(\frac{x}{u}, \frac{y}{u})$. The projective curve $\mathrm{V}(h_F)$ is the projective closure of C in $\mathbf{P}^2_{\mathbb{K}}$. By hypothesis, $(0, 1, 0)$ is the unique point of $\mathrm{V}(h_F)$ at the line at infinity $u = 0$. We say that F *has one place at infinity* if h_F is analitycally irreducible at $(0, 1, 0)$. Set $F_\infty(u, y) = h_F(u, 1, y)$. Then F has one place at infinity if and only if the formal power series $F_\infty(u, y)$ is irreducible in $\mathbb{K}[\![u]\!][y]$.

Lemma 91. *Let the notations be as above. Let $f(x, y) = F(x^{-1}, y) \in \mathbb{K}[x^{-1}, y]$.*

(1) $f(x, x^{-1}y) = x^{-n}F_\infty(x, y)$.

(2) F has one place at infinity if and only if $f(x, y)$ is irreducible in $\mathbb{K}((x))[y]$.

Proof. Write $F(x, y) = y^n + \sum_{i+j<n} a_{ij}x^i y^j$. We have $f(x, y) = y^n + \sum_{i+j<n} a_{ij}x^{-i}y^j$. Hence $f(x, x^{-1}y) = x^{-n}y^n + \sum_{i+j<n} a_{ij}x^{-i-j}y^j = x^{-n}(y^n + \sum_{i+j<n} a_{ij}x^{n-i-j}y^j) = x^{-n}F_\infty(x, y)$. This proves (1).

Now suppose that f is irreducible in $\mathbb{K}((x))[y]$. If $F_\infty(x, y)$ is not irreducible in $\mathbb{K}[\![x]\!][y]$, then $F = F_1F_2, F_1, F_2 \in \mathbb{K}[\![x]\!][y]$ and $\deg_y F_i = n_i > 0$. But $\tilde{f}(x, y) = f(x, x^{-1}y) = x^{-n}F_\infty(x, y) = x^{-n_1}F_1x^{-n_2}F_2$ and $f(x, y) = \tilde{f}(x, xy) = x^{-n_1}F_1(x, xy)x^{-n_2}F_2(x, y) = f_1(x, y)f_2(x, y)$ with $f_1, f_2 \in \mathbb{K}((x))[y]$ and $\deg_y f_1 = n_1$, $\deg_y f_2 = n_2$. This is a contradiction. A similar argument proves the converse. □

Assume that $F(x, y)$ has one place at infinity. Let $G(x, y)$ be a nonzero element of $\mathbb{K}[x, y]$ and denote by $\mathrm{Int}(F, G)$ the rank of the $\mathbb{K}$-vector space $\mathbb{K}[x, y]/(F, G)$. After possibly a change of variables ($y = Y^q - x$, $x = Y$, $q \gg 0$, for example), we may assume that $G(x, y) = y^p + \sum_{i+j<p} b_{ij}x^i y^j$.

Proposition 92. *Let the notations be as above, in particular $G(x, y) = y^p + \sum_{i+j<p} b_{ij}x^i y^j \in \mathbb{K}[x, y]$. Let $f(x, y) = F(x^{-1}, y)$ and $g(x, y) = G(x^{-1}, y)$. We have $\mathrm{Int}(F, G) = -\mathrm{int}(f, g)$.*

Proof. Let $y(t)$ be a root of $f(t^n, y) = 0$. We have $\mathrm{int}(f, g) = \mathrm{ord}_t g(t^n, y(t))$. Also, $F_\infty(x, y) = x^n f(x, x^{-1}y)$ and $G_\infty(x, y) = x^p g(x, x^{-1}y)$. It follows that $F_\infty(t^n, t^n y(t)) = t^{2n}f(t^n, t^{-n}t^n y(t)) = t^{2n}f(t^n, y(t)) = 0$. Hence $t^n y(t)$ is a root of $F_\infty(t^n, y) = 0$. Now

$$\begin{aligned}\mathrm{int}(F_\infty, G_\infty) = \mathrm{ord}_t G_\infty(t^n, t^n y(t)) &= \mathrm{ord}_t(x^p g(x, x^{-1}y))(t^n, t^n y(t)) \\ &= \mathrm{ord}_t(t^{np}) + \mathrm{ord}_t g(t^n, y(t)) = np + \mathrm{int}(f, g).\end{aligned}$$

Finally $\mathrm{int}(F_\infty, G_\infty) - \mathrm{int}(f, g) = np$. By Bézout's Theorem, $\mathrm{int}(F_\infty, G_\infty) + \mathrm{Int}(F, G) = np$. This implies that $\mathrm{Int}(F, G) = -\mathrm{int}(f, g)$. □

More generally we have the following:

Proposition 93. *Assume that $F(x, y)$ has one place at infinity and let $G(x, y)$ be a nonzero element of $\mathbb{K}[x, y]$. Let $f(x, y) = F(x^{-1}, y)$ and $g(x, y) = G(x^{-1}, y)$. We have $\mathrm{Int}(F, G) = -\mathrm{int}(f, g)$.*

Proof. Let $G(x, y) = G_p + G_{p-1} + \cdots + G_0$ be the decomposition of G into homogeneous components. Write $G_p = \prod_{k=1}^s (a_k y + b_k x)^{p_k}$.

i) If for all $1 \le k \le s, b_k \neq 0$, then F and G do not have common points at infinity. By Bézout theorem, $\mathrm{Int}(F, G) = np$. For all $0 \le i \le p$, write $g_{p-i}(x, y) = G_{p-i}(x^{-1}, y)$. We have $g(x, y) = \sum_{i=0}^p g_{p-i}(x, y)$, and if $y(t)$ is a root of $f(t^n, y) = 0$, then $g_p(t^n, y(t)) = \prod_{k=1}^s (a_k y(t) + b_k t^{-n})^{p_k}$, hence $\mathrm{ord}_t g_p(t^n, y(t)) = -np = \mathrm{ord}_t(x^{-p})(t^n, y(t))$. Furthermore, if $g_{p-i}(x, y) = \sum_{k+l=p+i} b_{kl}x^{-k}y^l$, then $\mathrm{ord}_t g_{p-i}(t^n, y(t)) \ge \min_{k,l}(-kn - lm) \ge \min_{k,l}(-kn - ln) = -(p - i)n > -pn$ for all $1 \le i \le p$. It follows that $\mathrm{Int}(F, G) = -\mathrm{int}(f, g)$.

ii) Suppose that $b_1 = 0$, and that, without loss of generality, $a_1 = 1$. We have $G_p = y^{p_1}\prod_{k=2}^{s}(a_k y + b_k x)^{p_k}$ and $b_k \neq 0$ for all $2 \leq k \leq s$. Let $P(0:1:0)$ be the unique common point of F and G at infinity. We have $\mathrm{int}(F_\infty, G_\infty) = \mathrm{int}_P(F, G)$, and by Bézout theorem, $\mathrm{Int}(F, G) + \mathrm{int}_P(F, G) = np$. Clearly $F_\infty(x, y)$ is the local equation of F at P. Let $g_p(x, y) = G_p(x^{-1}, y)$ and write $g(x, y) = g_p(x, y) + \sum_{k+l<p} b_{kl}x^{-k}y^l$. We have

$$\begin{aligned} g(x, x^{-1}y) &= x^{-p_1}y^{p_1}\prod_{k=2}^{s}(a_k x^{-1}y + b_k x^{-1})^{p_k} + \sum_{k+l<p} b_{kl}x^{-k}x^{-l}y^l \\ &= x^{-p}(y^{p_1}\prod_{k=2}^{s}(a_k y + b_k)^{p_k} + \sum_{k+l<p} x^{p-k-l}y^l). \end{aligned}$$

Hence the local equation of G at P, denoted G_P, is given by $G_P(x, y) = x^p g(x, x^{-1}y)$. Now the same calculations as in Proposition 92 show that $\mathrm{int}(F_\infty, G_P) = np + \mathrm{int}(f, g)$, hence $\mathrm{Int}(F, G) = -\mathrm{int}(f, g)$.

□

Proposition 94. *Let the notations be as above. If F has one place at infinity, then so is for $F(x, y) - \lambda$, for all $\lambda \in \mathbb{K}^*$.*

Proof. Clearly $\mathrm{Int}(F, F - \lambda) = 0 = \mathrm{int}(f, f - \lambda) > -r_h d_h$. By Proposition 87, $f - \lambda$ is irreducible in $\mathbb{K}((x))[y]$, hence $F - \lambda$ has one place at infinity by Lemma 91. This proves our assertion. □

Remark 95. The result of Proposition 94 is proper to curves with one place at infinity. More precisely, for all $N > 1$, there exist a polynomial F with N places at infinity and $\lambda \in \mathbb{K}^*$ such that the number of places of $F - \lambda$ at infinity is not equal to N.

Let

$$\Gamma_\infty(F) = \{\mathrm{Int}(F, G) \mid G \in \mathbb{K}[x][y]\}.$$

Lemma 91 and the calculations above imply the following.

Proposition 96. *Under the standing hypothesis.*

(i) The semigroup $\Gamma_\infty(F)$ is generated by $r_0, \ldots, r_h$.
(ii) $\Gamma_\infty(F)$ is a numerical semigroup.
(iii) $\Gamma_\infty(F)$ is free for the arrangement $(r_0, \ldots, r_h)$.
(iv) For all $k \in \{1, \ldots, h\}$, $r_k d_k > r_{k+1}d_{k+1}$.
(v) $\mathrm{Int}(F, F_y) = \mathrm{Int}(F_x, F_y) + n - 1 = \sum_{k=1}^{h}(e_k - 1)r_k$.
(vi) The conductor $\mathrm{C}(\Gamma_\infty(F)) = \mathrm{Int}(F_x, F_y) = (\sum_{k=1}^{h}(e_k - 1)r_k) - n + 1$.

Example 97. Sequences fulfilling the Condition (iv) in Proposition 96 are known as δ-sequences.

```
gap> DeltaSequencesWithFrobeniusNumber(11);
[ [ 5, 4 ], [ 6, 4, 9 ], [ 7, 3 ], [ 9, 6, 4 ], [ 10, 4, 5 ], [ 13, 2 ] ]
gap> List(last, CurveAssociatedToDeltaSequence);
[ y^5-x^4, y^6-2*x^2*y^3+x^4-x^3, y^7-x^3, y^9-3*x^2*y^6+3*x^4*y^3-x^6-y^2,
  y^10-2*x^2*y^5+x^4-x, y^13-x^2 ]
gap> List(last,SemigroupOfValuesOfPlaneCurveWithSinglePlaceAtInfinity);
[ <Modular numerical semigroup satisfying 5x mod 20 <= x >,
  <Numerical semigroup with 3 generators>,
```

```
  <Modular numerical semigroup satisfying 7x mod 21 <= x >,
  <Numerical semigroup with 3 generators>,
  <Numerical semigroup with 3 generators>,
  <Modular numerical semigroup satisfying 13x mod 26 <= x > ]
gap> List(last,MinimalGeneratingSystemOfNumericalSemigroup);
[ [ 4, 5 ], [ 4, 6, 9 ], [ 3, 7 ], [ 4, 6, 9 ], [ 4, 5 ], [ 2, 13 ] ]
```

Corollary 98. *Let the notations be as above. If* $\mathrm{Int}(F_x, F_y) = 0$*, then* $r_k = d_{k+1}$ *for all* $k \in \{1, \ldots, h\}$*. In particular,* $\Gamma_\infty(F) = \mathbb{N}$ *and* r_1 *divides* n*.*

Proof. For all $1 \leq k \leq h, r_k \geq d_{k+1}$. If $r_i > d_{i+1}$ for some $1 \leq i \leq h$, we get $\sum_{k=1}^{h}(e_k - 1)r_k) - n + 1 > (\sum_{k=1}^{h}(d_k - d_{k+1})) - n + 1 = 0$, which contradicts the hypothesis. This proves the first assertion. Since $r_h = d_{h+1} = 1$, then $\Gamma_\infty(F) = \mathbb{N}$. On the other hand, $r_1 = d_2 = \gcd(n, r_1)$, whence r_1 divides n. □

Proposition 99. *Let the notations be as above. If* $d_2 < r_1$ *(that is,* r_1 *does not divide* n*), then* $\mathrm{Int}(F_x, F_y) \geq n - 1$ *with equality if and only if* $r_k = 2d_{k+1}$ *for all* $1 \leq k \leq h$*.*

Proof. We have $\mathrm{Int}(F_x, F_y) + n - 1 = (\sum_{k=1}^{h}(e_k - 1)r_k)$. But $r_k \geq 2d_{k+1}$ for all $1 \leq k \leq n$. Hence $\sum_{k=1}^{h}(e_k - 1)r_k \geq 2\sum_{k=1}^{h}(e_k - 1)d_{k+1} \geq 2\sum_{k=1}^{h}(d_k - d_{k+1}) = 2(n-1)$. In particular. $\mathrm{Int}(F_x, F_y) \geq n - 1$. Clearly, if $r_k > 2d_{k+1}$ for some $k \in \{1, \ldots, n\}$, then $\mathrm{Int}(F_x, F_y) > n - 1$. This proves our assertion. □

Corollary 100. *(i) Let* $h = 1$*, then* $\mathrm{Int}(F_x, F_y) = n - 1$ *if and only if* $\Gamma_\infty(F) = \langle n, 2\rangle$*.*
(ii) Let $h \geq 2$ *and suppose that* $d_2 < r_1$*. If* 2 *does not divide* n*, then* $\mathrm{Int}(F_x, F_y) > n - 1$*.*

Proof. (i) follows from Proposition 96. If 2 does not divide n, then $r_2 > 2d_3$. Hence $\mathrm{Int}(F_x, F_y) > n - 1$. This proves (ii). □

Let the notations be as above and assume that F has one place at infinity. It follows that $F_\infty(u, y)$ is a monic irreducible polynomial of $\mathbb{K}[\![u]\!][y]$ of degree n in y. Let $f(t^n, y) = \prod_{i=1}^{n}(y - y_i(t))$. We have, as in the proof of Proposition 92, $f(t^n, t^{-n}y) = \prod_{i=1}^{n}(t^{-n}y - y_i(t)) = t^{-n^2}\prod_{i=1}^{n}(y - t^n y_i(t))$. Also $F_\infty(x, y) = x^n f(x, x^{-1}y)$, and thus

$$F_\infty(t^n, y) = \prod_{i=1}^{n}(y - t^n y_i(t)).$$

In particular, the roots of $F(t^n, y) = 0$ are given by $Y_i(t) = t^n y_i(t)$.

Proposition 101. *(i) The set of characteristic exponents of* F_∞ *is given by* $\bar{m}_k = n + m_k$*.*
(ii) The $\underline{d}$*-sequence of* F_∞ *is equal to the* $\underline{d}$*-sequence of* f*.*
(iii) The $\underline{r}$*-sequence of* F_∞ *is given by* $\bar{r}_k = n\frac{n}{d_k} - r_k$
(iv) For all $k \in \{1, \ldots, h\}$*,* $\mathrm{App}(F_\infty, d_k) = h_{G_k}(u, 1, y)$*, where we recall that* $G_k = \mathrm{App}(F, d_k)$*.*

Proof. (i) The formal power series $Y_1(t) = t^n y_1(t)$ is a root of $F_\infty(t^n, y) = 0$. Hence $\mathrm{Supp}(Y_1(t)) = \{n + i, i \in \mathrm{Supp}(y_1(t))\} = n + \mathrm{Supp}(y_1(t))$. Now the proof of (i) follows immediately.

(ii) In fact, for all k with $1 \leq k \leq h$, we have $\gcd(n, m_1, \ldots, m_k) = \gcd(n, n + m_1, \ldots, n + m_k)$.

(iii) We shall prove the result by induction on k, with $1 \leq k \leq h$. We have $\bar{r}_0 = n$ and $\bar{r}_1 = n + m_1 = n - r_1 = n\frac{n}{d_1} - r_1$. Suppose that $\bar{r}_k = n\frac{n}{d_k} - r_k$ for some $1 < k \leq h$. We

have $\bar{r}_{k+1}d_{k+1} = \bar{r}_k d_k + (n + m_{k+1} - (n + m_k))d_{k+1} = (n\frac{n}{d_k} - r_k)d_k + (m_{k+1} - m_k)d_{k+1} = (-r_k d_k + (m_{k+1} - m_k)d_{k+1}) + n^2 = -r_{k+1}d_{k+1} + n^2$. Hence $\bar{r}_{k+1} = n\frac{n}{d_{k+1}} - r_{k+1}$.

(iv) Easy exercise.

□

Proposition 102. *Let the notations be as above and let $\Gamma(F_\infty)$ be the numerical semigroup associated with F_∞. We have the following:*

(i) The conductor of $\Gamma(F_\infty)$ is given by $\mathrm{C}(\Gamma(F_\infty)) = (\sum_{k=1}^{h}(e_k - 1)\bar{r}_k) - n + 1 = (\sum_{k=1}^{h}(e_k - 1)(n\frac{n}{d_k} - r_k)) - n + 1$.

(ii) $\mathrm{C}(\Gamma(F_\infty)) + \mathrm{C}(\Gamma_\infty(F)) = (n-1)(n-2)$.

Proof. (i) Follows from Proposition 96.

(ii) $C(\Gamma(F_\infty)) + C(\Gamma_\infty(F)) = (\sum_{k=1}^{h}(e_k - 1)(n\frac{n}{d_k} - r_k)) - n + 1 + \sum_{k=1}^{h}(e_k - 1)r_k - n + 1 = (\sum_{k=1}^{h}(e_k - 1)(n\frac{n}{d_k})) - 2(n-1) = n(n-1) - 2(n-1) = (n-1)(n-2)$. □

Corollary 103. *Let the notations be as above. The following are equivalent.*

(i) $\mathrm{C}(\Gamma_\infty(F)) = 0$.

(ii) $\mathrm{C}(\Gamma(F_\infty)) = (n-1)(n-2)$.

(iii) For all $k \in \{1, \ldots, h\}$, $r_k = d_{k+1}$.

(iv) For all $k \in \{1, \ldots, h\}$, $\bar{r}_k = n\frac{n}{d_k} - d_{k+1}$.

Proof. This follows from Corollary 98 and Proposition 102. □

Corollary 104. *Let the notations be as above. Then $\mathrm{C}(\Gamma(F_\infty)) \leq (n-1)(n-3)$ and the following are equivalent.*

(i) $\mathrm{C}(\Gamma(F_\infty)) = (n-1)(n-3)$.

(ii) $\mathrm{C}(\Gamma_\infty(F)) = n - 1$.

(iii) For all $k \in \{1, \ldots, h\}$, $r_k = 2d_{k+1}$.

(iv) For all $k \in \{1, \ldots, h\}$, $\bar{r}_k = n\frac{n}{d_k} - 2d_{k+1}$.

Proof. This follows from Corollary 99 and Proposition 102. □

4. Minimal presentations

It is usual in Mathematics to represent objects by means of a free object in some generators under certain relations fulfilled by these generators. The reader familiar to Group Theory surely has used many times definitions of groups by means of generators and relations. Relations are usually represented by means of equalities, or simply words in the free group on the generators (this means that they are equal to the identity element; this is due to the fact that we have inverse in groups). Here we represent relations by pairs.

Let S be a numerical semigroup minimally generated by $\{n_1, \ldots, n_p\}$. Then the monoid morphism

$$\varphi : \mathbb{N}^p \to S,\ \varphi(a_1, \ldots, a_p) = \sum_{i=1}^{p} a_i n_i,$$

known as the *factorization homomorphism* of S, is an epimorphism, and consequently S is isomorphic to $\mathbb{N}^p / \ker\varphi$, where $\ker\varphi$ is the kernel congruence of φ:

$$\ker\varphi = \{(a, b) \in \mathbb{N}^p \times \mathbb{N}^p \mid \varphi(a) = \varphi(b)\}.$$

Notice that for groups, vector spaces, rings ... the kernel is defined by the elements mapping to the identity element. This is because there we have inverses and from $f(a) = f(b)$ we get $f(a - b) = 0$. This is not the case in numerical semigroups, and this is why the kernel is a congruence, and not a "subject" of the domain.

Given $\tau \subset \mathbb{N}^p \times \mathbb{N}^p$, the *congruence generated* by τ is the smallest congruence on $\mathbb{N}^p$ containing τ, that is, the intersection of all congruences containing τ. We denote by $\operatorname{cong}(\tau)$ the congruence generated by τ. Accordingly, we say that τ is a generating system of a congruence σ on $\mathbb{N}^p$ if $\operatorname{cong}(\tau) = \sigma$.

The congruence generated by a set is just the reflexive, symmetric, transitive closure (this would just make the closure an equivalence relation), to which we adjoin all pairs $(a+c, b+c)$ whenever (a, b) is in the closure; so that we make the resulting relation a congruence. This can be formally written as follows.

Proposition 105. *Let $\rho \subseteq \mathbb{N}^p \times \mathbb{N}^p$. Define*

$$\rho^0 = \rho \cup \{(b, a) \mid (a, b) \in \rho\} \cup \{(a, a) \mid a \in \mathbb{N}^p\},$$

$$\rho^1 = (v + u, w + u), (v, w) \in \rho^0, u \in \mathbb{N}^p.$$

Then $\operatorname{cong}(\rho)$ *is the set of pairs $(v, w) \in \mathbb{N}^p \times \mathbb{N}^p$ such that there exist $k \in \mathbb{N}$ and $v_0, \dots, v_k \in \mathbb{N}^p$ with $v_0 = v$, $v_k = w$ and $(v_i, v_{i+1}) \in \rho^1$ for all $i \in \{0, \dots, k-1\}$.*

Proof. We first show that the set constructed in this way is a congruence. Let us call this set σ.

(1) Since $(a, a) \in \rho^0 \subseteq \sigma$ for all $a \in \mathbb{N}^p$, the binary relation σ is reflexive.
(2) If $(v, w) \in \sigma$, there exist $k \in \mathbb{N}$ and $v_0, \dots, v_k \in \mathbb{N}^p$ such that $v_0 = v$, $v_k = w$ and $(v_i, v_{i+1}) \in \rho^1$ for all $i \in \{0, \dots, k-1\}$. Since $(v_i, v_{i+1}) \in \rho^1$ implies that $(v_{i+1}, v_i) \in \rho^1$, by defining $w_i = v_{k-i}$ for every $i \in \{0, \dots k\}$, we obtain that $(w, v) \in \sigma$. Hence σ is symmetric.
(3) If (u, v) and (v, w) are in σ, then there exists $k, l \in \mathbb{N}$ and $v_0, \dots, v_k, w_0, \dots, w_l \in \mathbb{N}^p$ such that $v_0 = u$, $v_k = w_0 = v$, $w_l = w$ and $(v_i, v_{i+1}), (w_j, w_{j+1}) \in \rho^1$ for all suitable i, j. By concatenating these we obtain $(u, w) \in \sigma$. Thus σ is transitive.
(4) Finally, let $(v, w) \in \sigma$ and $u \in \mathbb{N}^p$. There exists $k \in \mathbb{N}$ and $v_0, \dots, v_k \in \mathbb{N}^p$ such that $v_0 = v$, $v_k = w$ and $(v_i, v_{i+1}) \in \rho^1$ for all $i \in \{0, \dots, k-1\}$. By defining $w_i = v_i + u$ for all $i \in \{0, \dots, k\}$ we have $(w_i, w_{i+1}) \in \rho^1$ and consequently $(v + u, w + u) \in \sigma$.

It is clear that every congruence containing ρ must contain σ and this means that σ is the least congruence on $\mathbb{N}^p$ that contains ρ, whence, $\sigma = \operatorname{cong}(\rho)$. □

A *presentation* for S is a generating system of $\ker \varphi$ as a congruence, and a *minimal presentation* is a presentation such that none of its proper subsets is a presentation.

Example 106. For instance, a minimal presentation for $S = \langle 2, 3\rangle$ is $\{((3, 0), (0, 2))\}$. This means that S is the commutative monoid generated by two elements, say a and b, under the relation $3a = 2b$.

For $s \in S$, the *set of factorizations* of s in S is the set

$$\mathsf{Z}(s) = \varphi^{-1}(s) = \{a \in \mathbb{N}^p \mid \varphi(a) = s\}.$$

Notice that the set of factorizations of s has finitely many elements. This can be shown in different ways. For instance the ith coordinate of a factorization is smaller than or equal to

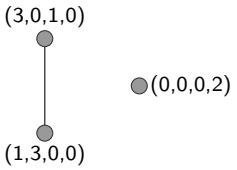
s/n_i. Also, two factorizations are incomparable with respect to the usual partial ordering on $\mathbb{N}^p$, and thus Dickson's lemma ensures that there are finitely many of them.

We define, associated to s, the graph ∇_s whose vertices are the elements of $\mathsf{Z}(s)$ and ab is an edge if $a \cdot b \neq 0$ (dot product).

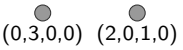
We say that two factorizations a and b of s are $\mathcal{R}$-related if they belong to the same connected component of ∇_s, that is, there exists a chain of factorizations $a_1, \ldots, a_t \in \mathsf{Z}(s)$ such that

- $a_1 = a$, $a_t = b$,
- for all $i \in \{1, \ldots, t-1\}$, $a_i \cdot a_{i-1} \neq 0$.

Example 107. Let $S = \langle 5, 7, 11, 13\rangle$. We draw ∇_{26}.



This graph has two connected components. Also, we have that $((3,0,1,0),(0,0,0,2)) \in \ker\varphi$, and as $((3,0,1,0),(1,3,0,0)) \in \ker\varphi$, we also have that removing the common part we obtain a new element in the kernel: $((2,0,1,0),(0,3,0,0))$. This new element corresponds to $21 = 2\times 5 + 11 = 3 \times 7$. If we draw ∇_{21}, we obtain



which is another nonconnected graph.

Let $\tau \subset \mathbb{N}^p \times \mathbb{N}^p$. We say that τ is *compatible* with $s \in S$ if either ∇_s is connected or if $R_1, \ldots, R_t$ are the connected components of ∇_s, then for every $i \in \{1, \ldots, t\}$ we can choose $a_i \in R_i$ such that for every $i, j \in \{1, \ldots, t\}$, $i \neq j$, there exists $i_1, \ldots, i_k \in \{1, \ldots, t\}$ fulfilling

- $i_1 = i$, $i_k = j$,
- for every $m \in \{1, \ldots, k-1\}$ either $(a_{i_m}, a_{i_{m+1}}) \in \tau$ or $(a_{i_{m+1}}, a_{i_m}) \in \tau$.

Even though this definition might seem strange, we are going to show next that we only have to look at those ∇_n that are nonconnected in order to construct a (minimal) presentation.

Denote by $\mathbf{e}_i$ the ith row of the $p \times p$ identity matrix.

Theorem 108. *Let S be a numerical semigroup minimally generated by $\{n_1, \ldots, n_p\}$, and let $\tau \subseteq \mathbb{N}^p \times \mathbb{N}^p$. Then τ is a presentation of S if and only if τ is compatible with s for all $s \in S$.*

Proof. Necessity. If ∇_s is connected, then there is nothing to prove.

Let $R_1, \ldots, R_t$ be the $\mathcal{R}$-classes contained in $\mathsf{Z}(s)$. Let i and j be in $\{1, \ldots, t\}$ with $i \neq j$. Let $a \in R_i$ and $b \in R_j$. As $a, b \in \mathsf{Z}(n)$, $(a,b) \in \ker\varphi$. Since $\operatorname{cong}(\tau) = \ker\varphi$, by Proposition 105, there exist $b_0, b_1, \ldots, b_r \in \mathbb{N}^p$, such that $a = b_0$, $b = b_r$ and $(b_i, b_{i+1}) \in \beta^1$ for $i \in \{0, \ldots, r-1\}$. Hence there exist for all $i \in \{0, \ldots, r-1\}$, $z_i \in \mathbb{N}^p$ and $(x_i, y_i) \in \tau$ such that either $(b_i, b_{i+1}) = (x_i + z_i, y_i + z_i)$ or $(b_i, b_{i+1}) = (y_i + z_i, x_i + z_i)$. If $z_i \neq 0$, then $b_i \mathcal{R} b_{i+1}$. And if $z_i = 0$, then $\{b_i, b_{i+1}\} \subseteq \mathsf{Z}(s)$. Hence the pairs $(b_i, b_{i+1}) \notin \mathcal{R}$ yield the a_i's we are looking for.

Sufficiency. It suffices to prove that for every $s \in S$ and $a, b \in \mathsf{Z}(s)$, $(a,b) \in \operatorname{cong}(\tau)$. We use induction on s. The result follows trivially for $s = 0$, since $\mathsf{Z}(0) = \{0\}$.

If $a\mathcal{R}b$, then there exists $a_1, \ldots, a_k \in \mathsf{Z}(s)$ such that $a_1 = a$, $a_k = b$ and $a_i \cdot a_{i+1} \neq 0$ for all $i \in \{1, \ldots, k-1\}$. Hence for every i, there exists $j \in \{1, \ldots, p\}$ such that $a_i - \mathbf{e}_j, a_{i+1} - \mathbf{e}_j \in \mathsf{Z}(s - n_j)$. By induction hypothesis $(a_i - \mathbf{e}_j, a_{i+1} - \mathbf{e}_j) \in \operatorname{cong}(\tau)$, whence $(a_i, a_{i+1}) \in \operatorname{cong}(\tau)$ for all i. By transitivity $(a, b) \in \tau$.

Assume now that a and b are in different connected components of ∇_s. If $R_1, \ldots, R_t$ are the connected components of ∇_s, we may assume without loss of generality that $a \in R_1$ and $b \in R_2$. As τ is compatible with s, there exists a chain $a_1, \ldots, a_k$ such that either $(a_i, a_{i+1}) \in \tau$ or $(a_{i+1}, a_i) \in \tau$, $a_1 \in R_1$ and $a_2 \in R_2$. Hence $(a_i, a_{i+1}) \in \operatorname{cong}(\tau)$, and by the above paragraph, $(a, a_1), (a_k, b) \in \operatorname{cong}(\tau)$. By transitivity we deduce that $(a, b) \in \operatorname{cong}(\tau)$. □

Observe that as a consequence of this theorem, in order to obtain a presentation for S we only need for every $s \in S$ with nonconnected graph ∇_s and every connected component R choose a factorization x and pairs (x, y) such that every two connected components of ∇_s are connected by a sequence of these factorizations with consecutive elements either a chosen pair or its symmetry. The least possible number of edges we need is when we choose the pairs so that we obtain a tree connecting all connected components. Thus the least possible number of pairs for every $s \in S$ with associated nonconnected graph is the number of connected components of ∇_s minus one.

Corollary 109. *Let S be a numerical semigroup. The cardinality of any minimal presentation of S equals $\sum_{s \in S}(\operatorname{nc}(\nabla_s) - 1)$, where $\operatorname{nc}(\nabla_s)$ is the number of connected components of ∇_s.*

We now show that this cardinality is finite by showing that only finitely many elements of S have nonconnected associated graphs.

Proposition 110. *Let S be a numerical semigroup minimally generated by $\{n_1, \ldots, n_p\}$, and let $s \in S$. If ∇_s is not connected, then $s = n_i + w$ with $i \in \{2, \ldots, p\}$ and $w \in \operatorname{Ap}(S, n_1)$.*

Proof. Observe that $\nabla_{n_i} = \{\mathbf{e}_i\}$. Hence $s \notin \{n_1, \ldots, n_p\}$, and thus there exists $i \in \{1, \ldots, p\}$ such that $s - n_i \in S^*$. If $s \in \operatorname{Ap}(S, n_1)$, then $s - n_i \in \operatorname{Ap}(S, n_1)$, and we are done.

Now assume that $s - n_1 \in S$. There exists an element $a \in \mathsf{Z}(s)$ with $a - \mathbf{e}_1 \in \mathbb{N}^p$. Take $b \in \mathsf{Z}(s)$ in a different connected component of ∇_s than the one containing a. Clearly $a \cdot b = 0$, and thus $b - \mathbf{e}_1 \notin \mathbb{N}^p$. Since $b \neq 0$, there exists $i \in \{2, \ldots, p\}$ such that $b - \mathbf{e}_i \in \mathbb{N}^p$, and consequently $s - n_i \in S$. We prove that $s - (n_i + n_1) \notin S$, and thus $s = (s - n_i) + n_i$ with $s - n_i \in \operatorname{Ap}(S, n_1)$. Suppose to the contrary that $s - (n_1 + n_i) \in S$. Hence there exists a factorization of c of s such that $c - (\mathbf{e}_1 + \mathbf{e}_i) \in \mathbb{N}^p$. Then $a \cdot c \neq 0$ and $c \cdot b \neq 0$. This force a and b to be in the same connected component of ∇_s, a contradiction. □

We say that $s \in S$ is a *Betti element* if ∇_s is not connected.

Example 111. We continue with the semigroup in Example 107.

```
gap> s:=NumericalSemigroup(5,7,11,13);;
```

We can use the following to compute a minimal presentation for this semigroup.

```
gap> MinimalPresentationOfNumericalSemigroup(s);
[ [ [ 0, 1, 1, 0 ], [ 1, 0, 0, 1 ] ], [ [ 0, 3, 0, 0 ], [ 2, 0, 1, 0 ] ],
  [ [ 1, 3, 0, 0 ], [ 0, 0, 0, 2 ] ], [ [ 2, 2, 0, 0 ], [ 0, 0, 1, 1 ] ],
  [ [ 3, 1, 0, 0 ], [ 0, 0, 2, 0 ] ], [ [ 4, 0, 0, 0 ], [ 0, 1, 0, 1 ] ] ]
```

Let us have a look at ∇_{50}.

```
gap> FactorizationsElementWRTNumericalSemigroup(50,s);
[ [ 10, 0, 0, 0 ], [ 3, 5, 0, 0 ], [ 5, 2, 1, 0 ], [ 0, 4, 2, 0 ],
  [ 2, 1, 3, 0 ], [ 6, 1, 0, 1 ], [ 1, 3, 1, 1 ], [ 3, 0, 2, 1 ],
  [ 2, 2, 0, 2 ], [ 0, 0, 1, 3 ] ]
gap> RClassesOfSetOfFactorizations(last);
[ [ [ 0, 0, 1, 3 ], [ 0, 4, 2, 0 ], [ 1, 3, 1, 1 ], [ 2, 1, 3, 0 ],
      [ 2, 2, 0, 2 ], [ 3, 0, 2, 1 ], [ 3, 5, 0, 0 ], [ 5, 2, 1, 0 ],
      [ 6, 1, 0, 1 ], [ 10, 0, 0, 0 ] ] ]
gap> Length(last);
1
```

And this means that ∇_{50} has a single connected component, and thus is not a Betti element.

We can compute the set of Betti elements.

```
gap> BettiElementsOfNumericalSemigroup(s);
[ 18, 20, 21, 22, 24, 26 ]
```

So for instance ∇_{26} has two connected components as we already saw in Example 107.

```
gap> FactorizationsElementWRTNumericalSemigroup(26,s);
[ [ 1, 3, 0, 0 ], [ 3, 0, 1, 0 ], [ 0, 0, 0, 2 ] ]
gap> RClassesOfSetOfFactorizations(last);
[ [ [ 1, 3, 0, 0 ], [ 3, 0, 1, 0 ] ], [ [ 0, 0, 0, 2 ] ] ]
```

We now show an alternative method to compute a presentation based on what is known in the literature as Herzog's correspondence ([15]).

Let S be a numerical semigroup minimally generated by $\{n_1, \ldots, n_p\}$. For $\mathbb{K}$ a field, the *semigroup ring* associated to S is the ring $\mathbb{K}[S] = \bigoplus_{s\in S} \mathbb{K}t^s$, where t is a symbol or an indeterminate. Addition in $\mathbb{K}[S]$ is performed componentwise, while multiplication is done by using distributivity and the rule $t^s t^{s'} = t^{s+s'}$, for $s, s' \in S$. We can see the elements in $\mathbb{K}[S]$ as polynomials in t whose nonnegative coefficients correspond to exponents in S. Also $\mathbb{K}[S] = \mathbb{K}[t^{n_1}, \ldots, t^{n_p}] \subseteq \mathbb{K}[t]$. Thus, $\mathbb{K}[S]$ can be seen as the coordinate ring of a curve parametrized by monomials.

Let $x_1, \ldots, x_p$ be indeterminates, and $\mathbb{K}[x_1, \ldots, x_p]$ be the polynomial ring over these indeterminates with coefficients in the field $\mathbb{K}$. For $a = (a_1, \ldots a_p) \in \mathbb{N}^p$ write

$$X^a = x_1^{a_1} \cdots x_p^{a_p}.$$

Let ψ the ring homomorphism determined by

$$\psi : \mathbb{K}[x_1, \ldots, x_p] \to \mathbb{K}[S], \quad x_i \mapsto t^{n_i}.$$

This can be seen as a graded morphism if we grade $\mathbb{K}[x_1, \ldots, x_p]$ in the following way: a polynomial p is S-homogeneous of degree $s \in S$ if $p = \sum_{a\in A} c_a X^a$ for some $A \subset \mathbb{N}^p$ with finitely many elements and $\varphi(a) = s$ for all $a \in A$. Observe that $\mathbb{K}[S]$ is also S-graded in a natural way, and so ψ is a graded epimorphism.

For $A \subseteq \mathbb{K}[x_1, \ldots, x_p]$, denote by (A) the ideal generated by A.

Proposition 112. $\ker \psi = (X^a - X^b \mid (a, b) \in \ker \varphi)$.

Proof. Clearly $\psi(X^a) = t^{\varphi(a)}$. Hence for $(a,b) \in \ker\varphi$, $\psi(X^a - X^b) = 0$. This implies that $(X^a - X^b \mid (a,b) \in \ker\varphi) \subseteq \ker\psi$. Since ψ is a graded morphism, for the other inclusion, it suffices to proof that if $f \in \ker\psi$ is S-homogeneous of degree $s \in S$, then $f \in (X^a - X^b \mid (a,b) \in \ker\varphi)$. Write $f = \sum_{a\in A} c_a X^a$, with $c_a \in \mathbb{K}$ and $a \in \mathsf{Z}(s)$ for all $a \in A$, and A a finite set. Then $\varphi(f) = t^s \sum_{a\in A} c_a = 0$, and consequently $\sum_{a\in A} c_a = 0$. Choose $a \in A$. Then $f = \sum_{a'\in A\setminus\{a\}} c_a(X^{a'} - X^a)$, and thus $f \in (X^a - X^b \mid (a,b) \in \ker\varphi)$. □

From Proposition 105, it can be easily derived that for any $\tau \in \mathbb{N}^p \times \mathbb{N}^p$

$$(X^a - X^b \mid (a,b) \in \tau) = (X^a - X^b \mid (a,b) \in \operatorname{cong}(\tau)).$$

Hence, we get the following consequence.

Corollary 113. *Let S be a numerical semigroup and τ a presentation of S. Then*

$$\ker\psi = (X^a - X^b \mid (a,b) \in \tau).$$

Observe that the generators of $\ker\psi$ can be seen as the implicit equations of the curve whose coordinate ring is $\mathbb{K}[S]$. In this way we can solve the implicitation problem without the use of elimination theory nor Gröbner bases.

Example 114. Let $S = \langle 3,5,7\rangle$. Then $\operatorname{Ap}(S,3) = \{0,5,7\}$. According to Proposition 110, $\operatorname{Betti}(S) \subseteq \{10,12,14\}$. The sets of factorizations of 10, 12 and 14 are $\{(0,2,0),(1,0,1)\}$, $\{(4,0,0),(0,1,1)\}$ and $\{(3,1,0),(0,0,2)\}$, respectively. Hence $\operatorname{Betti}(S) = \{10,12,14\}$, and by Theorem 108,

$$\{((0,2,0),(1,0,1)),((3,1,0),(0,0,2)),((4,0,0),(0,1,1))\}$$

is a minimal presentation of S. The implicit equations of the curve parametrized by (t^3,t^5,t^7) are

$$\begin{cases} xz - y^2 & = 0, \\ x^3y - z^2 & = 0, \\ x^4 - yz & = 0. \end{cases}$$

Let us reproduce this example with the use of polynomials. Take $\psi : K[x,y,z] \to K[t]$ be determined by $x \mapsto t^3$, $y \mapsto t^5$ and $z \mapsto t^7$. We consider now the ideal $(x - t^3, y - t^5, z - t^7)$. We now compute a Gröbner basis with respect to any eliminating order on t. We can for instance do this with `Singular`, [9].

```
> ring r=0,(t,x,y,z),lp;
> ideal i=(x-t^3,y-t^5,z-t^4);
> std(i);
_[1]=y4-z5
_[2]=xz3-y3
_[3]=xy-z2
_[4]=x2z-y2
_[5]=x3-yz
_[6]=tz-y
_[7]=ty-x2
_[8]=tx-z
_[9]=t3-x
```

Now we choose those not having t, or we can just type:

```
> eliminate(i,t);
_[1]=y7-z5
_[2]=xz-y2
_[3]=xy5-z4
_[4]=x2y3-z3
_[5]=x3y-z2
_[6]=x4-yz
```

Which by Herzog's correspondence yields a presentation for S. However this is not a minimal presentation. In order to get a minimal presentation we can use `minbase` in `Singular`, but this applies only to homogeneous ideals. To solve this issue, we give weights 3,5,7 to x, y, z, respectively.

```
> ring r=0,(t,x,y,z),(dp(1),wp(3,5,7));
> ideal i=(x-t^3,y-t^5,z-t^7);
> ideal j=eliminate(i,t);
> minbase(j);
_[1]=y2-xz
_[2]=x4-yz
_[3]=x3y-z2
```

5. Factorizations

Let S be a numerical semigroup minimally generated by $\{n_1, \ldots, n_p\}$. For $s \in S$, recall that the set of factorizations of s is $\mathsf{Z}(s) = \varphi^{-1}(s)$.

For a factorization $x = (x_1, \ldots, x_p)$ of s its *length* is defined as

$$|x| = x_1 + \cdots + x_p,$$

and the *set of lengths* of s is

$$\mathsf{L}(s) = \{|x| \mid x \in \mathsf{Z}(s)\}.$$

Since $\mathsf{Z}(s)$ has finitely many elements, so has $\mathsf{L}(s)$. A monoid is *half factorial* if the cardinality of $\mathsf{L}(s)$ is one for all $s \in S$.

Example 115. Let $S = \langle 2, 3\rangle$. Here 6 factors as $6 = 2{\times}3 = 3{\times}2$, that is, $\mathsf{Z}(6) = \{(3,0),(0,2)\}$. The length of $(3,0)$ is 3, while that of $(0,2)$ is 2. So S is not a unique factorization monoid, and it is not either a half factorial monoid. The only half factorial numerical semigroup is $\mathbb{N}$.

5.1. **Length based invariants.** One of the first nonunique factorization invariants that appeared in the literature was the elasticity. It was meant to measure how far is a monoid from being half factorial. The elasticity of a numerical semigroup is a rational number greater than one. Actually, half factorial monoids are those having elasticity one.

Let $s \in S$. The *elasticity* of s, denoted by $\rho(s)$ is defined as

$$\rho(s) = \frac{\max \mathsf{L}(s)}{\min \mathsf{L}(s)}.$$

The elasticity of S is defined as

$$\rho(S) = \sup_{s \in S} \rho(s).$$

The computation of the elasticity in finitely generated cancellative monoids requires the calculation of primitive elements of $\ker \varphi$. However in numerical semigroups, this calculation is quite simple, as the following example shows.

Theorem 116. *Let S be a numerical semigroup minimally generated by $\{n_1, \ldots, n_p\}$ with $n_1 < \cdots < n_p$. Then*

$$\rho(S) = \frac{n_p}{n_1}.$$

Proof. Let $s \in S$ and assume that $a = (a_1, \ldots, a_p)$ and $b = (b_1, \ldots, b_p)$ are such that $|a| = \max \mathsf{L}(S)$ and $|b| = \min \mathsf{L}(S)$. We know that $\varphi(a) = \varphi(b)$, that is, $a_1 n_1 + \cdots + a_p n_p = b_1 n_1 + \cdots + b_p n_p = s$. Now by using that $n_1 < \cdots < n_p$, we deduce that

$$n_1|a| \leq s \leq n_p|b|,$$

and thus

$$\rho(s) = \frac{|a|}{|b|} \leq \frac{n_p}{n_1}.$$

This implies that $\rho(S) \leq \frac{n_p}{n_1}$. Also $\rho(n_1 n_p) \geq \frac{n_p}{n_1}$, since $n_p \mathbf{e}_1, n_1 \mathbf{e}_p \in \mathsf{Z}(n_1 n_p)$. Hence

$$\frac{n_p}{n_1} \leq \rho(n_1 n_p) \leq \rho(S) \leq \frac{n_p}{n_1},$$

and we get an equality. □

Another way to measure how far we are from half factoriality, is to measure how distant are the different lengths of factorizations. This is the motivation for the following definition.

Assume that $\mathsf{L}(s) = \{l_1 < \cdots < l_k\}$. Define the *Delta set* of s as

$$\Delta(s) = \{l_2 - l_1, \ldots, l_k - l_{k-1}\},$$

and if $k = 1$, $\Delta(s) = \emptyset$. The Delta set of S is defined as

$$\Delta(S) = \bigcup_{s \in S} \Delta(s).$$

So, the bigger $\Delta(S)$ is, the farther is S from begin half factorial.

A pair of elements $(a, b) \in \mathbb{N}^p \times \mathbb{N}^p$ is in $\ker \varphi$ if a and b are factorizations of the same element in S. As a presentation is a system of generators of $\ker \varphi$ it seems natural that the information on the factorizations could be recovered from it. We start showing that this is the case with the Delta sets, and will see later that the same holds for other invariants.

Let $M_S = \{a - b \mid (a, b) \in \ker \varphi\} \subseteq \mathbb{Z}^p$. Since $\ker \varphi$ is a congruence, it easily follows that M_S is a subgroup of $\mathbb{Z}^p$.

Lemma 117. *Let σ be a presentation of S. Then M_S is generated as a group by $\{a - b \mid (a, b) \in \sigma\}$.*

Proof. Let $z \in M_S$. Then there exists $(a, b) \in \ker \varphi$. From Proposition 105, there exists $x_1, \ldots, x_t$ such that $x_1 = a$, $x_t = b$, and for all $i \in \{1, \ldots, t-1\}$ there exists (a_i, b_i) and $c_i \in \mathbb{N}^p$ such that $(x_i, x_{i+1}) = (a_i + c_i, b_i + c_i)$ with either $(a_i, b_i) \in \sigma$ or $(b_i, a_i) \in \sigma$. Then

$$a - b = (x_1 - x_2) + (x_2 - x_3) + \cdots + (x_{t-1} - x_t) = \sum_{i=1}^{t-1} (a_i - b_i),$$

and the proof follows easily. □

For a given $z = (z_1, \ldots, z_p) \in \mathbb{Z}^p$, we also use the notation $|z| = z_1 + \cdots + z_p$.

Lemma 118. *Let $\sigma = \{(a_1, b_1), \dots, (a_t, b_t)\}$ be a presentation of S, and set $\delta_i = |a_i - b_i|$, $i \in \{1, \dots, s\}$. Then every element in $\Delta(S)$ is of the form*

$$\lambda_1\delta_1 + \cdots + \lambda_t\delta_t,$$

for some integers $\lambda_1, \dots, \lambda_t$.

Proof. The proof follows easily from the proof of Lemma 117. □

Theorem 119. *Let S be a numerical semigroup and let σ be a presentation of S. Then*

$$\min \Delta(S) = \gcd\{|a - b| \mid (a, b) \in \sigma\}.$$

Proof. In order to simplify notation, write $d = \gcd\{|a - b| \mid (a, b) \in \sigma\}$. If $\delta \in \Delta(S)$, then by Lemma 118, we know that δ is a linear combination with integer coefficients of elements of the form $|a - b|$ with $(a, b) \in \sigma$. Hence $d \mid \delta$, and consequently $d \leq \min \Delta(S)$. Now let $(a_1, b_1), \dots, (a_k, b_k) \in \sigma$ and $\lambda_1, \dots, \lambda_k \in \mathbb{Z}$ be such that $\lambda_1|a_1 - b_1| + \cdots + \lambda_k|a_k - b_k| = d$. If $\lambda_i < 0$, change (a_i, b_i) with $(b_i - a_i)$, so that we can assume that all λ_i are nonnegative. The element $s = \varphi(\lambda_1 a_1 + \cdots + \lambda_k a_k) = \varphi(\lambda_1 b_1 + \cdots + \lambda_k b_k)$ has two factorizations $z = \lambda_1 a_1 + \cdots + \lambda_k a_k$ and $z' = \lambda_1 b_1 + \cdots + \lambda_k b_k$ such that the differences in their lengths is d. Hence

$$\min \Delta(S) \leq \min \Delta(s) \leq d \leq \min \Delta(S),$$

and we get an equality. □

Theorem 120. *Let S be a numerical semigroup. Then*

$$\max \Delta(S) = \max\{\max \Delta(b) \mid b \in \mathrm{Betti}(S)\}.$$

Proof. The inequality $\max_{n \in \mathrm{Betti}(S)} \max \Delta(n) \leq \max \Delta(S)$ is clear.

Assume to the contrary $\max \Delta(S) > \max \Delta(b)$ for all Betti elements b of S. Take x, y factorizations of an element $s \in S$ so that $|y| - |x| = \max \Delta(S)$, and consequently no other factorization z of s fulfills $|x| < |z| < |y|$. As $\varphi(x) = \varphi(y)$, Proposition 105, ensures the existence of $x_1, \dots, x_t$ in $\mathsf{Z}(s)$ such that $x = x_1$, $x_t = y$ and $(x_i, x_{i+1}) = (a_i + c_i, b_i + c_i)$, with either $(a_i, b_i) \in \sigma$ or $(b_i, a_i) \in \sigma$ for all $i \in \{1, \dots, t - 1\}$. From the above discussion, there exists $i \in \{1, \dots, t - 1\}$, with $|x_i| \leq |x| < |y| \leq |x_{i+1}|$. Both a_i and b_i are factorizations of an element n with $\mathsf{Z}(n)$ having more than one $\mathcal{R}$-class. So there is a chain of factorizations, say $z_1, \dots, z_u$, of n such that $a_i = z_1, \dots, z_u = b_i$, and $|z_{j+1}| - |z_j| \leq \max \Delta(n)$, which we are assuming smaller than $\Delta(S)$. But then $\varphi(z_j + c_i) = \varphi(x) = \varphi(y)$ for all j, and from the choice of x and y, there is no j such that $|x| < |z_j + c_i| < |y|$. Again, we can find $j \in \{1, \dots, u-1\}$ such that $|z_j + c_i| \leq |x| < |y| \leq |z_{j+1} + c_i|$. And this leads to a contradiction, since $\max \Delta(S) = |y| - |x| \leq |z_{j+1} + c_i| - |z_j + c_i| = |z_{i+1} - z_i| \leq \max \Delta(n) < \max \Delta(S)$. □

Example 121. Let us go back to $S = \langle 2, 3\rangle$. We know that the only Betti element of S is 6. The set of factorizations of 6 is $\mathsf{Z}(6) = \{(3, 0), (0, 2)\}$, and $\mathsf{L}(S) = \{2, 3\}$. Whence $\Delta(6) = \{1\}$. The above theorem implies that $\Delta(S) = \{1\}$. This is actually the closest we can be in a numerical semigroup to be half factorial.

Example 122. Now we do some computations with a numerical semigroup with four generators.

```
gap> s:=NumericalSemigroup(10,11,17,23);;
gap> FactorizationsElementWRTNumericalSemigroup(60,s);
[ [ 6, 0, 0, 0 ], [ 1, 3, 1, 0 ], [ 2, 0, 1, 1 ] ]
```

```
gap> LengthsOfFactorizationsElementWRTNumericalSemigroup(60,s);
[ 4, 5, 6 ]
gap> ElasticityOfFactorizationsElementWRTNumericalSemigroup(60,s);
3/2
gap> DeltaSetOfFactorizationsElementWRTNumericalSemigroup(60,s);
[ 1 ]
gap> BettiElementsOfNumericalSemigroup(s);
[ 33, 34, 40, 69 ]
gap> Set(last, x->DeltaSetOfFactorizationsElementWRTNumericalSemigroup(x,s));
[ [  ], [ 1 ], [ 2 ], [ 3 ] ]
gap> ElasticityOfNumericalSemigroup(s);
23/10
```

5.2. **Distance based invariants.** We now introduce some invariants that depend on distances between factorizations. These invariants will measure how spread are the factorizations of elements in the monoid.

The set $\mathbb{N}^p$ is a lattice with respect to the partial ordering $\leq$. Infimum and supremum of a set with two elements is constructed by taking minimum and maximum coordinate by coordinate, respectively. For $x = (x_1, \ldots, x_p), y = (y_1, \ldots, y_p) \in \mathbb{N}^p$, $\inf\{x, y\}$ will be denoted by $x \wedge y$. Thus

$$x \wedge y = (\min\{x_1, y_1\}, \ldots, \min\{x_p, y_p\}).$$

The *distance* between x and y is defined as

$$\mathrm{d}(x, y) = \max\{|x - (x \wedge y)|, |y - (x \wedge y)|\}$$

(equivalently $\mathrm{d}(x, y) = \max\{|x|, |y|\} - |x \wedge y|$).

The distance between two factorizations of the same element is lower bounded in the following way.

Lemma 123. *Let $x, y \in \mathbb{N}^p$ with $x \neq y$ and $\varphi(x) = \varphi(y)$. Then*

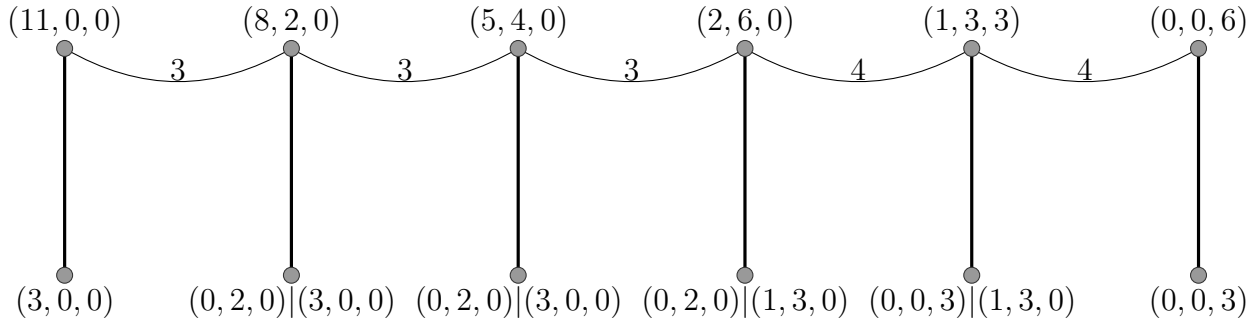
$$2 + \big||x| - |y|\big| \leq \mathrm{d}(x, y).$$

Proof. We can assume that $x \wedge y = 0$, since distance is preserved under translations, $||x| - |y|| = ||x - (x \wedge y)| - |y - (x \wedge y)||$ and $\varphi(x - (x \wedge y)) = \varphi(y - (x \wedge y))$. As $\varphi(x) = \varphi(y)$ and $x \neq y$, in particular we have that $|x| \geq 2$ and the same for $|y|$. Also, as $x \wedge y = 0$, $\mathrm{d}(x, y) = \max\{|x|, |y|\}$. If $|x| \geq |y|$, then $2 + ||x| - |y|| = |x|(2 - |y|) \leq |x| = \mathrm{d}(x, y)$. A similar argument applies for $|x| \leq |y|$. □

Example 124. The factorizations of $66 \in \langle 6, 9, 11\rangle$ are

$$\mathsf{Z}(66) = \{(0, 0, 6), (1, 3, 3), (2, 6, 0), (4, 1, 3), (5, 4, 0), (8, 2, 0), (11, 0, 0)\}.$$

The distance between $(11, 0, 0)$ and $(0, 0, 6)$ is 11. However we can put other factorizations of 66 between them so that the maximum distance of two consecutive links is at most 4:



In the above picture the factorizations are depicted in the top of a post, and they are linked by a "catenary" labeled with the distance between two consecutive sticks. On the bottom we have drawn the factorizations removing the common part with the one on the left and that of the right, respectively. We will say that the catenary degree of 66 in $\langle 6, 9, 11\rangle$ is at most 4.

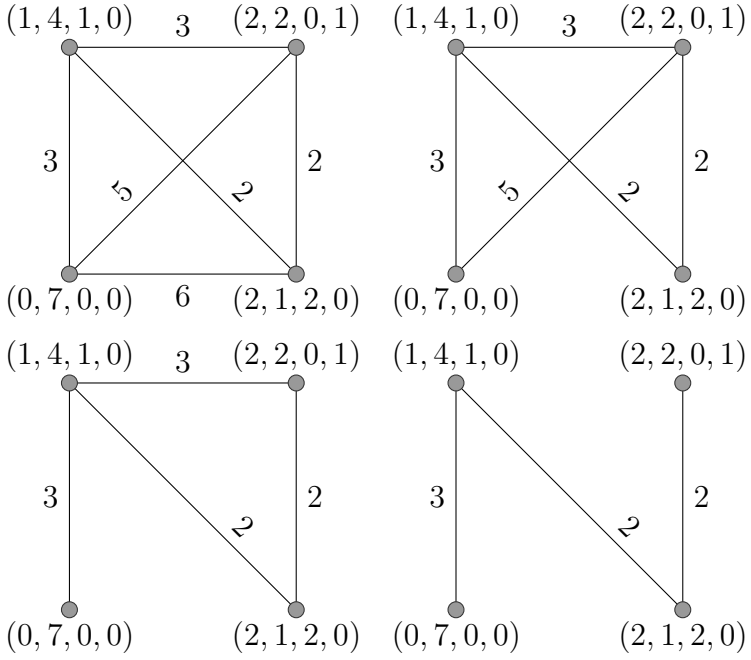
Given $s \in S$, $x, y \in \mathsf{Z}(s)$ and a nonnegative integer N, an *N-chain* joining x and y is a sequence $x_1, \dots, x_k \in \mathsf{Z}(s)$ such that

- $x_1 = x$, $x_k = y$,
- for all $i \in \{1, \dots, k-1\}$, $\mathrm{d}(x_i, x_{i+1}) \le N$.

The *catenary degree* of s, denoted $\mathsf{c}(s)$, is the least N such that for any two factorizations $x, y \in \mathsf{Z}(s)$, there is an N-chain joining them. The catenary degree of S, $\mathsf{c}(S)$, is defined as

$$\mathsf{c}(S) = \sup_{s \in S} \mathsf{c}(S).$$

Example 125. Let us compute the catenary degree of $77 \in S = \langle 10, 11, 23, 35\rangle$. We start with a complete graph with vertices the factorizations of 77 and edges labeled with the distances between them. Then we remove one edge with maximum distance, and we repeat the process until we find a bridge. The label of that bridge is then the catenary degree of 77.



Thus the catenary degree of 77 is 3.

If one looks at Proposition 105 and Example 124, one sees some interconnection between the transitivity and the way we can move from one factorization to another to minimize distances. This idea is exploited in the following result.

Theorem 126. *Let S be a numerical semigroup. Then*

$$\mathsf{c}(S) = \max\{\mathsf{c}(b) \mid b \in \mathrm{Betti}(S)\}.$$

Proof. Set $c = \max_{b\in \mathrm{Betti}(S)} \mathsf{c}(b)$. Clearly $c \leq \mathsf{c}(S)$. Let us prove the other inequality. Take $s \in S$ and $x, y \in \mathsf{Z}(s)$. Let σ be a minimal presentation of S. Then by Proposition 105, there exists a sequence $x_1, \dots, x_k$ such that $x_1 = x$, $x_k = y$, and for every i there exists $c_i \in \mathbb{N}^p$ (with p the embedding dimension of S) such that $(x_i, x_{i+1}) = (a_i + c_i, b_i + c_i)$ for some (a_i, b_i) such that either $(a_i, b_i) \in \sigma$ or $(b_i, a_i) \in \sigma$. According to Theorem 108, a_i, b_i are factorizations of a Betti element of S. By using the definition of catenary degree, there is a c-chain joining a_i and b_i (also b_i and a_i). If we add c_i to all the elements of this sequence, we have a c-chain joining x_i and x_{i+1} (distance is preserved under translations). By concatenating all these c-chains for $i \in \{1, \dots, k-1\}$ we obtain a c-chain joining x and y. And this proves that $\mathsf{c}(S) \leq c$, and the equality follows. □

Example 127. With the package `numericalsgps` the catenary degree of an element and of the whole semigroup can be obtained as follows.

```
gap> s:=NumericalSemigroup(10,11,17,23);;
gap> FactorizationsElementWRTNumericalSemigroup(60,s);
[ [ 6, 0, 0, 0 ], [ 1, 3, 1, 0 ], [ 2, 0, 1, 1 ] ]
gap> CatenaryDegreeOfElementInNumericalSemigroup(60,s);
4
gap> CatenaryDegreeOfNumericalSemigroup(s);
6
```

5.3. **How far is an irreducible from being prime.** As the title suggests, the last invariant we are going to present measures how far is an irreducible from being prime. Recall that a prime element is an element such that if it divides a product, then it divides one of the factors. Numerical semigroups are monoids under addition, and thus the concept of divisibility must be defined accordingly.

Given $s, s' \in S$, recall that we write $s \leq_S s'$ if $s' - s \in S$. We will say that s *divides* s'. Observe that s divides s' if and only if s' belongs to the ideal $s + S = \{s + x \mid x \in S\}$ of S. If $s \leq_S s'$, then t^s divides $t^{s'}$ in the semigroup ring $K[S]$, in the "multiplicative" sense.

The *ω-primality* of s in S, denoted $\omega(S, s)$, is the least positive integer N such that whenever s divides $a_1 + \cdots + a_n$ for some $a_1, \dots, a_n \in S$, then s divides $a_{i_1} + \cdots + a_{i_N}$ for some $\{i_1, \dots, i_N\} \subseteq \{1, \dots, n\}$.

Observe that an irreducible element in S (minimal generator) is prime if its ω-primality is 1. It is easy to observe that a numerical semigroup has no primes.

In the above definition, we can restrict the search to sums of the form $a_1 + \cdots + a_n$, with $a_1, \dots, a_n$ minimal generators of S as the following lemma shows.

Lemma 128. *Let S be numerical semigroup and $s \in S$. Then $\omega(S, s)$ is the smallest $N \in \mathbb{N} \cup \{\infty\}$ with the following property:*

For all $n \in \mathbb{N}$ and $a_1, \ldots, a_n$ minimal generators of S, if b divides $a_1 + \cdots + a_n$, then there exists a subset $\Omega \subset [1, n]$ with cardinality less than or equal to N such that

$$b \leq_S \sum_{i \in \Omega} a_i.$$

Proof. Let $\omega'(S, s)$ denote the smallest integer $N \in \mathbb{N}_0 \cup \{\infty\}$ satisfying the property mentioned in the lemma. We show that $\omega(S, s) = \omega'(S, s)$. By definition, we have $\omega'(S, s) \leq \omega(S, s)$.

In order to show that $\omega(S, s) \leq \omega'(S, s)$, let $n \in \mathbb{N}$ and $a_1, \ldots, a_n \in S$ with $s \leq_S a_1 + \cdots + a_n$. For every $i \in [1, n]$ we pick a factorization $a_i = u_{i,1} + \cdots + u_{i,k_i}$ with $k_i \in \mathbb{N}$ and $u_{i_1}, \ldots, u_{i,k_i}$ minimal generators of S. Then there is a subset $I \in [1, n]$ and, for every $i \in I$, a subset $\emptyset \neq \Lambda_i \subset [1, k_i]$ such that

$$\#I \leq \sum_{i \in I} \#\Lambda_i \leq \omega'(S, s) \quad \text{and} \quad s \leq_S \sum_{i \in I} \sum_{\nu \in \Lambda_i} u_{i,\nu},$$

and hence $s \leq_S \sum_{i \in I} a_i$. □

In order to compute the ω-primality of an element s in a numerical semigroup S, one has to look at the minimal factorizations (with respect to the usual partial ordering) of the elements in the ideal $s + S$; this is proved in the next result.

Proposition 129. *Let S be a numerical semigroup minimally generated by $\{n_1, \ldots, n_p\}$. Let $s \in S$. Then*

$$\omega(S, s) = \max \{|m| \mid m \in \text{Minimals}_{\leq}(\mathsf{Z}(s + S))\}.$$

Proof. Notice that by Dickson's lemma, the set $\text{Minimals}_{\leq}(\mathsf{Z}(s + S))$ has finitely many elements, and thus $N = \max \{|m| \mid m \in \text{Minimals}_{\leq}(\mathsf{Z}(s + S))\}$ is a nonnegative integer.

Choose $x = (x_1, \ldots, x_p) \in \text{Minimals}_{\leq}(\mathsf{Z}(s + S))$ such that $|x| = N$. Since $x \in \mathsf{Z}(s + S)$, s divides $s' = x_1 n_1 + \cdots + x_p n_p$. Assume that s divides $s'' = y_1 n_1 + \cdots + y_p n_p$ with $(y_1, \ldots, y_p) < (x_1, \ldots, x_p)$ (that is, s divides a proper subset of summands of s') . Then $s'' \in s + S$, and $(y_1, \ldots, y_p) \in \mathsf{Z}(s + S)$, contradicting the minimality of x. This proves that $\omega(S, s) \geq N$.

Now assume that s divides $x_1 n_1 + \cdots + x_p n_p$ for some $x = (x_1, \ldots, x_p) \in \mathbb{N}^p$. Then $x \in \mathsf{Z}(s + S)$, and thus there exists $m = (m_1, \ldots, m_p) \in \text{Minimals}_{\leq}(\mathsf{Z}(s + S))$ with $m \leq x$. By definition, $m_1 n_1 + \cdots + m_p n_p \in s + S$, and $|m| \leq N$. This proves in view of Lemma 128 that $N \leq \omega(S, s)$. □

For S a numerical semigroup minimally generated by $\{n_1, \ldots, n_p\}$, the ω-primality of S is defines as

$$\omega(S) = \max\{\omega(S, n_i) \mid i \in \{1, \ldots, p\}\}.$$

We are going to relate Delta sets with catenary degree and ω-primality. To this end we need the following technical lemma.

For $b = (b_1, \ldots, b_p) \in \mathbb{N}^p$, define $\text{Supp}(b) = \{i \in \{1, \ldots, p\} \mid b_i \neq 0\}$.

Lemma 130. *Let S be a numerical semigroups minimally generated by $\{n_1, \ldots, n_p\}$, and let $n \in \text{Betti}(S)$. Let $a, b \in \mathsf{Z}(n)$ in different $\mathcal{R}$-classes. For every $i \in \text{Supp}(b)$ it follows that $a \in \text{Minimals}_{\leq}\mathsf{Z}(n_i + S)$.*

Proof. Assume to the contrary that there exists $c \in \mathsf{Z}(n_i + S)$ and $x \in \mathbb{N}^k \setminus \{0\}$ such that $c + x = a$. From $c < a$, $a \cdot b = 0$ and $i \in \mathrm{Supp}(b)$, we deduce that $i \notin \mathrm{Supp}(c)$. As $c \in \mathsf{Z}(n_i + S)$, there exists $d \in \mathsf{Z}(n_i + S)$ with $i \in \mathrm{Supp}(d)$ and $\varphi(c) = \varphi(d)$. Hence $\varphi(d + x) = \varphi(c + x) = \varphi(a)$. Moreover $(d + x) \cdot (c + x) = (d + x) \cdot a \neq 0$, and $(d + x) \cdot b \neq 0$, which leads to $a\mathcal{R}b$, a contradiction. □

Theorem 131. *Let S be a numerical semigroup. Then*

$$\max \Delta(S) + 2 \leq \mathsf{c}(S) \leq \omega(S).$$

Proof. Assume that $d \in \Delta(S)$. Then there exists $s \in S$ and $x, y \in \mathsf{Z}(s)$ such that $|x| < |y|$, $d = |y| - |x|$ and there is no $z \in \mathsf{Z}(s)$ with $|x| < |z| < |y|$. From the definition of $\mathsf{c}(S)$, there is a $\mathsf{c}(S)$-chain $z_1, \ldots, z_k$ joining x and y. As in the proof of Theorem 120, we deduce that there exists i such that $|z_i| < |x| < |y| < |z_{i+1}|$. Then $2 + d = 2 + |y| - |x| \leq 2 + |z_{i+2}| - |z_i|$, and by Lemma 123, $2 + |z_{i+2}| - |z_i| \leq \mathrm{d}(z_i, z_{i+1})$. The definition of $\mathsf{c}(S)$-chain implies that $\mathrm{d}(z_i, z_{i+1}) \leq \mathsf{c}(S)$. Hence $2 + d \leq \mathsf{c}(S)$, and consequently $\max \Delta(S) + 2 \leq \mathsf{c}(S)$.

Let σ be a minimal presentation of $\ker \varphi$. For every $(a, b) \in \sigma$, there exists n_i and n_j minimal generators such that $a \in \mathrm{Minimals}_{\leq} \mathsf{Z}(n_i + S)$ and $b \in \mathrm{Minimals}_{\leq} \mathsf{Z}(n_j + S)$ (Lemma 130). From the definition of $\omega(S)$, both $|a|$ and $|b|$ are smaller than or equal to $\omega(S)$. Set $c = \max\{\max\{|a|, |b|\} \mid (a, b) \in \sigma\}$. Then $c \leq \omega(S)$. Now we prove that $\mathsf{c}(S) \leq c$. Let $s \in S$ and $x, y \in \mathsf{Z}(s)$. Then $\varphi(x) = \varphi(y)$ and as σ is a presentation, by Proposition 105, there exists a sequence $x_1, \ldots, x_k \in \mathbb{N}^p$ ($p = \mathrm{e}(S)$) such that $x_1 = x$, $x_k = y$ and for every i there exists $a_i, b_i, c_i \in \mathbb{N}^p$ such that $(x_i, x_{i+1}) = (a_i + c_i, b_i + c_i)$, with either $(a_i, b_i) \in \sigma$ or $(b_i, a_i) \in \sigma$. Notice that $\mathrm{d}(x_i, x_{i+1}) = \mathrm{d}(a_i, b_i) = \max\{|a_i|, |b_i|\}$ (a_i and b_i are in different $\mathcal{R}$-classes and thus $a_i \cdot b_i = 0$, or equivalently, $a_i \wedge b_i = 0$). Hence $\mathrm{d}(x_i, x_{i+1}) \leq c$, and consequently $x_1, \ldots, x_k$ is a c-chain joining x and y. This implies that $\mathsf{c}(S) \leq c$, and we are done. □

Example 132. Let us go back to $S = \langle 10, 11, 17, 23 \rangle$. From Example 122 and Theorem 120, we know that $\max \Delta(S) = 3$.

```
gap> OmegaPrimalityOfNumericalSemigroup(s);
6
```

From Theorem 131, we deduce that $\mathsf{c}(S) \in \{5, 6\}$. Recall that by Example 127, we know that $\mathsf{c}(S) = 6$.

The are many other nonunique factorization invariants that can be defined on any numerical semigroup. It was our intention just to show some of them and the last theorem that relates these invariants coming from lengths, distances and primality (respectively), and at the same time show how minimal presentations can be used to study them. The reader interested in this topic is referred to [14].

References

[1] S.S. Abhyankar.- Lectures on expansion techniques in Algebraic Geometry, Tata Institue of Fundamental research, Bombay, 1977.

[2] S.S. Abhyankar.- On the semigroup of a meromorphic curve, Part 1, in Proceedings of International Symposium on Algebraic Geometry, Kyoto, pp. 240-414, 1977.

[3] S.S. Abhyankar.- Irreducibility criterion for germs of analytic functions of two complex variables, Advances in Mathematics 74, pp. 190-257, 1989.

[4] S.S. Abhyankar and T.T. Moh.- Newton Puiseux expansion and generalized Tschirnhausen transformation, J.Reine Angew.Math, 260, pp. 47-83 and 261, pp. 29-54, 1973.

[5] S.S. Abhyankar and T.T. Moh.- Embedding of the line in the plane, J.Reine Angew.Math., 276, pp. 148-166, 1975.
[6] A. Assi, Meromorphic plane curves, Math. Z. 230(1999), no. 1, 165-183
[7] V. Barucci, D. E. Dobbs, M. Fontana, Maximality Properties in Numerical Semigroups and Applications to One-Dimensional Analytically Irreducible Local Domains, Memoirs of the Amer. Math. Soc. **598** (1997).
[8] J. Bertin, P. Carbonne, Semi-groupes d'entiers et application aux branches, J. Algebra **49** (1977), 81-95.
[9] Decker, W.; Greuel, G.-M.; Pfister, G.; Schönemann, H.: SINGULAR 3-1-6 — A computer algebra system for polynomial computations. http://www.singular.uni-kl.de (2012).
[10] M. Delgado, J. I. Farrán, P. A. García-Sánchez, D. Llena, On the weight hierarchy of codes coming from semigroups with two generators, IEEE Transactions on Information Theory 60 (2014), 282 - 295.
[11] M. Delgado, P.A. García-Sánchez, and J. Morais, "numericalsgps": a `gap` package on numerical semigroups,
`(http://www.gap-system.org/Packages/numericalsgps.html)`.
[12] C. DELORME. *Sous-monoïdes d'intersection complète de* $\mathbb{N}$. Ann. Scient. École Norm. Sup. (4), **9** (1976), 145-154.
[13] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.7.5*; 2014,
`(http://www.gap-system.org)`.
[14] Geroldinger, A.; Halter-Koch, F. *Non-Unique Factorizations. Algebraic, Combinatorial and Analytic Theory*, Pure and Applied Mathematics, vol. 278, Chapman & Hall/CRC, 2006.
[15] J. Herzog, Generators and relations of abelian semigroups and semigroup rings, *Manuscripta Math.* 3 (1970), 175–193.
[16] M. Lejeune Jalabert.-Sur l'équivalence des singularités des courbes algebroides planes. Coefficients de Newton, Thesis, 1972.
[17] J. L. Ramírez Alfonsín, The Diophantine Frobenius Problem, Oxford University Press, 2005.
[18] J. C. Rosales y P. A. García-Sánchez, Numerical semigroups, Developments in Mathematics, 20. Springer, New York, 2009.
[19] K. Watanabe, Some examples of one dimensional Gorenstein domains, Nagoya Math. J. **49** (1973), 101–109.
[20] O. Zariski.-Le problème des modules pour les branches planes, Cours au Centre de Mathématiques, Ecole Polytechnique, 1973.

UNIVERSITÉ D'ANGERS, MATHÉMATIQUES, 49045 ANGERS CEDED 01, FRANCE
E-mail address: `assi@univ-angers.fr`

DEPARTAMENTO DE ÁLGEBRA AND CITIC-UGR, UNIVERSIDAD DE GRANADA, E-18071 GRANADA, ESPAÑA
E-mail address: `pedro@ugr.es`