On the class semigroup of a numerical semigroup

Valentina Barucci and Faten Khouja

Abstract

The class semigroup of a numerical semigroup $S$ is the semigroup $S(S)$ of classes of the relative ideals of $S$. Our aim is to find some properties of $S(S)$. In particular we observe that $S(S)$ is finite and compute its cardinality in some cases, using the poset of gaps of $S$. Moreover, we study the generators of $S(S)$ and the reduction number of its elements.

Keywords: Numerical semigroup, class semigroup, reduction number.
AMS Subject Classification: 20M14

1 Introduction

A numerical semigroup is a subset $S$ of the set of nonnegative integers $\mathbb{N}$ that is closed under addition, with $0$ and with finite complement in $\mathbb{N}$. A relative ideal of $S$ is a nonempty subset $I$ of $\mathbb{Z}$ such that $I + S \subseteq I$ and $I + s \subseteq S$ for some $s \in S$. This last condition is equivalent to request that $I$ is bounded below. The relative ideals of $S$ are known also as $S$-semimodules. The set of relative ideals of $S$ is a commutative semigroup with respect to the sum of ideals and it is a finite semigroup modulo the congruence $\sim$ defined setting $I \sim J$ if there exists $z \in \mathbb{Z}$ such that $I = J + z$.

Other finite commutative semigroups which arise from numerical semigroups have been recently studied by M. Delgado and V.H. Fernandes in [5]. The semigroup of classes of the relative ideals of $S$ which we study in this paper is indicated by $S(S)$ and corresponds to the semigroup of classes of nonzero fractional ideals of an integral domain. Not much is known about $S(S)$ and its cardinality has been valuated in terms of the generators of $S$ only for $S$ of embedding dimension two (cf. [8, Theorem 3.7]).

It turns out that the study of $S(S)$ is strictly connected to the study of the set of gaps of $S$, i.e. $G(S) = \mathbb{N} \setminus S$, which is a finite poset with respect to the order relation defined by $a \preceq b$ if there exists $s \in S$ such that $a + s = b$. The type of $S$ is given by the number of maximal
elements in the poset $G(S)$ (cf. Lemma 2.5.2), and $G(S)$ can always be partitioned in $e - 1$ chains, where $e$ is the multiplicity of $S$. We show that the partition of $G(S)$ in $e - 1$ chains is unique if and only if $S$ is of maximal embedding dimension (cf. Theorem 2.11), we give an upper bound for the cardinality of $G(S)$ in terms of the cardinality of these chains (cf. Corollary 2.10) and characterize the numerical semigroups such that this bound is attained (cf. Theorem 2.15).

In Section 3, we also give some results on the generators of the class semigroup $S(S)$. In particular we characterize a three-generated element of $S(S)$ which is a minimal generator of $S(S)$ (cf. Proposition 3.3) and compute the number of minimal generators of $S(S)$ in case of multiplicity 3 (cf. Corollary 3.6).

The reduction number $r(I)$, with $I \in S(S)$, is studied in the last section and a precise formula for a two-generated $I$ is given, if $S$ is a semigroup which realizes the bound of Corollary 2.10 (cf. Theorem 4.5). Finally, using the semigroup version of a well known fact of ring theory, i.e. $r(I) \leq e - 1$, we deduce an arithmetic corollary (cf. Corollary 4.12) and show that, for any numerical semigroup $S$ of multiplicity $e$, there exists $I \in S(S)$ with reduction number $r(I)$ equal to $i$, for each $i, 1 \leq i \leq e - 1$.

Throughout the paper we will use the following notation. $S$ is a numerical semigroup. $M = S \setminus \{0\}$ is the maximal ideal of $S$, $e$ is the multiplicity of $S$, $f$ is the Frobenius number of $S$, that is the greatest integer which does not belong to $S$, $n_2$ is the number of elements of $S$ smaller than $f$. Thus we have $S = \{0 = s_0 < s_1 = e < s_2 < \ldots < s_{n_2} = f + 1, \rightarrow\}$. It is well known that if $I$ is a relative ideal of a numerical semigroup $S$, then $I \setminus (I + M)$ is the unique minimal set of generators of $I$ and so the minimal number of generators of $I$ is $\nu(I) = |I \setminus (I + M)| \leq e$. If $I$ and $J$ are relative ideals of $S$, we set $I - J = \{x \in \mathbb{Z} \mid x + J \subseteq I\}$. The cardinality of $(S - M) \setminus S$ is called the type of $S$. Finally we denote by $g$ the genus of $S$, i.e. the cardinality of $G(S) = N \setminus S$.

2 The class semigroup and its cardinality

Given a numerical semigroup $S$, we consider the set $R(S)$ of relative ideals of $S$. If $I, J \in R(S)$, then $I + J = \{i + j; i \in I, j \in J\}$ is also a relative ideal of $S$, and so $R(S)$ is a monoid with respect to this addition. We define an equivalence relation on $R(S)$ by:

$$I \sim J \iff \exists z \in \mathbb{Z} \text{ such that } I = J + z.$$ 

Moreover, for all $I, I', J, J' \in R(S)$, if $I \sim I'$ and $J \sim J'$ then $I + J \sim I' + J'$, thus "\sim" is a congruence on $R(S)$.
Definition 2.1. The monoid \( S(S) = R(S)/\sim \), the quotient monoid of \( R(S) \) modulo \( \sim \), is the class semigroup of \( S \).

The identity element of \( S(S) \) is clearly \([S]\), the class containing all the principal ideals.

Lemma 2.2. Let \( I \) be a relative ideal of \( S \), then there exists a relative ideal \( I_0 \) of \( S \) such that \( I \sim I_0 \) and \( S \subseteq I_0 \subseteq \mathbb{N} \).

Proof. We take \( I_0 = I - i_0 \), where \( i_0 \) is the multiplicity of \( I \) i.e. the smallest integer in \( I \). We have that if \( x \in I \), then \( x \geq i_0 \) so \( x - i_0 \geq 0 \), thus \( I_0 \subseteq \mathbb{N} \). Moreover, \( I - i_0 + S = I + S - i_0 \subseteq I - i_0 = I_0 \), thus \( I_0 \) is a relative ideal of \( S \) with multiplicity 0. Finally, if \( s \in S, s = 0 + s \in I_0 \), so \( S \subseteq I_0 \). Therefore, \( I \sim I_0 \) and \( S \subseteq I_0 \subseteq \mathbb{N} \).

We observe that if \( I \sim J \), then \(|I \setminus (I + M)| = |J \setminus (J + M)| \) and if \( S \subseteq I \subseteq \mathbb{N} \), then \( I \setminus (I + M) \) is a set of the form \( \{0, g_1, \ldots, g_n\} \), where \( g_k \in G(S) \) for all \( k, 1 \leq k \leq n \), and \( g_k - g_l \notin S \), for all \( k \neq l \), (in \([8]\) such a set is called an \( S \)-Lean). In this case we will write \( I = (0, g_1, \ldots, g_n) \), always assuming \( 0 < g_1 < \cdots < g_n \). In what follows, we represent every class of \( S(S) \) by its unique representative \( I, S \subseteq I \subseteq \mathbb{N} \).

Proposition 2.3. \( S(S) \) is a group if and only if \( S = \mathbb{N} \).

Proof. If \( S = \mathbb{N} \), then \(|S(S)| = 1 \) and \( S(S) = \{S\} = \{\} \). Thus, \( S(S) \) is the trivial group. Conversely, if \( S(S) \) is a group, then for every \( I \in S(S) \), there exists \( J \in S(S) \) such that \( I + J = S \). Observing that \( \mathbb{N} \) is a relative ideal of \( S \), for each \( S \), we can take \( I = \mathbb{N} \), then \( S = \mathbb{N} + J = \mathbb{N} \), thus \( S = \mathbb{N} \).

Proposition 2.4. Let \( S \) be a numerical semigroup of genus \( g \). Then, \(|S(S)| \leq 2^g \). In particular, \( S(S) \) is finite.

Proof. As we have seen, for each \( I \in S(S) \), \( I = (0, g_1, \ldots, g_n) \), where \( g_k \in G(S) \). Associating to \( I = (0, g_1, \ldots, g_n) \) the subset \( \{g_1, \ldots, g_n\} \) of \( G(S) \), we get an injective map from \( S(S) \) to the power set of \( G(S) \). Since \(|G(S)| = g \), we have \(|S(S)| \leq 2^g \).

The cardinality of \( S(S) \) has been precisely computed in case \( S \) is generated by two elements. In fact, in \([8, \text{Theorem 3.7}]\), it is shown that if \( S = \langle d_1, d_2 \rangle \) then \(|S(S)| = \frac{1}{d_1 + d_2} \left( \frac{d_1 + d_2}{d_1} \right) \).

We consider the partial order relation \( \prec \) on \( G(S) \) defined by

\[
a \prec b \iff \exists s \in S \text{ such that } a + s = b,
\]

we write \( a \prec b \) if \( a \prec b \) and \( a \neq b \), in this case we say that \( b \) is above \( a \). We list some, partially already known, properties of this order:
Lemma 2.5. 1) The minimal elements of $G(S)$ are $\{1, \ldots, e-1\}$.
2) The number of maximal elements in $G(S)$ is the type of $S$. In particular, $S$ is symmetric if and only if $G(S)$ has a maximum and $S$ is of maximal embedding dimension if and only if $G(S)$ has $e-1$ maximal elements.

Proof. 1) Let $a \in G(S)$, then $a \equiv i \pmod{e}$, $1 \leq i \leq e-1$, thus $i \lessdot a$. Therefore, for each $i$, $1 \leq i \leq e-1$, $i$ is minimal and if $a = i + ke$, with $k > 0$, then $a$ is not minimal.
2) The maximal elements in $G(S)$ are the pseudo-Frobenius numbers of $S$ (cf. [9, Proposition 2.19]) and the cardinality of this set is the type of $S$.

Let $P$ be a poset and $s, t \in P$, then we say that $t$ covers $s$ or $s$ is covered by $t$, if $s \prec t$ and no element $u \in P$ satisfies $s \preceq u \prec t$.

The Hasse diagram of a finite poset $P$ is the graph whose vertices are the elements of $P$, and the edges are the cover relations, and such that if $s \prec t$ then $t$ is drawn above $s$. An antichain of a poset $P$ is a subset $A$ of $P$ such that any two distinct elements of $A$ are incomparable [10]. The width of a poset is the maximum cardinality of an antichain. A chain of a poset $P$ is a subset $C$ of $P$ such that any two elements of $C$ are comparable. We say that two chains $C_i$ and $C_j$ are incomparable if $h$ is incomparable with $k$ for each $(h, k) \in C_i \times C_j$. The length $l(C)$ of a finite chain is defined by $l(C) = |C| - 1$.

We are interested in studying the poset $G(S)$.

Proposition 2.6. Let $h_1, \ldots, h_r \in G(S)$.

1) The set $\{h_1, \ldots, h_r\}$ is an antichain of $G(S)$ $\iff (0, h_1, \ldots, h_r)$ is a minimal system of generators of an element $I \in S(S)$. Thus the number of elements in $S(S)$ is the number of antichains in the Hasse diagram of $G(S)$.

2) The number of antichains of cardinality $r$ equals the number of elements of $S(S)$ generated by $r+1$ elements.

Proof. 1) The result follows immediately from the definitions:

$\{h_1, \ldots, h_r\}$ is an antichain $\iff h_j - h_i \notin S, \forall i, j, 1 \leq i < j \leq r$

2) The antichains of cardinality $r$ in the poset $G(S)$ are in one to one correspondence with the elements $S(S)$ generated by $r+1$ gaps.

According to Dilworth’s Theorem ([6, Theorem 2.1, page 438]), if $P$ is a poset of width $m$, then there exists a partition $P = C_1 \cup C_2 \cup \ldots \cup C_m$ where each $C_i$ is a chain.
Example 2.7. Let $S = \langle 4, 5 \rangle$, $G(S) = \{1, 2, 3, 6, 7, 11\}$. The Hasse diagram of $G(S)$ is:

```
11
7
3
6
12
```

The width of $G(S)$ is 3 and we have: $P = C_1 \cup C_2 \cup C_3$, where $C_1 = \{1, 6\}$, $C_2 = \{2\}$, $C_3 = \{3, 7, 11\}$ or else $P = C_1' \cup C_2' \cup C_3'$ where $C_1' = \{1, 6, 11\}$, $C_2' = \{2, 7\}$, $C_3' = \{3\}$. Thus such a partition of the poset $G(S)$ is not unique.

Proposition 2.8. 1) The width of $G(S)$ is $e - 1$.
2) For each $a \in G(S)$, there are at most $n_S - 1$ elements above $a$. In particular, any chain in $G(S)$ contains at most $n_S$ elements.
3) If $C_1 \cup \ldots \cup C_{e-1}$ is a partition of $G(S)$ in $e-1$ chains and $|C_k| = c_k$, for $1 \leq k \leq e - 1$, then the number of elements of $S(S)$ generated by $i + 1$ elements is less or equal to:

$$\sigma_i(c_1, \ldots, c_{e-1})$$

where $\sigma_i$ is the elementary symmetric polynomial of degree $i$ in $c_1, \ldots, c_{e-1}$.

Proof. 1) $\{1, 2, \ldots, e - 1\}$ is an antichain of $G(S)$ of cardinality $e - 1$. Moreover any set of gaps with more than $e - 1$ elements contains at least two elements congruent mod $e$, which are comparable.
2) For each $a \in G(S)$ we have that at most $a + s_0, a + s_1, \ldots, a + s_{n_S-1}$ are not in $S$.
3) $G(S) = C_1 \cup \ldots \cup C_{e-1}$, where we denote by $C_i$ a chain with minimal element $i$. Two distinct elements in an antichain must be in two different chains. Thus the number of antichains of cardinality $i$ is at most:

$$\sum_{1 \leq j_1 < j_2 < \ldots < j_i \leq e-1} c_{j_1} c_{j_2} \ldots c_{j_i} = \sigma_i(c_1, \ldots, c_{e-1}).$$

Finally, recall that by Proposition 2.6,2) the number of antichains of cardinality $i$ equals the number of elements of $S(S)$ generated by $i + 1$ elements. 

\[ \square \]
Observe that the number of classes of $S(S)$ generated by two elements is equal to the genus of $S$ which is equal also to $\sigma_1(c_1, \ldots, c_{e-1}) = c_1 + \ldots + c_{e-1}$. As a matter of fact a class generated by two elements is generated by 0 and a gap.

**Example 2.9.** Let $S = \langle 3, 7 \rangle$, where the partition $G(S) = C_1 \cup C_2$ is that described in the picture:

![Diagram](image.png)

We have the empty antichain of cardinality $i = 0$ which corresponds to the class $S \in S(S)$ generated by $\{0\}$.

The number of antichains containing one element is the number of gaps of $S$, which is also equal to $\sigma_1(c_1, c_2) = c_1 + c_2 = 6$.

The antichains of cardinality 2 are: $\{1, 2\}$, $\{1, 5\}$, $\{4, 2\}$, $\{4, 5\}$, $\{4, 8\}$ which correspond to the classes: $(0, 1, 2)$, $(0, 1, 5)$, $(0, 2, 4)$, $(0, 4, 5)$, $(0, 4, 8)$.

However $\sigma_2(c_1, c_2) = c_1 \cdot c_2 = 2 \cdot 4 = 8$ which is strictly greater than 5, the number of antichains of cardinality 2.

We can consider a different partition of $G(S)$, $G(S) = C'_1 \cup C'_2$, where $C'_1 = \{1, 4, 11\}$ and $C'_2 = \{2, 5, 8\}$. Also, $\sigma_2(c'_1, c'_2) = c_1 \cdot c_2 = 3 \cdot 3 = 9 > 5$.

**Corollary 2.10.**

$$|S(S)| \leq \sum_{i=0}^{e-1} \sigma_i(c_1, \ldots, c_{e-1}).$$

**Proof.** The cardinality of $S(S)$ is the sum of the cardinalities of classes of $S(S)$ generated by 1, 2, \ldots, $e$ elements. \qed
We will characterize in the following the semigroups $S$ such that the partition of $G(S)$ in chains is uniquely determined and those such that $|S(G)|$ realizes the bound of Corollary 2.10.

**Theorem 2.11.** $S$ is of maximal embedding dimension if and only if the partition of $G(S)$ in $e - 1$ chains is unique.

*Proof.* If $S$ is of maximal embedding dimension, $G(S)$ has $e - 1$ maximal elements $1 + k_1 e, 2 + k_2 e, \ldots, e - 1 + k_{e-1} e$ (cf. Lemma 2.5.2). For $i = 1, \ldots, e - 1$, we denote by $C_i$ the chain $i, i + e, \ldots, i + k_i e$. Hence we have a partition: $G(S) = C_1 \cup \ldots \cup C_{e-1}$. Suppose that $C'_i \cup \ldots \cup C'_{e-1}$ is another partition of $G(S)$ in chains where $C'_i$ is a chain with minimal element $i$, for $i = 1, \ldots, e - 1$. We claim that $C'_i = C_i$ for each $i$.

We have $l(C_i) = k_i$, and each chain with minimal element $i$ has length $\leq k_i$ because $e$ is the smallest element in $S$. If $l(C'_i) < k_i$, then either there are more than $e - 1$ chains in the partition or there is some $j$ with $l(C'_j) > k_j$, a contradiction. So $l(C'_i) = l(C_i) = k_i$, for each $i$.

Suppose that $i$ is the maximum index such that $C'_i \neq C_i$. We have $C_i = \{i, i + e, i + 2e, \ldots, i + k_i e\}$ and $C'_i = \{i, a_1, \ldots, a_k\}$. If $h$ is the smallest index such that $a_h \neq i + he$, we have $a_h = j + he$, with $j < i$ or $j > i$. If $j < i$, then $a_h - a_{h-1} = j + he - (i + (h-1)e) = e - (i-j) \notin S$, a contradiction. If $j > i$, then $C'_i$ would be different from $C_j$, a contradiction with maximality of $i$. Thus $C'_i = C_i$.

Conversely, if $S$ is not of maximal embedding dimension then the maximal element in the poset $G(S)$ are less then $e - 1$ by Lemma 2.5.2). If $1 \leq i < j \leq e - 1$ are such that $m$ is a maximal element above both $i$ and $j$, then it is easy to see that the partition is not unique because $m$ can be included in a chain with minimal element $i$ or $j$. □

A numerical semigroup $S$ is called an Arf semigroup if $I_s - s_i$ is a semigroup, where $I_s = \{s \in S; s \geq s_1\}$. In this case we have $I_i - s_i = I_i - I_1 = \{x \in \mathbb{Z}; x + I_1 \subseteq I_s\}$ (cf. [2, Theorem 1.3.4 (vii)]).

Given an Arf semigroup $S = \{s_0 = 0 < s_1 < \ldots < s_{n_s} = f + 1 \rightarrow\}$, the multiplicity sequence of $S$ is $s_1 - s_0, s_2 - s_1, s_3 - s_2, \ldots$. It follows that the multiplicity sequence $e_0, e_1, \ldots, e_{n_s} = 1, e_{n_s+1} = 1, \ldots$ of an Arf semigroup is such that for all $i$, $e_i = \sum_{h=1}^{k} e_{i+h}$, for some $k \geq 1$. Conversely, any sequence of natural numbers $e_0, e_1, \ldots$ such that $e_n = 1$, for $n >> 0$, and, for all $i$, $e_i = \sum_{h=1}^{k} e_{i+h}$, for some $k \geq 1$, is the multiplicity sequence of an Arf semigroup $S = \{0, e_0, e_0 + e_1, e_0 + e_1 + e_2, \ldots\}$, [1].

**Proposition 2.12.** If $S$ is an Arf semigroup with multiplicity sequence $e_0, e_1, \ldots$ then in the Hasse diagram of $G(S)$, for all $0 \leq i \leq n_S$, there are $e_i - 1$ elements which have $i$ elements above.

*Proof.* By [3, Lemma 2.3], if $a \in G(S)$, then there are $i$ elements $b \in G(S)$ such that $a < b$, i.e. $a$ has valency $i + 1$, with the ter-
minology of [3], if and only if \( a \in (I_{i+1} - I_{i+1}) \setminus (I_i - I_i) \). Since 
\( S \) is Arf, we obtain 
\[ |I_{i+1} - I_{i+1} \setminus I_i| = |I_{i+1} - s_{i+1} \setminus I_i - s_i| = 
 |(I_{i+1} - (s_{i+1} - s_i)) \setminus I_i| = s_{i+1} - s_i - 1 = e_i - 1. \]

\[ \blacksquare \]

**Example 2.13.** Let \( S = \{0, 6, 9, 12, 15, \rightarrow\} \). The multiplicity sequence of \( S \) is \( e_0 = 6, e_1 = 3, e_2 = 3, e_3 = 3, e_4 = 1 \). And its poset \( G(S) \) is:

Consider for example \( i = 0 \). We have \( e_0 = 6 \), so there are 5 elements
which have 0 elements above: they are 3, 11, 14, 10, 13. For \( i = 3 \), we
have \( e_3 = 3 \), so there are 2 elements which have 3 elements above: they
are 1 and 2.

**Lemma 2.14.** If two consecutive natural numbers \( s, s + 1 \) are in an
Arf semigroup \( S \), then \( f < s \).

**Proof.** \( (s + 1) - s = 1 = e_i \), so \( e_j = 1 \), for all \( j \geq t \). Thus, \( S = 
\{0, e_0, e_0 + e_1, \ldots, s = e_0 + \ldots + e_{i-1}, \rightarrow\} \). Hence \( f < s \).

**Theorem 2.15.** Given a partition \( C_1 \cup \ldots \cup C_{e-1} \) of \( G(S) \) with \( |C_i| = 
c_i \), the following conditions are equivalent:

1) \( |S(S)| = \sum_{i=0}^{e-1} \sigma_i(c_1, \ldots, c_{e-1}). \)
2) The chains \( C_1, \ldots, C_{e-1} \) are pairwise incomparable.
3) \( S = \{0, e, 2e, \ldots, (n-1)e, (n-1)e + j, \rightarrow\} \), for some \( n \in \mathbb{N} \) and \( j \),
   \( 1 < j \leq e \).
4) \( S \) is Arf and \( C_i \) is incomparable with \( C_i \), for each \( i = 2, \ldots, e-1 \).
5) \( |C_1| = n_S \).

**Proof.** All the conditions are trivially satisfied if \( e = 2 \). Thus we can
suppose that \( S \) has multiplicity \( e > 2 \).

1) \( \Rightarrow 2) \) If \( C_i \) and \( C_j \) are comparable, i.e. there exist \( a \in C_i \), \( b \in C_j \)
   such that \( b = a + s \), for some \( s \in S \), then we have \( (0, a, b) = (0, a) \). Thus
   the number of 3-generated classes is strictly less than \( \sigma_2(c_1, \ldots, c_{e-1}) \).
   So, \( |S(S)| < \sum_{i=0}^{e-1} \sigma_i(c_1, \ldots, c_{e-1}) \), a contradiction.

2) \( \Rightarrow 1) \) The number of antichains of cardinality \( i \), which by Proposition
   2.6.2 equals the number of \( i + 1 \)-generated elements of \( S(S) \), is
   \( \sigma_i(c_1, \ldots, c_{e-1}) \) if the chains are two by two incomparable.
2) \( \Rightarrow 3) \) Let \( s \in S \), \( s < f \) be the biggest element that is not a multiple.
of $e$. Then $s + 1$ or $s + 2$ is a gap and so $1 \nless s + 1$ or $2 \nless s + 2$. Thus the chain $C_1$ or the chain $C_2$ is not incomparable with the chain where the gap $s + 1$ or $s + 2$ is. Thus we have a contradiction.

3) $\Rightarrow$ 2) Suppose that there exist $i, j$, $i \neq j$ such that $C_i$ and $C_j$ are comparables, i.e. there exist $a = i + he \in C_i$, $b = j + te \in C_j$ such that $b = a + s$, with $s \in S$. Since $s < f$, we have $s = le$, for some $l \in \mathbb{N}$. It follows that $i \equiv j \pmod{e}$, a contradiction.

3) $\Rightarrow$ 4) It is easy to see that $S$ is Arf. Moreover, the implication 3) $\Rightarrow$ 2) gives in particular that $C_1$ is incomparable with $C_i$, if $i \neq 1$.

4) $\Rightarrow$ 5) By Lemma 2.14 we have that $1 + s_i \notin S$ for each $i$, $i = 0, \ldots, n_S - 1$. So by Proposition 2.8,2) and since $C_1$ is incomparable with $C_i$ we have $|C_1| = n_S$. Therefore $S$ is of the form described in 3).

If $S$ is a numerical semigroup such that there exists a partition $C_1 \cup \ldots \cup C_{e-1}$ of $G(S)$ which satisfies one of the equivalent conditions of the Theorem 2.15, then $S$ is Arf, hence of maximal embedding dimension and the partition is unique.

Such $S = \{0, e, 2e, \ldots, (n - 1)e, (n - 1)e + j, \rightarrow\}$ has $n_S = n$ elements before the Frobenius number, it has $(e - 1)(n - 1) + j - 1$ gaps and the chains $C_1, \ldots, C_{e-1}$ have cardinality $c_i = n$ (for $i = 1, \ldots, j - 1$), $c_i = n - 1$ (for $i = j, \ldots, e - 1$). In particular, if $j = e$, we have:

**Corollary 2.16.** If $S = \langle e, ne+1, \ldots, ne+(e-1) \rangle = \{0, e, 2e, \ldots, ne, \rightarrow\}$, then

$$|S(S)| = \sum_{i=0}^{e-1} \binom{e - 1}{i} n^i.$$  

**Proof.** By Theorem 2.15, $|S(S)| = \sum_{i=0}^{e-1} \sigma_i(c_1, \ldots, c_{e-1})$. Moreover $c_i = n$ for $i = 1, \ldots, e - 1$ and $\sigma_i(n, \ldots, n) = \binom{e - 1}{i} n^i$. As a matter of fact, the Hasse diagram of $G(S)$ is:
If we set \( n = 1 \) in Corollary 2.16, we get a semigroup of genus \( g = e - 1 \) with \(|S(S)| = 2^g\). Thus the inequality of Proposition 2.4 is in this case an equality:

**Corollary 2.17.** Let \( S = \langle e, e + 1, e + 2, \ldots, 2e - 1 \rangle \). Then,

\[
|S(S)| = 2^{e-1}.
\]

**Proof.** We have \( \sum_{i=0}^{e-1} \binom{e-1}{i} = 2^{e-1} \). As a matter of fact the Hasse diagram of \( G(S) \) is:

\[
\begin{array}{cccc}
1 \bullet & 2 \bullet & \ldots & e - 1 \bullet
\end{array}
\]

We close the section with some examples of symmetric and pseudo-symmetric semigroups and their poset of gaps.

**Example 2.18.** 1) Let \( S = \langle e, e + 1, \ldots, 2e - 2 \rangle \). Then:

\[
|S(S)| = 2^{e-1} + 1.
\]

The Frobenius number of \( S \) is \( f = 2e - 1 \) and its genus is \( g = e = \frac{f + 1}{2} \), thus it is a symmetric semigroup. The Hasse diagram of \( G(S) \) is:
The antichains of $G(S)$ are the subsets of the set $\{1, \ldots, e-1\}$ and the set $\{f\}$. Thus, $|S(S)| = 2^{e-1} + 1$

2) Let $S = \{0, e, e + 1, \ldots, 2e - 3, 2e - 1, \rightarrow\}$, with $e > 2$. Then:

$$|S(S)| = 2^{e-1} + 2.$$ 

The pseudo-Frobenius numbers of $S$ are $f = 2e - 2$ and $e - 1 = \frac{2e-2}{2}$, thus it is a pseudo-symmetric semigroup. Tracing the Hasse diagram of $G(S)$,

we obtain that the antichains of $G(S)$ are all the subsets of $\{1, \ldots, e-1\}$ (in number of $2^{e-1}$), the set $\{f\}$ and the set $\{f, f^{2} = e - 1\}$. Thus, $|S(S)| = 2^{e-1} + 2$.

3 The generators of the class semigroup

For each numerical semigroup $S$, $S(S)$ is a finite commutative semigroup and there are not invertible elements besides $S$, so it has a unique minimal system of generators. As usual, $I \in S$ is a generator if for all $J, K \in S$ such that $I = J + K$, we have $J = I$ or $K = I$.

Denote by $\mu$ the cardinality of the minimal system of generators of $S(S)$. 

11
**Proposition 3.1.** Let $S$ be a numerical semigroup of genus $g$. Then, $\mu \geq g + 1$.

*Proof.* We claim that each two-generated class of ideals, $I = (0, h)$ is a generator of $S(S)$. In fact, if there exist $J, K \in S(S)$, $J \neq I$ and $K \neq I$ such that $I = J + K$, $J = (0, h_1, \ldots, h_n)$, $K = (0, k_1, \ldots, k_m)$, then $h_1, \ldots, h_n, k_1, \ldots, k_m \in (0, h)$. Thus $h_i = h + s_i$, $1 \leq i \leq n$ and $k_j = h + t_j$, $1 \leq j \leq m$, where $s_i, t_j \in S$. Therefore, $\forall i, 1 \leq i \leq n, \forall j, 1 \leq j \leq m, h_i, k_j \geq h$. Since $h \in J + K$, then $h_1 = h$ or $k_1 = h$, thus $J = I$ or $K = I$. It follows that $I = (0, h)$ is a necessary generator of $S(S)$. Since the class $S$ of principal ideals is also a generator, we get at least $g + 1$ generators for $S(S)$.

**Example 3.2.** Let $S = \langle 2, 2k + 1 \rangle$ of genus $k$. Let $I \in S(S)$, then either $I = S$ or $I$ is of the form $(0, h)$ with $h \in G(S)$. By the preceding proposition all these elements are generators of $S(S)$. Thus, $\mu(S(S)) = k + 1$. Indeed in this case, $|S(S)| = k + 1$ by Corollary 2.16, so all the elements of $S(S)$ are generators.

**Proposition 3.3.** Let $I = (0, h_1, h_2)$ be a three-generated class in $S(S)$. Then

$I$ is a generator of $S(S) \iff h_2 - h_1 \notin I$ and $h_1 + h_2 \notin I$.

*Proof.* We prove the equivalent assertion:

$s$ If $h_2 - h_1 \in I$, then $I = (0, h_1) + (0, h_2 - h_1)$.

If $h_1 + h_2 \in I$, then $I = (0, h_1) + (0, h_2)$.

$\Rightarrow$ Since $I$ is not a generator, there exist $J, K \in S(S)$, $J \neq I$ and $K \neq I$ such that $I = J + K$, $J = (0, f_1, \ldots, f_l)$, $K = (0, g_1, \ldots, g_m)$. Since $J, K \subseteq I$, $f_i \geq h_1$, for all $i$ and $g_j \geq h_1$, for all $j$. As, $h_1 \in I = J + K$, then $h_1 = f_1$ or $h_1 = g_1$. We set for example $h_1 = f_1$. Since $h_2 \in J + K$ and $h_2 \notin J$ (because $I \neq J$), we have that $h_2$ is realized as a sum and so $h_2 = 2h_1 + s$, for some $s \in S$, hence $h_2 - h_1 = h_1 + s \in I$, or $h_2 \in K$ and so $h_1 + h_2 \in J + K = I$. \qed

**Example 3.4.** Let $S = (5, 6)$.

- $I = (0, 1, 2)$, $2 - 1 = 1 \in I$ then $I$ is not a generator, $I = (0, 1) + (0, 1)$ or $I = (0, 1, 14) + (0, 1)$.
- $I = (0, 1, 3)$, $1 + 3 = 4 \notin I$ and $3 - 1 = 2 \notin I$ then $I$ is a generator.
- $I = (0, 2, 3)$, $2 + 3 = 5 \in I$, then $I$ is not a generator, $I = (0, 2) + (0, 3)$.

**Corollary 3.5.** If $h_1, h_2 \in G(S)$, $h_1 \neq h_2$, such that $h_1, h_2 \leq \frac{s}{2}$ and $h_2 \neq 2h_1$ then $I = (0, h_1, h_2)$ is a generator of $S(S)$. 

12
Proof. We have $h_1 + h_2 < e$, thus $h_1 + h_2 \notin I$. Since $h_2 \neq 2h_1$ also $h_2 - h_1 \notin I$ and we can apply Proposition 3.3. \qed

**Corollary 3.6.** Let $S$ be of multiplicity 3 and genus $g$. Then

$$
\mu = g + 1
$$

Proof. Let $I = (0, h_1, h_2) \in S(S)$, then $h_1 = 3k_1 + r_1$, $r_1 = 1$ or $2$, and $h_2 = 3k_2 + r_2$, $r_2 = 1$ or $2$, for some $k_1, k_2 \in \mathbb{N}$.

If $r_1 = r_2$ then $h_2 - h_1 \in S$ and, by Proposition 3.3, $I$ is not a generator.

If $r_1 = 1$ and $r_2 = 2$ then $h_1 + h_2 \in S$ and again, by Proposition 3.3, $I$ is not a generator. Thus, the generators of $S(S)$ are the classes generated by two elements, in number of $g$, and $S$. \qed

The inequality of Proposition 3.1 can be strict as shown in the following example:

**Example 3.7.** Let $S = \langle 5, 6, 7, 8, 9 \rangle$, $I = (0, 1, 3) \in S(S)$ is a generator of $S(S)$ by Proposition 3.3. So, $\mu > g + 1$.

**Proposition 3.8.** Let $I = (0, h_1, \ldots, h_k) \in S(S)$. If $h_i + h_j \notin I$ and $h_i - h_j \notin I$ for all $i > j$, then $I$ is a generator of $S(S)$.

Proof. Suppose there exist $J, K \in S(S)$ such that $I = J + K$, $J = (0, f_1, \ldots, f_l)$, $K = (0, g_1, \ldots, g_p)$. We show that $J = I$ or $K = I$.

Since $J, K \subseteq I$, we have $f_i, g_j \geq h_1$ for all $i$ and $j$. As $h_1 \in I = J + K$, then $h_1 = f_1$ or $h_1 = g_1$. We assume that $h_1, \ldots, h_i \in J$ and show $h_{i+1} \in J$. Since $h_{i+1} \in I$ then $h_{i+1} \in J$ or $h_{i+1} \in K$ or $h_{i+1}$ is realized as a sum, $h_{i+1} = h_i + g_1 + s$, for some $s \in S$. If $h_{i+1} \in K$, then $h_{i+1} + h_1 \in I$, a contradiction. If $h_{i+1} = h_j + g_1 + s$, then $h_{i+1} - h_j = g_1 + s \in K \subseteq I$, also a contradiction. Thus, $h_{i+1} \in J$ and $I = J$. \qed

**Example 3.9.** Let $S = \{0, 9, \rightarrow\}$ and $I = (0, 1, 3, 5)$. We have $1 + 3, 1 + 5, 3 + 5, 3 - 1, 5 - 1, 5 - 3 \notin I$, so $I$ is a generator of $S(S)$.

The converse of Proposition 3.8 is not true as shown in the example below.

**Example 3.10.** Let $S = \{6, 7, 8, 9, 10, 11\} = \{0, 6, \rightarrow\}$ and $I = (0, 1, 2, 4)$. We claim that $I$ is a generator. In fact, suppose $I = J + K$. We have $1 \in J + K$, thus $1 \in J$ or $1 \in K$, say $1 \in J$. We have $2 \in J + K$.

If $2 \in K$ then $2 + 1 = 3 \in I$, a contradiction. Thus, $1 \in J \cap K$ and $2 \notin J \cup K$ or $1, 2 \in J$ and $1, 2 \notin K$. We have $4 \in J + K$. If $4 \in K$, then $4 + 1 = 5 \in I$, a contradiction. Hence $J = (0, 1, 2, 4)$, and so $I$ is a generator. However for example $4 + 2 = 6 \in I$, $2 - 1 = 1 \in I$. 

13
4 The reduction number in $S(S)$

Similarly to ring context, the reduction number $r(J)$ of a relative ideal $J$ of a numerical semigroup $S$ is by definition the smallest positive integer $r$ such that $(r+1)J = rJ + e(J)$, where $e(J)$ is the multiplicity of $J$, i.e. the smallest integer in $J$. With $rJ$ we mean $J + \cdots + J$ ($r$ summands).

We observe now that the reduction number is well defined for a class of ideals, i.e. for an element of $S(S)$.

Lemma 4.1. If $I \sim J$ are relative ideals of a numerical semigroup $S$, then $r(I) = r(J)$.

Proof. If $I \sim J$ they are both in the same class of an ideal $I_0$ of multiplicity zero, $S \subseteq I_0 \subseteq \mathbb{N}$ (cf. Lemma 2.2) and we have that $(r+1)I = rI + e(I)$ if and only if $(r+1)I_0 = rI_0$ if and only if $(r+1)J = rJ + e(J)$.

Hence we can extend to $S(S)$ the notion of reduction number setting $r([I]) := r(I)$.

As above, we can consider as representative of a class a relative ideal $I$ such that $S \subseteq I \subseteq \mathbb{N}$. So in this case, the multiplicity of $I$ is zero, and $r(I)$ is the smallest integer $r$ such that $rI = (r+1)I$.

Proposition 4.2. Let $I$ be a relative ideal of $S$ such that $S \subseteq I \subseteq \mathbb{N}$. Then,

$$ jI = (j+1)I \iff jI \text{ is a numerical semigroup.} $$

Proof. $\Rightarrow$ We claim that $jI = (j+k)I$, for each $k \geq 1$. For $k = 1$, is the hypothesis. We assume the equality for $k$ and show the equality for $k+1$. In fact: $(j+k+1)I = (j+k)I + I = jI + I = (j+1)I = jI$. Thus, $jI = nI$, for each $n \geq j$ and $jI$ is a numerical semigroup.

$\Leftarrow$ Trivial.

We can easily deduce the following well known fact:

Lemma 4.3. Let $M$ be the maximal ideal of $S$. Then:

$$ \nu(jM) = e, \text{ if } j \geq r(M). $$

Proof. Let $M_0 = M - e$. If $j \geq r(M) = r(M_0)$, then $jM_0 = (j+1)M_0$, therefore $jM + e = (j+1)M$, and so $\nu(jM) = |jM \setminus (j+1)M| = e$.

We characterize next when $r(I) \leq 2$ for each $I \in S(S)$. Recall that a commutative additive semigroup $S$ is called a Clifford semigroup if, for all $a$ in $S$, $a$ is regular according to Von Neumann, i.e. there exists $x$ in $S$ such that $a = 2a + x$, see [4].
Proposition 4.4. The following conditions are equivalent:
1) $S(S)$ is a Clifford semigroup.
2) $I = 2I$, for each $I \in S(S)$.
3) $S = \mathbb{N}$ or $S = \{2, 2k + 1\}$.

Proof. 1) $\Rightarrow$ 2) Let $I \in S(S)$. Then there exists a class $J$ of $S(S)$ such that $I = 2I + J$. Hence $2I \subseteq 2I + J = I$, so $I = 2I$.
2) $\Rightarrow$ 3) Suppose that $e > 2$. Let $I = \{0, 1, \ldots, e - 2, e, \rightarrow\}$, then $(e - 2) + 1 = e - 1 \notin I$, so $I \subset 2I$, a contradiction. Thus $e \leq 2$ and $S = \mathbb{N}$ or $S = \{2, 2k + 1\}$.
3) $\Rightarrow$ 1) The implication is trivial if $S = \mathbb{N}$. Let $I \in S(S)$ with $S = \{2, 2k + 1\}$ then $I = (0, h)$, $h \in G(S)$. Thus $2I = (0, h, 2h) = I$, since $2h \in S$. □

We can give a precise estimate of $r(I)$, for $I = (0, h) \in S(S)$, where $S$ is a semigroup as in Theorem 2.15. We have $S = \{0, e, 2e, \ldots, (n - 1)e, (n - 1)e + j = c, \rightarrow\}$, for some $j$, $1 < j \leq e$, that is $S$ contains all the multiples of $e$ and all the integers $\geq c$, which is the conductor.

Theorem 4.5. Let $S = \{0, e, 2e, 3e, \ldots, \rightarrow\}$ and $I = (0, h) \in S(S)$. Denote by $d$ the order of $h$ in $\mathbb{Z}_e$. Then,

1) If $c > (d - 1)h$, we have $r(I) = d - 1$.
2) If $c \leq (d - 1)h$, then $r(I) = q$ where $q$ is the biggest integer $j$ such that $jh < c$.

Proof. 1) Each element $a$ of $dI$ is of the form $a = a_1 + \ldots + a_d$, where each summand $a_i$ is in $S$ or $a_i = h + s$, with $s \in S$. If at least one summand $a_i$ is in $S$, then $a = a_1 + \ldots + a_d \in (d - 1)I$. If all the summands $a_i$ are of the form $h + s$, then, since $dh \equiv 0 \pmod{e}$, we have for some $k$, $a = dh + s = ke + s \in S \subseteq I \subseteq (d - 1)I$. Therefore $dI = (d - 1)I$ and so $r(I) \leq d - 1$. Moreover, since $c > (d - 1)h$, if $2 \leq j \leq (d - 1)$ we have $jh \in jI \setminus (j - 1)I$ and the inclusions $I \subset 2I \subset \ldots \subset (d - 1)I$ are all strict.
2) As shown in 1), we have a strict inclusion $(j - 1)I \subset jI$ if and only if $jh \notin S$, i.e. if and only if $jh < c$. □

Example 4.6. We consider $e = 6$, $c = 36$ so $S = \{0, 6, 12, 18, 24, 30, 36, \rightarrow\}$ and $I = (0, 7)$. In $\mathbb{Z}_6$ we have that the order of 7 is 6, $c > 5 \cdot 7 = (6 - 1) \cdot 7$, then by the previous Theorem $r(I) = 5$. However if we take $S = \{0, 6, 12, 18, 24, 28, \rightarrow\}$, $c = 28 = 4 \cdot 7$, then $r(I) = 3$.

The result below is known in ring theory, see [7, Theorem 2.1]. We show the same result for numerical semigroups.
**Theorem 4.7.** Let $I \in S(S)$ and $j \leq r(I)$ then:

$$\nu(jI) > j$$

**Proof.** Set $r = r(I)$. We have: $rI + M \subset rI$. Then there exist $a_1, \ldots, a_r \in I$ such that $a_1 + \ldots + a_r \notin (rI + M)$. We set: $y_0 = a_1 + \ldots + a_r$. Let $j \leq r$, we take: $y_{i,j} = a_{i+1} + \ldots + a_j$, for $0 \leq i \leq j$. Observe that $y_{i,j} \in (j - i)I \subseteq jI$; in particular $y_{i,j} = 0 \in S \subseteq jI$, so we have $j + 1$ distinct elements of $jI$. It’s enough to show that $y_{i,j} \notin jI + M$. Let $0 \leq i \leq j$, we assume $y_{i,j} \notin jI + M$, then:

$$y_{i,j} = y_{i,j} + a_1 + \ldots + a_i \in jI + M + I \subseteq rI + M.$$

Hence $y_{0,j} \in rI + M$, and so $y_0 = y_{0,j} + a_{j+1} + \ldots + a_r \in rI + M + (r - j)I \subseteq rI + M$, which contradicts the choice of $y_0$. Thus, $\nu(jI) > j$, if $j \leq r$. \hfill \square

**Corollary 4.8.** For each $I \in S(S)$, we have

$$r(I) \leq e - 1$$

**Proof.** Set $r = r(I)$. By Theorem 4.7, we have $r < \nu(rI)$, that is $r + 1 \leq \nu(rI) \leq e$. Thus, $r \leq e - 1$. \hfill \square

**Proposition 4.9.** For all $r$, $1 \leq r \leq e - 1$, there exists $I \in S(S)$ such that $r(I) = r$.

**Proof.** For $r = 1$ we take $I = S$, otherwise we take $I = \{0, 1, r + 1, \rightarrow\}$. We have $N = rI = (r + 1)I$, and $r$ is the smallest integer which satisfies the equality. \hfill \square

**Example 4.10.** Let $S = \langle 4, 5, 6 \rangle = \{0, 4, 5, 6, 8, \rightarrow\}$. If $I = \{0, 1, 4, \rightarrow\}$ then $r(I) = 3$. If $J = \{0, 1, 3, \rightarrow\}$ then $r(J) = 2$. $I = S$, $r(S) = 1$.

**Corollary 4.11.** The multiplicity $e$ of $S$ is equal to $m + 1$, where $m = \max\{r(I); I \in S(S)\}$.

**Proof.** According to Corollary 4.8, $m \leq e - 1$. By Proposition 4.9, there exists $I \in S(S)$ such that $r(I) = e - 1$. Thus $m + 1 = e$. \hfill \square

From Theorem 4.7, we easily get the following corollary which we could not find in the literature.

**Corollary 4.12.** Let $e, i_1, \ldots, i_n, a_1, \ldots, a_n \in \mathbb{N}$. Then there exist $a_1', \ldots, a_n' \in \mathbb{N}$ such that:

1) $a_1' + \ldots + a_n' < e$

2) $a_1i_1 + \ldots + a_ni_n \equiv a_1'i_1 + \ldots + a_n'i_n \pmod{e}$
Proof. Let \( j = a_1 + \ldots + a_n \). We consider a numerical semigroup \( S = \{0, e, 2e, \ldots, c, \rightarrow\} \), with \( c > a_1 i_1 + \ldots + a_n i_n \), and \( I \in \mathcal{S}(S) \) generated by \( 0, i_1, \ldots, i_n \).

By Corollary 4.8, there exists \( r < e \) such that \( rI = eI = (e+1)I = \ldots \). If \( j \leq r \), we take \( a'_i = a_i \), for each \( i \). If \( j > r \), we have \( a_1 i_1 + \ldots + a_n i_n \in jI = rI \). Thus, there exists \( a'_1, \ldots, a'_n, a'_1 + \ldots + a'_n = j' \leq r \) such that

\[
    a_1 i_1 + \ldots + a_n i_n = a'_1 i_1 + \ldots + a'_n i_n + s, \quad \text{with} \quad s \in S.
\]

Since \( a_1 i_1 + \ldots + a_n i_n < c \) and the only elements of \( S \) smaller than \( c \) are the multiples of \( e \), we have necessarily \( s = ke \), for some \( k \). Therefore,

\[
    a_1 i_1 + \ldots + a_n i_n \equiv a'_1 i_1 + \ldots + a'_n i_n \pmod{e}.
\]

\[ \square \]

Example 4.13. Let \( e = 6, i_1 = 2, i_2 = 7, a_1 = 3, a_2 = 5 \), we have \( a_1 i_1 + a_2 i_2 = 41 \). According to Corollary 4.12, we can find \( a'_1, a'_2 \in \mathbb{N} \) such that \( a'_1 + a'_2 < 6 \) and \( 41 \equiv a'_1 2 + a'_2 7 \pmod{6} \). We consider \( S = \{0, 6, 12, 18, 24, 30, 36, 42, \rightarrow\} \) and \( I = (0, 2, 7) \). By an easy calculation we get \( r(I) = 3 \), and \( a'_1 = 2, a'_2 = 1 \) are such that \( a'_1 + a'_2 = 3 < 6 \) and \( 41 \equiv (2 \cdot 2) + (1 \cdot 7) \pmod{6} \). We observe that such \( a'_1, \ldots, a'_n \) are not unique. In fact if we take: \( a_1 = 0, a_2 = 6 \), we have:

\[
    6 \cdot 7 \equiv 0 \cdot 2 + 0 \cdot 7 \pmod{6} \\
    \equiv 3 \cdot 2 + 0 \cdot 7 \pmod{6} \\
    \equiv 2 \cdot 2 + 2 \cdot 7 \pmod{6}
\]

From Theorem 4.7, we get the following result, well known in ring context:

Corollary 4.14. 1) Let \( I \in \mathcal{S}(S) \) be two-generated, then

\[
    \nu(jI) = j + 1, \quad \text{if} \quad j \leq r(I).
\]

2) If \( S = \langle e, b \rangle \), then \( r(M) = e - 1 \).

Proof. 1) We have: \( I = (0, h) \) then \( jI = (0, h, 2h, \ldots, jh) \). Thus, \( \nu(jI) \leq j + 1 \). Moreover, according to Theorem 4.7, \( \nu(jI) \geq j + 1 \). Therefore, the equality.

2) Set \( r = r(M) \). We have: \( \nu(M) = 2 \). According to 1), \( \nu(jM) = j + 1 \), if \( j \leq r \). Thus \( \nu(rM) = e = r + 1 \). Therefore, \( r = e - 1 \). \[ \square \]

Acknowledgements. We would like to thank the referee for her/his careful reading and helpful suggestions.
References


Valentina Barucci, Dipartimento di Matematica, Sapienza, Università di Roma, Piazzale A. Moro 2, 00185 Rome, ITALY.
e-mail: barucci@mat.uniroma1.it

Faten Khouja, Department of Mathematics, Faculty of Sciences, 5000 Monastir, TUNISIA.
e-mail: koja-faten@yahoo.fr