Journal of Mathematical Inequalities
Volume 1, Number 4 (2007), 491–501

CONTRACTIONS OF A NUMERICAL SEMIGROUP

J. C. ROSALES

(*communicated by R. Ger*)

Abstract. Given a numerical semigroup S, a positive integer a and $m \in S\setminus\{0\}$, we introduce the set $\mathrm{C}(S,a,m) = \{x \in \mathbb{N} \mid aw(x \bmod m) \leqslant x\}$, where $\{w(0), w(1), \ldots, w(m-1)\}$ is the Apéry set of m in S, which is a numerical semigroup and that we call (a,m) - contraction of S. We study the Frobenius number and the singularity degree of $\mathrm{C}(S,a,m)$. We also characterize the contractions $\mathrm{C}(S,a,m)$ that are symmetric and pseudo-symmetric numerical semigroups. Finally we see that the contractions of $\mathbb{N}$ are solutions of modular Diophantine inequalities.

Introduction

A *numerical semigroup* S is a subset of $\mathbb{N}$ (the set of nonnegative integers) closed under addition, $0 \in S$ and so that $\mathbb{N} \setminus S$ has finitely many elements. The elements of $\mathrm{H}(S) = \mathbb{N} \setminus S$ are the *gaps* of S and its cardinality, denoted by $\#\mathrm{H}(S)$, is the *degree of singularity* of S, which has been widely studied in the literature (see for instance [2]). Another important invariant of S is the largest integer not belonging to S, known as the *Frobenius number* of S and denoted here by $\mathrm{g}(S)$ (see [2, 3, 6]). For $m \in S \setminus \{0\}$, the Apéry set of m in S is the set $\mathrm{Ap}(S,m) = \{s \in S \mid s-m \notin S\}$ (see [1]). It is well known and easy to check (see for instance [9]) that $\mathrm{Ap}(S,m) = \{w(0), w(1), \ldots, w(m-1)\}$, where $w(i)$ is the least element in S congruent with i modulo m.

Let S be a numerical semigroup, $m \in S \setminus \{0\}$ and a a positive integer. Write as above $\mathrm{Ap}(S,m) = \{w(0), w(1), \ldots, w(m-1)\}$. The (a,m) - *contraction of* S is the set

$$\mathrm{C}(S,a,m) = \{x \in \mathbb{N} \mid aw(x \bmod m) \leqslant x\},$$

where $x \bmod m$ denotes the remainder of the division of x by m. In Section 1., we prove that $\mathrm{C}(S,a,m)$ is a numerical semigroup contained in S. The main result in this section gives a formula relating the degrees of singularity of S and $\mathrm{C}(S,a,m)$. In Section 2., we present a similar result for the Frobenius number of $\mathrm{C}(S,a,m)$.

A numerical semigroup is *irreducible* if it cannot be expressed as an intersection of two numerical semigroups properly containing it. A numerical semigroup is irreducible if and only it is either symmetric or pseudo-symmetric, depending on the parity of

Mathematics subject classification (2000): 20M14, 13H1.

Key words and phrases: Numerical semigroup, symmetric, pseudo-symmetric, modular Diophantine inequality, Frobenius number, singularity degree.

The author is supported by the project MTM2004-01446 and FEDER founds and wants to thank P. A. García-Sánchez, P. Vasco and the referee for their comments and suggestions.

Paper JMI-01-41

its Frobenius number (see [8]). These two kinds of numerical semigroups have been widely studied in the literature due to their connections with Commutative Algebra and Algebraic Geometry (see [2] and the references given there).

From the results obtained in the preceding sections, in Section 3. we characterize those numerical semigroups whose contractions yield irreducible numerical semigroups.

A *modular Diophantine inequality* is an expression of the form $ax \bmod b \leqslant x$ where a and b are positive integers. In [10] it is shown that the set $\mathrm{M}(a,b)$ of integer solutions of the above inequality is a numerical semigroup. At the beginning of Section 4. we point out that $\mathrm{C}(\mathbb{N},a,m) = \mathrm{M}(a,am)$. This allows us to compare the results appearing in [10] and the ones obtained in the present paper for (a,m) - contractions of $\mathbb{N}$.

1. The degree of singularity

In this section, and unless otherwise stated, S is a numerical semigroup, m is a nonzero element of S and a is a positive integer. We write as usual $\mathrm{Ap}(S,m) = \{w(0) = 0, w(1), \ldots, w(m-1)\}$ and define the (a,m) - contraction of S as $\mathrm{C}(S,a,m) = \{x \in \mathbb{N} \mid aw(x \bmod m) \leqslant x\}$.

The next result follows from [9, Proposition 10.5]. It states the relationship between the elements in $\mathrm{Ap}(S,m)$ and shows that the membership problem to S is trivial once we know the elements of $\mathrm{Ap}(S,m)$.

LEMMA 1. *Let $x \in \mathbb{N}$. Then $x \in S$ if and only if $w(x \bmod m) \leqslant x$. Moreover, if $i,j \in \{0,1,\ldots,m-1\}$, then $w(i) + w(j) \geqslant w((i+j) \bmod m)$.*

An integer x belongs to S if and only if $w(x \bmod m) \leqslant x$, and belongs to $\mathrm{C}(S,a,m)$ if and only if $aw(x \bmod m) \leqslant x$. This is why we have chosen the name contraction for $\mathrm{C}(S,a,m)$.

With the above lemma is now easy to prove that $\mathrm{C}(S,a,m)$ is a numerical semigroup.

PROPOSITION 1. *$\mathrm{C}(S,a,m)$ is a numerical semigroup contained in S and $m \in \mathrm{C}(S,a,m)$. Moreover, if $a \geqslant 2$, then m is the least positive integer belonging to $\mathrm{C}(S,a,m)$.*

Proof. If $x,y \in \mathrm{C}(S,a,m)$, then $aw(x \bmod m) \leqslant x$ and $aw(y \bmod m) \leqslant y$. By Lemma 1, we have that $aw((x+y) \bmod m) \leqslant a(w(x \bmod m) + w(y \bmod m))$, and consequently $aw((x+y) \bmod m) \leqslant x+y$. Hence $x+y \in \mathrm{C}(S,a,m)$. Besides, observe that if $x \in \mathbb{N}$ and $x \geqslant a(\max\{w(1),\ldots,w(m-1)\})$, then $x \in \mathrm{C}(S,a,m)$, which implies that $\mathbb{N} \setminus \mathrm{C}(S,a,m)$ has finitely many elements. Clearly, $0, m \in \mathrm{C}(S,a,m)$. Thus $\mathrm{C}(S,a,m)$ is a numerical semigroup containing m. Note that since $w(x \bmod m) \leqslant aw(x \bmod m)$, by using Lemma 1, we deduce that $\mathrm{C}(S,a,m) \subseteq S$.

Assume that $a \geqslant 2$ and that $x \in \{1,\ldots,m-1\}$. Then $x = x \bmod m \leqslant w(x \bmod m) < aw(x \bmod m)$ and thus $x \notin \mathrm{C}(S,a,m)$. □

The least positive integer belonging to a numerical semigroup M is its multiplicity and is denoted by $\mathrm{m}(M)$. In view of Proposition 1, if $a \geqslant 2$, then $\mathrm{m}(\mathrm{C}(S,a,m)) = m$.

As $m \in \mathrm{C}(S,a,m)$, we can take into account the Apéry set of m in $\mathrm{C}(S,a,m)$. Along this section we write $\mathrm{Ap}(\mathrm{C}(S,a,m),m) = \{\overline{w}(0),\overline{w}(1),\ldots,\overline{w}(m-1)\}$. The following result can be easily proved.

LEMMA 2. *If $i \in \{0,1,\ldots,m-1\}$, then $\overline{w}(i)$ is the least integer congruent with i modulo m greater than or equal to $aw(i)$.*

With this we can explicitly describe the set $\mathrm{Ap}(\mathrm{C}(S,a,m),m)$.

PROPOSITION 2. *For $i \in \{0,1,\ldots,m-1\}$, $\overline{w}(i) = aw(i) + (1-a)i \bmod m$.*

Proof. As $0 \leqslant (1-a)i \bmod m < m$, in view of Lemma 2, it suffices to show that $aw(i) + (1-a)i \bmod m$ is congruent with i modulo m. This is easy to prove. □

The degree of singularity of a numerical semigroup can be computed from the Apéry set of any of its nonzero elements as the next result appearing in [12] points out.

LEMMA 3. *Let M be a numerical semigroup and let $m \in M \setminus \{0\}$. Then*

$$\#\mathrm{H}(M) = \frac{1}{m}\left(\sum_{w \in \mathrm{Ap}(M,m)} w\right) - \frac{m-1}{2}.$$

Hence in view of Proposition 2, we must be able to compute a sum of the form $\sum_{i=1}^{m-1}(1-a)i \bmod m$. This is accomplished in the next result that appears in [4] and whose easy prove we include here.

LEMMA 4. *Let α be an integer, β be a positive integer, and $\gamma = \gcd\{\alpha,\beta\}$ (where* gcd *stands for greatest common divisor). Then*

$$\sum_{i=0}^{\beta-1} \alpha i \bmod \beta = \frac{\beta(\beta-\gamma)}{2}.$$

Proof. Observe that

$$\sum_{i=0}^{\beta-1} \alpha i \bmod \beta = \gamma \sum_{i=0}^{\beta-1} \frac{\alpha}{\gamma} i \bmod \frac{\beta}{\gamma} = \gamma^2 \sum_{i=0}^{\frac{\beta}{\gamma}-1} i = \gamma^2 \frac{\frac{\beta}{\gamma}\left(\frac{\beta}{\gamma}-1\right)}{2} = \frac{\beta(\beta-\gamma)}{2}.$$

□

Thus, we are now able to relate the degrees of singularity of S and $\mathrm{C}(S,a,m)$.

THEOREM 1. *Let S be a numerical semigroup and $m \in S \setminus \{0\}$. For a positive integer a we have*

$$\#\mathrm{H}(\mathrm{C}(S,a,m)) = a\#\mathrm{H}(S) + \frac{a(m-1)+1-\gcd\{a-1,m\}}{2}.$$

Proof. In view of Lemma 3,

$$\#\mathrm{H}(\mathrm{C}(S,a,m)) = \frac{\overline{w}(0)+\overline{w}(1)+\cdots+\overline{w}(m-1)}{m} - \frac{m-1}{2}.$$

From Proposition 2, we deduce that

$$\#\mathrm{H}(\mathrm{C}(S,a,m)) = a\frac{w(0)+w(1)+\cdots+w(m-1)}{m} - a\frac{m-1}{2} - (1-a)\frac{m-1}{2} + \frac{1}{m}\sum_{i=0}^{m-1}(1-a)i \bmod m.$$

By Lemma 3 (now for S) and Lemma 4, we obtain

$$\#\mathrm{H}(\mathrm{C}(S,a,m)) = a\#\mathrm{H}(S) - (1-a)\frac{m-1}{2} + \frac{1}{m}\frac{m(m-\gcd\{a-1,m\})}{2}.$$

By simplifying, we get the desired formula. □

We illustrate the results appearing in this section with an example. If $n_1,\ldots,n_p \in \mathbb{N}$, we denote by $\langle n_1,\ldots,n_p\rangle$ the numerical semigroup generated by $\{n_1,\ldots,n_p\}$, that is, the set $\{\lambda_1 n_1+\cdots+\lambda_p n_p \mid \lambda_1,\ldots,\lambda_p \in \mathbb{N}\}$. From Lemma 1, one easily deduces that $S = \langle \mathrm{Ap}(S,m)\cup\{m\}\rangle$.

EXAMPLE 1. Let $S=\langle 4,5\rangle$. Then $\mathrm{Ap}(S,4)=\{w(0)=0,w(1)=5,w(2)=10,w(3)=15\}$. By applying Proposition 2, we obtain that $\mathrm{Ap}(\mathrm{C}(S,2,4),4)=\{0,13,22,31\}$. Hence $\mathrm{C}(S,2,4)=\langle 4,13,22,31\rangle$. By using Lemma 3, we have that $\#\mathrm{H}(S)=6$ and $\#\mathrm{H}(\mathrm{C}(S,2,4))=15$, which coincides with the result obtained from Theorem 1.

2. The Frobenius number

As in the preceding section, S is a numerical semigroup, m is a nonzero element of S and a is a positive integer. We also assume that

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

and

$$\mathrm{Ap}(\mathrm{C}(S,a,m),m)=\{\overline{w}(0),\overline{w}(1),\ldots,\overline{w}(m-1)\}.$$

For $i\in\{0,\ldots,m-1\}$ there exists $k_i,\overline{k}_i\in\mathbb{N}$ such that $w(i)=k_i m+i$ and $\overline{w}(i)=\overline{k}_i m+i$.

Observe that both S and $\mathrm{C}(S,a,m)$ are determined by the k_i's and the $\overline{k}_i$'s, respectively. Thus it is interesting to describe the relationship between them, as we did for $w(i)$ and $\overline{w}(i)$.

Let q be a rational number. Denote by $\lfloor q\rfloor$ (respectively $\lceil q\rceil$) the greatest integer less than (respectively smallest integer greater than) or equal to q.

LEMMA 5. *For* $i\in\{0,1,\ldots,m-1\}$, $\overline{k}_i = ak_i + \left\lceil \frac{(a-1)i}{m}\right\rceil$.

Proof. Let $k\in\mathbb{N}$. As $km+i \geqslant a(k_i m+i)$ if and only if $k\geqslant ak_i+\frac{(a-1)i}{m}$, the result follows from Lemma 2. □

As occurred with the degree of singularity, the Frobenius number of a numerical semigroup is also easily determined once we know the Apéry set of any of its nonzero elements. This is a well known result (and easy to prove) that can be found for instance in [9].

LEMMA 6. *Let M be a numerical semigroup and let m be a nonzero element of M. Then*

$$\mathrm{g}(M) = \max \mathrm{Ap}(M, m) - m.$$

Since we already know the relationship between $w(i)$ and $\overline{w}(i)$, as well as the one existing between k_i and $\overline{k}_i$, we can try to see how $\mathrm{g}(S)$ and $\mathrm{g}(\mathrm{C}(S, a, m))$ are related.

THEOREM 2. *Let S be a numerical semigroup and $m \in S \setminus \{0\}$. For a positive integer a we have*

$$\mathrm{g}(\mathrm{C}(S, a, m)) = \begin{cases} a\mathrm{g}(S) + (a-1)m & \text{if } (a-1)\mathrm{g}(S) \bmod m = 0, \\ a\mathrm{g}(S) + am - ((a-1)\mathrm{g}(S) \bmod m) & \text{otherwise.} \end{cases}$$

Proof. Let $g = \mathrm{g}(S)$ and $r = g \bmod m$. We see that $\overline{k}_r m + r = \max \mathrm{Ap}(\mathrm{C}(S, a, m), m)$. Thus, we must show that for $i \in \{0, 1, \ldots, m-1\}$, the inequality $\overline{k}_i m + i \leqslant \overline{k}_r m + r$ holds. In view of Lemma 5, we must prove that $(ak_i + \left\lceil \frac{(a-1)i}{m} \right\rceil)m + i \leqslant (ak_r + \left\lceil \frac{(a-1)r}{m} \right\rceil)m + r$. From Lemma 6, we know that $g + m = k_r m + r$ and that $k_i m + i \leqslant k_r m + r$. Hence $k_i \leqslant k_r$. We distinguish two cases.

- If $k_i < k_r$, then $(ak_i + \left\lceil \frac{(a-1)i}{m} \right\rceil)m + i = ak_i m + \left\lceil \frac{(a-1)i}{m} \right\rceil m + i \leqslant ak_i m + (a-1)m + i$, since $\left\lceil \frac{(a-1)i}{m} \right\rceil \leqslant \left\lceil \frac{(a-1)(m-1)}{m} \right\rceil = \left\lceil a - 1 - \frac{a-1}{m} \right\rceil \leqslant a - 1$. As $ak_i m + (a-1)m + i \leqslant a(k_i + 1)m$, we deduce that $(ak_i + \left\lceil \frac{(a-1)i}{m} \right\rceil)m + i \leqslant a(k_i + 1)m \leqslant ak_r m \leqslant (ak_r + \left\lceil \frac{(a-1)r}{m} \right\rceil)m + r$.
- If $k_i = k_r$, then as $k_i m + i \leqslant k_r m + r$, we have that $i \leqslant r$.. Hence $(ak_i + \left\lceil \frac{(a-1)i}{m} \right\rceil)m + i \leqslant (ak_r + \left\lceil \frac{(a-1)r}{m} \right\rceil)m + r$.

The rest of the proof follows from Lemma 6, by taking into account that if $(a-1)r \bmod m \neq 0$, then $\left\lceil \frac{(a-1)r}{m} \right\rceil = \left\lfloor \frac{(a-1)r}{m} \right\rfloor + 1$ and that $(a-1)r = \lfloor \frac{(a-1)r}{m} \rfloor m + (a-1)r \bmod m$. □

We illustrate these result with several examples.

EXAMPLE 2. Let $S = \langle 4, 5 \rangle$ be as in Example 1. Then $\mathrm{g}(S) = 11$. By taking $a = 2$ and $m = 4$, we obtain that $(a-1)11 \bmod m = 3$. Theorem 2 is telling us that $\mathrm{g}(\mathrm{C}(S, 2, 4)) = 27$.

EXAMPLE 3. For $S = \mathbb{N}$, $\#\mathrm{H}(S) = 0$ and $\mathrm{g}(S) = -1$. Hence for m and a positive integers, we obtain in view of Theorems 1 and 2 that

$$\#\mathrm{H}(\mathrm{C}(\mathbb{N}, a, m)) = \frac{a(m-1) + 1 - \gcd\{a-1, m\}}{2},$$

and

$$\mathrm{g}(\mathrm{C}(\mathbb{N}, a, m)) = \begin{cases} (a-1)m - a & \text{if } (1-a) \bmod m = 0, \\ am - a - (1-a) \bmod m & \text{otherwise.} \end{cases}$$

EXAMPLE 4. Let $b \in \mathbb{N} \setminus \{0,1\}$. If $S = \{0, b, \rightarrow\}$ (the symbol $\rightarrow$ means that all the integers greater than b are also in the set), and a, m are positive integers such that $m \geqslant b$, then $\#\mathrm{H}(S) = \mathrm{g}(S) = b - 1$. By Theorems 1 and 2, we have that

$$\#\mathrm{H}(\mathrm{C}(\{0, b, \rightarrow\}, a, m)) = a(b-1) + \frac{a(m-1) + 1 - \gcd\{a-1, m\}}{2}$$

and

$$\mathrm{g}(\mathrm{C}(\{0, b, \rightarrow\}, a, m)) = \begin{cases} a(b-1) + (a-1)m, & \text{if } (a-1)(b-1) \bmod m = 0, \\ a(b-1) + am - (a-1)(b-1) \bmod m, & \text{otherwise.} \end{cases}$$

EXAMPLE 5. Let s and t be two coprime integers greater than or equal to two. Then $\#\mathrm{H}(\langle s, t\rangle) = \dfrac{(s-1)(t-1)}{2}$ and $\mathrm{g}(\langle s, t\rangle) = (s-1)(t-1) - 1$ (see [14, 13]). Hence, by Theorems 1 and 2, we get

$$\#\mathrm{H}(\mathrm{C}(\langle s, t\rangle, a, m)) = a\frac{(s-1)(t-1)}{2} + \frac{a(m-1) + 1 - \gcd\{a-1, m\}}{2}$$

and

$$\mathrm{g}(\mathrm{C}(\langle s, t\rangle, a, m)) = \begin{cases} a((s-1)(t-1) - 1) + (a-1)m, \\ \quad \text{if } (a-1)((s-1)(t-1) - 1) \bmod m = 0, \\ a((s-1)(t-1)-1) + am - (a-1)((s-1)(t-1)-1) \bmod m, \\ \quad \text{otherwise.} \end{cases}$$

These examples can be used to construct numerical semigroups with given multiplicity, Frobenius number and degree of singularity, and thus coordinate rings of curves with these properties (see [2] for the correspondence between these concepts in numerical semigroups and in one-dimensional unramified local domains).

3. Irreducible contractions

It is well known (see for instance [2, 5]) that if S is a numerical semigroup, then $2\#\mathrm{H}(S) \geqslant \mathrm{g}(S) + 1$. We say that a numerical semigroup is *symmetric* (respectively *pseudo-symmetric*) if $2\#\mathrm{H}(S) = \mathrm{g}(S) + 1$ (respectively $2\#\mathrm{H}(S) = \mathrm{g}(S) + 2$). Hence, symmetric (respectively pseudo-symmetric) numerical semigroups are those irreducible numerical semigroups with odd (respectively even) Frobenius number.

As in the preceding sections, assume that S is a numerical semigroup, $m \in S \setminus \{0\}$ and that a is a positive integer.

3.1. Symmetric contractions

PROPOSITION 3. *$\mathrm{C}(S, a, m)$ is symmetric if and only if S is symmetric and $\gcd\{a-1, m\} \in \{m, (a-1)\mathrm{g}(S) \bmod m\}$.*

Proof. Let $d = \gcd\{a-1, m\}$, $g = \mathrm{g}(S)$ and $h = \#\mathrm{H}(S)$. We know that $\mathrm{C}(S, a, m)$ is symmetric if and only if $2\#\mathrm{H}(\mathrm{C}(S, a, m)) = \mathrm{g}(\mathrm{C}(S, a, m)) + 1$. We distinguish two possibilities, depending on the cases we apply from Theorems 1 and 2.

- Assume that $(a-1)g \bmod m = 0$. Then by Theorems 1 and 2, we deduce that $\mathrm{C}(S,a,m)$ is symmetric if and only if $2ah+a(m-1)-d+1 = ag+(a-1)m+1$, or equivalently, $a(2h-g) = a+d-m$. As $2h-g \geqslant 1$ and $a+d-m \leqslant a$, this equality holds if and only if $2h-g=1$ and $d-m=0$. Thus, $\mathrm{C}(S,a,m)$ is symmetric if and only $d=m$ and S is symmetric.
- Assume now that $(a-1)g \bmod m \neq 0$. Then again by Theorems 1 and 2, we deduce that $\mathrm{C}(S,a,m)$ is symmetric if and only if $2ah+a(m-1)-d+1 = ag+am-((a-1)g \bmod m)+1$. This is equivalent to $a(2h-g) = a+d-((a-1)g \bmod m)$. Since $d \leqslant a-1$ and $(a-1)g \bmod m \geqslant 0$, we have that $a+d-((a-1)g \bmod m) \leqslant 2a-1$. Hence $a(2h-g) = a+d-((a-1)g \bmod m)$ if and only if $2h-g=1$ and $d-((a-1)g \bmod m) = 0$. Thus, $\mathrm{C}(S,a,m)$ is symmetric if and only $d = (a-1)g \bmod m$ and S is symmetric.

The proof now follows easily. □

By using this last proposition, from a given symmetric numerical semigroup, we can construct families with infinitely many elements of contractions of S that are again symmetric. The following two corollaries materialize two of these families.

COROLLARY 1. *If S is a symmetric numerical semigroup and $m \in S \setminus \{0\}$, then for every nonnegative integer k, the semigroup $\mathrm{C}(S, km+1, m)$ is also symmetric. Moreover, $\mathrm{g}(\mathrm{C}(S,km+1,m)) = (km+1)\mathrm{g}(S)+km^2$.*

COROLLARY 2. *Let S be a symmetric numerical semigroup with Frobenius number g. Let m and d be positive integers such that $dm \in S$ and $\gcd\{g,m\} = 1$. Let a be a positive integer such that $ag \bmod m = 1$. Then $\mathrm{C}(S, ad+1, md)$ is symmetric and $\mathrm{g}(\mathrm{C}(S,ad+1,md)) = (ad+1)(g+md)-d$.*

Proof. Observe that $\gcd\{g,m\} = 1$. Then the existence of a is guaranteed and $\gcd\{a,m\} = 1$. The result now follows from Proposition 3, by taking into account that $\gcd\{ad,md\} = d$ and that $adg \bmod md = d(ag \bmod m) = d$. The computation of $\mathrm{g}(\mathrm{C}(S,ad+1,md))$ is done by using Theorem 2. □

3.2. Pseudo-symmetric contractions

We proceed analogously for the pseudo-symmetric case, though the results obtained are not as the reader would probably expect.

PROPOSITION 4. *$\mathrm{C}(S,a,m)$ is pseudo-symmetric if and only if S is symmetric, $\gcd\{a-1,m\} = 1$ and $(a-1)\mathrm{g}(S) \bmod m = 2$.*

Proof. Let $d = \gcd\{a-1,m\}$, $g = \mathrm{g}(S)$ and $h = \#\mathrm{H}(S)$. We know that $\mathrm{C}(S,a,m)$ is pseudo-symmetric if and only if $2\#\mathrm{H}(\mathrm{C}(S,a,m)) = \mathrm{g}(\mathrm{C}(S,a,m))+2$. As above, we distinguish two possibilities, depending on the cases we apply from Theorems 1 and 2.

- We see that if $(a-1)g \bmod m = 0$, then $\mathrm{C}(S,a,m)$ is not pseudo-symmetric. Assume to the contrary that $\mathrm{C}(S,a,m)$ is pseudo-symmetric. Then in view of Theorems 1 and 2, we have that $2ah+a(m-1)-d+1 = ag+(a-1)m+2$.

Hence $a(2h-g) = a+d-m+1$. As $a+d-m+1 \leqslant 2a-1$, we have that $2h-g=1$ and $d-m+1=0$. Hence $m=d+1$ and since $d \mid m$, we have that $d=1$. This implies that $m=2$ and that $a-1$ is odd, because $d=1$. Observe also that as $2=m \in S$, then g must be odd. Then $(a-1)g \bmod 2 \neq 0$, contradicting the hypothesis.

- Assume now that $(a-1)g \bmod m \neq 0$. Then once more by Theorems 1 and 2, we deduce that $\mathrm{C}(S,a,m)$ is pseudo-symmetric if and only if $2ah + a(m-1) - d + 1 = ag + am - ((a-1)g \bmod m) + 2$. This is equivalent to $a(2h-g) = a+d-((a-1)g \bmod m)+1$. Since $a+d-((a-1)g \bmod m)+1 \leqslant a+a-1-1+1 = 2a-1$, $\mathrm{C}(S,a,m)$ is pseudo-symmetric if and only $2h-g=1$ and $d-((a-1)g \bmod m)+1=0$, or equivalently, S is symmetric and $(a-1)g \bmod m = d+1$. Note that since $d=\gcd\{a-1,m\}$, we have that $d \mid (a-1)g \bmod m$, whence $d|d+1$. This forces d to be 1.

□

With this proposition we can construct families of pseudo-symmetric numerical semigroups from a single symmetric numerical semigroup. One of these families is presented in the next corollary.

COROLLARY 3. *Let S be a symmetric numerical semigroup with Frobenius number g. Let $m \in S \setminus \{0\}$ be an odd integer such that $m \geqslant 3$ and $\gcd\{g,m\}=1$. Let a be a positive integer such that $ag \bmod m = 2$. Then $\mathrm{C}(S, a+1, m)$ is a pseudo-symmetric numerical semigroup with Frobenius number $(a+1)(g+m)-2$.*

Proof. The existence of a follows from the conditions $\gcd\{g,m\}=1$ and $m \geqslant 3$. As $ag \bmod m = 2$, $\gcd\{a,m\}|2$. Since m is odd, this implies that $\gcd\{a,m\}=1$. The proof now follows from Proposition 4 and Theorem 2. □

4. Contractions of $\mathbb{N}$ and modular numerical semigroups

Let a and b be positive integers. Denote by $\mathrm{M}(a,b)$ the set $\{x \in \mathbb{N} \mid ax \bmod b \leqslant x\}$. As we pointed out in the Introduction, $\mathrm{M}(a,b)$ is a numerical semigroup. A numerical semigroup is *modular* if it is of this form. There is a relationship between modular semigroups and contractions of $\mathbb{N}$ as the next result shows.

PROPOSITION 5. *Let a and m be positive integers. Then $\mathrm{C}(\mathbb{N},a,m) = \mathrm{M}(a,am)$.*

Proof. Clearly, $\mathrm{Ap}(\mathbb{N},m) = \{0,1,\ldots,m-1\}$. Hence $x \in \mathrm{C}(\mathbb{N},a,m)$ if and only if $a(x \bmod m) \leqslant x$, or equivalently, $ax \bmod am \leqslant x$. □

In Section 5 of [10] we studied numerical semigroups of the form $\mathrm{M}(a,ma)$. Thus some of the results appearing there can also be achieved from the tools introduced in this paper. Of course, some of the results presented in [10] can be used to obtain information for (a,m)- contractions of $\mathbb{N}$. The rest of this section is devoted to this exchange of information.

Given a and m positive integers, from [10, Theorem 44] one has the following description of the Apéry set of m in $\mathrm{M}(a, am)$

$$\mathrm{Ap}(\mathrm{M}(a,am),m) = \left\{ \left\lceil \frac{(a-1)i}{m} \right\rceil m + i \mid i \in \{0,\dots,m-1\} \right\}.$$

But this description is also an immediate consequence of Proposition 5 and Lemma 5.

By using Lemma 6 (as done in [10, Corollary 45]) one obtains a formula for the Frobenius number of $\mathrm{M}(a, am)$:

$$\mathrm{g}(\mathrm{M}(a,am)) = \left\lceil \frac{(a-1)(m-1)}{m} \right\rceil m - 1.$$

For a and b positive integers, [10, Theorem 12] states that

$$\#\mathrm{H}(\mathrm{M}(a,b)) = \frac{b+1-\gcd\{a,b\}-\gcd\{a-1,b\}}{2}.$$

Thus particularizing for $b = am$, we get that

$$\#\mathrm{H}(a,am) = \frac{am+1-a-\gcd\{a-1,m\}}{2}$$

as presented in Example 3.

Propositions 4 and 5 allow us to assert that there are numerical semigroups of the form $\mathrm{M}(a, ab)$ that are pseudo-symmetric. Thus, [10, Corollary 60] is false, as stated in [11]. Corollary 60 in [10] was deduced from the second part of [10, Proposition 58], and there is a mistake in that statement. The correct statement should be that "$\mathrm{M}(a, ab)$ is pseudo-symmetric if and only if $\gcd\{a-1,b\}+(a-1) \bmod b = b-1$" (and not $b+1$ as written originally). This lead to the erroneous conclusion given in [10, Corollary 60]. We reformulate [10, Proposition 58] with the language used in the preceding sections. We also include an alternative proof inspired in Propositions 3 and 4.

PROPOSITION 6. *Let a and m be positive integers. Then*

(1) $\mathrm{C}(\mathbb{N}, a, m)$ *is symmetric if and only if* $\gcd\{a-1,m\}+(a-1) \bmod m = m$,

(2) $\mathrm{C}(\mathbb{N}, a, m)$ *is pseudo-symmetric if and only if* $\gcd\{a-1,m\}+(a-1) \bmod m = m-1$.

Proof. Set $d = \gcd\{a-1,m\}$.

(1) In view of Proposition 3, it suffices to show that $d+(a-1) \bmod m = m$ if and only if $d \in \{m, (1-a) \bmod m\}$. Assume that $d+(a-1) \bmod m = m$. If $(a-1) \bmod m = 0$, then $d = m$. If to the contrary $(a-1) \bmod m \neq 0$, then $d = m-(a-1) \bmod m = (1-a) \bmod m$. Conversely, if $d = m$, then $(a-1) \bmod m = 0$ and thus $d+(a-1) \bmod m = m$. If $d = (1-a) \bmod m$, then $(a-1) \bmod m = m-d$ and $d+(a-1) \bmod m = m$.

(2) Proposition 4 asserts that we must prove that $d+(a-1) \bmod m = m-1$ if and only if $d = 1$ and $(1-a) \bmod m = 2$. As $d = \gcd\{a-1,m\}$, we have that $d \mid (a-1) \bmod m$. Hence if $d+(a-1) \bmod m = m-1$, we deduce that $d|m-1$. But then $d|m$ and $d|m-1$, which leads to $d = 1$. This implies that

$(a-1) \bmod m = m-2$, or equivalently, $(1-a) \bmod m = 2$.. Conversely, if $(1-a) \bmod m = 2$, then $(a-1) \bmod m = m-2$. If in addition $d = 1$, then we conclude that $d + (a-1) \bmod m = m-1$.

□

Every numerical semigroup has a unique minimal system of generators. The cardinality of this set is known as the *embedding dimension* of the numerical semigroup. In Section 5 of [10], the set of minimal generators of a numerical semigroup of the form $\mathrm{M}(a, am)$ is described (see Theorem 49 in that paper). By using this together with Proposition 5, we can obtain a description of the minimal generators of (a,m)-contractions of $\mathbb{N}$. As a consequence of [10, Corollary 53] we obtain the following lower bound for the embedding dimension of an (a,m)-contraction of $\mathbb{N}$, when $a \geqslant 3$.

COROLLARY 4. *Let a and m be positive integers with $a \geqslant 3$. Then the embedding dimension of $\mathrm{C}(\mathbb{N}, a, m)$ is greater than or equal to $\left\lfloor \frac{m}{a-1} \right\rfloor + 1$.*

For a numerical semigroup S, the set of pseudo-Frobenius numbers is defined as

$$\mathrm{T}(S) = \{x \in \mathbb{Z} \mid x + s \in S \text{ for all } s \in S \setminus \{0\}\},$$

where $\mathbb{Z}$ denotes as usual the set of integers. Its cardinality, $\mathrm{t}(S)$, is the *(Cohen-Macaulay) type* of S (this set and its cardinality have special relevance in the study of the semigroup ring associated to the numerical semigroup; see for instance [2]). The set of pseudo-Frobenius numbers of $\mathrm{M}(a, am)$ can be described by using Lemma 54 and Theorem 56 of [10], and thus in view of Proposition 5, we obtain a description of the pseudo-Frobenius numbers of the (a,m)-contractions of $\mathbb{N}$.

REFERENCES

[1] R. APÉRY, *Sur les branches superlinéaires des courbes algébriques*, C.R. Acad. Sci. Paris 222 (1946), 1198-1200.

[2] V. BARUCCI, D. E. DOBBS AND M. FONTANA, *Maximality Properties in Numerical Semigroups and Applications to One-Dimensional Analytically Irreducible Local Domains*, Memoirs of the Amer. Math. Soc. **598** (1997).

[3] A. BRAUER AND J. E. SCHOCKLEY, *On a problem of Frobenius*, J. Reine Angew. Math. **211** (1962), 215-220.

[4] M. DELGADO, J. C. ROSALES, *Modular Diophantine inequalities and rotations of numerical semigroups*, J. Australian Math. Soc. (to appear).

[5] R. FRÖBERG, G. GOTTLIEB AND R. HÄGGKVIST, *On numerical semigroups*, Semigroup Forum **35** (1987), 63-83.

[6] J. L. RAMÍREZ ALFONSÍN, *The diophantine Frobenius problem*, Oxford Univ. Press, 2005.

[7] J. C. ROSALES, *On symmetric numerical semigroups*, J. Algebra, **182** (1996) 422-434.

[8] J. C. ROSALES AND M. B. BRANCO, *Irreducible numerical semigroups*, Pacific J. Math. **209** (2003), 131-143.

[9] J. C. ROSALES AND P. A. GARCÍA-SÁNCHEZ, *Finitely generated commutative monoids*, Nova Science Publishers, New York, 1999.

[10] J. C. ROSALES, P. A. GARCÍA-SÁNCHEZ, J. M. URBANO-BLANCO, *Modular Diophantine inequalities and numerical semigroups*, Pacific J. Math. **218** (2005), 379-398.

[11] J. C. ROSALES, P. A. GARCÍA-SÁNCHEZ, J. M. URBANO-BLANCO, *Correction to "Modular Diophantine inequalities and numerical semigroups, Pacific J. Math.* **218** *(2005), 379-398"*, Pacific J. Math. **220** (2005),199.

[12] E. S. SELMER, *On a linear diophantine problem of Frobenius*, J. Reine Angew. Math. **293/294** (1977), 1-17.
[13] J. J. SYLVESTER, *Excursus on rational fractions and partitions*, Amer. J. Math. **5** (1882), 119-136.
[14] J. J. SYLVESTER, *Mathematical questions with their solutions*, Educational Times **41** (1884), 21.

(Received April 1, 2007)

J. C. Rosales
Departamento de Álgebra
Universidad de Granada
E-18071 Granada
Spain
e-mail: jrosales@ugr.es