MODULAR DIOPHANTINE INEQUALITIES AND ROTATIONS OF NUMERICAL SEMIGROUPS

M. DELGADO AND J. C. ROSALES

Introduction

Given two non negative integers a and b, with $b \neq 0$, we denote by $a \bmod b$ the remainder of the division of a by b. A *modular Diophantine inequality* (see [6]) is an expression of the form $ax \bmod b \leq x$. The set $\mathrm{M}(a, b)$ of the integer solutions of this inequality is a numerical semigroup, that is, a subset of the set $\mathbb{N}$ of the non negative integers that is closed under addition, contains 0 and whose complement in $\mathbb{N}$ is finite. Not all numerical semigroups can be described by an inequality of this form. We say that a numerical semigroup S is *modular* with *modulus* b and *factor* a if $S = \{x \in \mathbb{N} \mid ax \bmod b \leq x\}$.

When S is a numerical semigroup, we denote the finite set $\mathbb{N} \setminus S$ by $\mathrm{H}(S)$. The elements of $\mathrm{H}(S)$ are called the *gaps* of S, and its cardinality, denoted $\#\mathrm{H}(S)$, is an important invariant of the semigroup which is called the *singularity degree* of S (see [2]). Another important invariant of S is the greatest integer that does not belong to S, which is called the *Frobenius number* of S and it is denoted by $\mathrm{g}(S)$ (see [3]). Given $m \in S \setminus \{0\}$, the *Apéry set* (so called due to Apéry's paper [1]) of S with respect to m is defined by $\mathrm{Ap}(S, m) = \{s \in S \mid S - m \notin S\}$. It is well-known and easy to prove (see, for instance, [4]) that $\mathrm{Ap}(S, m) = \{w(0), w(1), \ldots, w(m-1)\}$ where $w(i)$ is the least element in S that is congruent with i modulo m. The set $\mathrm{Ap}(S, m)$ completely determines the semigroup S, since $S = \langle \mathrm{Ap}(S, m) \cup \{m\} \rangle$ (where by $\langle A \rangle$ we denote the submonoid of $(\mathbb{N}, +)$ generated by A, that is, the set of non negative integer linear combinations of elements of A). Besides that, $\mathrm{Ap}(S, m)$ contains, in general, much more information than an arbitrary system of generators of S; in particular the Frobenius number and the singularity degree can be easily computed from $\mathrm{Ap}(S, m)$.

In the first section we will give an explicit form of the set $\mathrm{Ap}(\mathrm{M}(a, b), b)$. As a consequence we obtain formulas for $\mathrm{g}(\mathrm{M}(a, b))$ and $\#\mathrm{H}(\mathrm{M}(a, b))$. Note that the formula we give for $\#\mathrm{H}(\mathrm{M}(a, b))$ was already obtained in [6]; we offer here an alternative proof.

The first author gratefully acknowledges support of FCT through the CMUP. He also acknowledges the hospitality of the Algebra Department of the University of Granada in which he was able to work bennifiting from a sabbatical grant of FCT.

The second author is supported by the project MTM2004-01446 and FEDER founds.

Both authors want to thank P. A. García-Sánchez for his usefull comments and suggestions.

In the second section we introduce the concept of rotation of a numerical semigroup and see how it is related with modular numerical semigroups. More precisely, if S is a numerical semigroup, $m \in S\setminus\{0\}$, $\mathrm{Ap}(S,m) = \{w(0), w(1), \ldots, w(m-1)\}$ and a is a positive integer, then we define the *(a,m)-rotation* of S as $\mathrm{R}(S,a,m) = \{x \in \mathbb{N} \mid w(ax \bmod m) \leq x\}$. We will see that $\mathrm{R}(S,a,m)$ is a numerical semigroup that contains m and is contained in $\mathrm{M}(a,m)$. Furthermore we will prove that $\mathrm{R}(S,a,m) = \mathrm{M}(a,m)$ if and only if $(a,m) \in S$, where (x,y) denotes the greatest common divisor of the integers x and y. In particular, we obtain that $\mathrm{M}(a,b) = \mathrm{R}(\mathbb{N},a,b)$ to any positive integers a and b.

If S is a numerical semigroup and d is a positive integer, then $\frac{S}{d} = \{x \in \mathbb{N} \mid dx \in \mathrm{S}\}$ is a numerical semigroup which clearly contains S (see [5]). Such a semigroup will be called the *quotient* of S by d.

In Section 3 we will see how to construct $\mathrm{Ap}(\mathrm{R}(S,a,m),m)$ from $\mathrm{Ap}(S,m)$. This will allow us to give formulas or bounds for the Frobenius number and the singularity degree of $\mathrm{R}(S,a,m)$ in terms of the Frobenius number and the singularity degree of a quotient of S in Section 5.

In Section 4 we show that when d is a positive divisor of m the set $\mathrm{Ap}\left(\frac{S}{d}, \frac{m}{d}\right)$ is obtained dividing by d the elements of $\mathrm{Ap}(S,m)$ that are multiples of d. This will allow us, in Section 5, to prove that if $(a,m) = d$, then $\#\mathrm{H}(\mathrm{R}(S,a,m)) = d\,\#\mathrm{H}\left(\frac{S}{d}\right) + \frac{m+1-d-(a-1,m)}{2}$ and that $d\mathrm{g}\left(\frac{S}{d}\right) + (d-1)\frac{m}{d} \leq \mathrm{g}(\mathrm{R}(S,a,m)) \leq d\mathrm{g}\left(\frac{S}{d}\right) + m - 1$. Notice that when a and b are coprime, as $\frac{S}{1} = S$, these results relate the invariants of S under study with the corresponding invariants of $\mathrm{R}(S,a,m)$.

Throughout this paper, and unless otherwise stated, S is a numerical semigroup and a, d and m are positive integers, with $m \in S \setminus \{0\}$ and $d = (a,m)$. Furthermore we will write $\mathrm{Ap}(S,m) = \{w(0), w(1), \ldots, w(m-1)\}$. As Proposition 10 states that $\mathrm{R}(S,a,m)$ is a numerical semigroup containing m, we will already announce the notation that will be used: $\mathrm{Ap}(\mathrm{R}(S,a,m),m) = \{\overline{w}(0), \overline{w}(1), \ldots, \overline{w}(m-1)\}$. For clarity, in the statments of many of our results we recall the notations fixed here.

1. Modular numerical semigroups

Recall that given two non negative integers a and b, with $b \neq 0$, the set $\mathrm{M}(a,b)$ of integer solutions of an inequality of the form $ax \bmod b \leq x$ is a numerical semigroup, which is said to be *modular*. Recall also that if S is a numerical semigroup and $m \in S \setminus \{0\}$, then the Apéry set of S with respect to m is $\mathrm{Ap}(S,m) = \{w(0), w(1), \ldots, w(m-1)\}$, where $w(i)$ is the least element in S that is congruent with i modulo m.

The proof of the following result is immediate.

Lemma 1. *Let a and b be positive integers. If $i \in \{0,1,\ldots,b-1\}$, then*

$$(b+1-a)i \bmod b = \begin{cases} i - (ai \bmod b) & \text{if} \quad ai \bmod b \leq i, \\ i - (ai \bmod b) + b & \text{if} \quad ai \bmod b > i. \end{cases}$$

It is clear that $b \in \mathrm{M}(a,b)$ and, in addition, that every integer greater than b also belongs to $\mathrm{M}(a,b)$.

Proposition 2. *Let a and b be positive integers. Then*

$$\mathrm{Ap}(\mathrm{M}(a,b),b) = \{(ai \bmod b) + (b+1-a)i \bmod b \mid i = 0,1,\ldots,b-1\}.$$

Proof. By Lemma 1 we know that

$$(ai \bmod b) + (b+1-a)i \bmod b = \begin{cases} i & \text{if} \quad ai \bmod b \le i, \\ i+b & \text{if} \quad ai \bmod b > i. \end{cases}$$

Thus

$$(ai \bmod b) + (b+1-a)i \bmod b = \begin{cases} i & \text{if} \quad i \in \mathrm{M}(a,b), \\ i+b & \text{if} \quad i \notin \mathrm{M}(a,b). \end{cases}$$

The proof of the proposition now follows easily from the definition of the Apéry set. □

Recall that if S is a numerical semigroup, then $\#\mathrm{H}(S)$ and $\mathrm{g}(S)$ denote the singularity degree and the Frobenius number of S, respectively.

The following result is well-known and easy to prove.

Lemma 3. *If S is a numerical semigroup and $m \in S \setminus \{0\}$, then*

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

As an immediate consequence of Proposition 2, we get this result.

Corollary 4. *Let a and b be positive integers. Then*

$$\mathrm{g}(\mathrm{M}(a,b)) = \max\{(ai \bmod b) + (b+1-a)i \bmod b \mid i = 0,1,\ldots,b-1\} - b.$$

The next result appears in [7] and shows how to compute the singularity degree of a numerical semigroup, once the Apéry set with respect to any of its non-zero elements is known.

Lemma 5. *Let S be a numerical semigroup and* $\mathrm{Ap}(S,m) = \{w(0), w(1), \ldots, w(m-1)\}$, *where $m \in S \setminus \{0\}$. Then*

$$\#\mathrm{H}(S) = \frac{1}{m}\left(w(1) + \cdots + w(m-1)\right) - \frac{m-1}{2}.$$

A usefull reformulation of this lemma is the following:

Lemma 6. *If* $\mathrm{Ap}(S,m) = \{0, k_1 m + 1, \ldots, k_{m-1} m + (m-1)\}$, *then*

$$\#\mathrm{H}(S) = k_1 + k_2 + \cdots + k_{m-1}.$$

Recall that we are aiming to give a formula for $\#\mathrm{H}(\mathrm{M}(a,b))$. In view of the formula given by Lemma 5 and due to the way Proposition 2 allows us to express the elements of $\mathrm{Ap}(\mathrm{M}(a,b),b)$, an important step is the observation contained in the following lemma. It provides a way to calculate the value of expressions of the form $\sum_{i=1}^{b-1} ai \bmod b$.

Lemma 7. *If a and b are positive integers and $d = (a,b)$, then*

$$\sum_{i=1}^{b-1} ai \bmod b = \frac{b(b-d)}{2}.$$

Proof. Clearly

$$\sum_{i=1}^{b-1} ai \bmod b = d\sum_{i=1}^{b-1} \frac{a}{d} i \bmod \frac{b}{d} = d^2 \sum_{i=1}^{\frac{b}{d}-1} i = d^2 \frac{\frac{b}{d}\left(\frac{b}{d}-1\right)}{2} = \frac{b(b-d)}{2}.$$

□

Now we exhibit a formula for #H(M(a,b)), which already appeared in [6, Theorem 12].

Proposition 8. *Let a and b be positive integers. Then*

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

Proof. By Proposition 2 and Lemma 5 we know that

$$\#\mathrm{H}(\mathrm{M}(a,b)) = \frac{1}{b}\left(\sum_{i=1}^{b-1} ai \bmod b + \sum_{i=1}^{b-1}(b+1-a)i \bmod b\right) - \frac{b-1}{2}.$$

By Lemma 7 we have that

$$\sum_{i=1}^{b-1} ai \bmod b = \frac{b(b-(a,b))}{2}$$

and

$$\sum_{i=1}^{b-1}(b+1-a)i \bmod b = \frac{b(b-(b+1-a,b))}{2} = \frac{b(b-(a-1,b))}{2}.$$

Thus

$$\begin{aligned}\#\mathrm{H}(\mathrm{M}(a,b)) &= \frac{1}{b}\left(\frac{b(b-(a,b))}{2} + \frac{b(b-(a-1,b))}{2}\right) - \frac{b-1}{2}\\ &= \frac{b-(a,b)}{2} + \frac{b-(a-1,b)}{2} - \frac{b-1}{2}\\ &= \frac{b+1-(a,b)-(a-1,b)}{2}.\end{aligned}$$

□

2. Rotations and modular semigroups

Recall that we use the notation $\mathrm{R}(S,a,m) = \{x \in \mathbb{N} \mid w(ax \bmod m) \leq x\}$ and say that $\mathrm{R}(S,a,m)$ is an (a,m)-*rotation* of S. The main result of this section, Theorem 17, shows that $(a,m) \in S$ if and only if $\mathrm{R}(S,a,m) = \mathrm{M}(a,m)$.

The following result can be easily deduced from [4, Proposition 10.5]. It plays an important role in the proofs of Proposition 10 and Lemma14.

Lemma 9. *Let $x \in \mathbb{N}$. Then $x \in$ S if and only if $w(x \bmod m) \leq x$. Furthermore, if $i, j \in \{0,1,\ldots,m-1\}$, then $w(i)+w(j) \geq w((i+j) \bmod m)$.*

Proposition 10. $\mathrm{R}(S,a,m)$ *is a numerical semigroup containing m.*

Proof. As $0 = w(0) = w(am \bmod m) \leq m$, we have that $0, m \in \mathrm{R}(S, a, m)$. Let $x, y \in \mathrm{R}(S, a, m)$. Then $w(ax \bmod m) \leq x$ and $w(ay \bmod m) \leq y$. By applying the preceding lemma, we have that $w(a(x+y) \bmod m) \leq w(ax \bmod m) + w(ay \bmod m) \leq x + y$, and therefore $x + y \in \mathrm{R}(S, a, m)$. Let $\alpha = \max\{w(0), w(1), \dots, w(m-1)\}$. Clearly if x is an integer such that $x \geq \alpha$, then $x \in \mathrm{R}(S, a, m)$. Thus $\mathbb{N} \setminus \mathrm{R}(S, a, m)$ is finite and consequently $\mathrm{R}(S, a, m)$ is a numerical semigroup. □

Now we can fix the notation $\mathrm{Ap}(\mathrm{R}(S, a, m), m) = \{\overline{w}(0), \overline{w}(1), \dots, \overline{w}(m-1)\}$ already announced.

When $(a, m) \in S$ the following lemma guarantees that if $i \in \{0, 1, \dots, m-1\}$ is a multiple of (a, m), then $w(i)$ is not greater that $m - 1$. As a consequence we will be able to prove a part of the main result of this section.

Lemma 11. *If* $(a, m) = d \in S$ *and* $w(i) = k_i m + i$ *for all* $i \in \{0, 1, \dots, m-1\}$, *then* $k_d = k_{2d} = \cdots = k_{(\frac{m}{d}-1)d} = 0$.

Proof. As $d \in S$ we have that $\left\{d, 2d, \dots, \left(\frac{m}{d} - 1\right)d\right\} \subseteq S$. From $\left(\frac{m}{d} - 1\right)d < m$, it follows that $id - m \notin S$ for all $i \in \left\{1, 2, \dots, \frac{m}{d} - 1\right\}$. Thus $\left\{d, 2d, \dots, \left(\frac{m}{d} - 1\right)d\right\} \subseteq \mathrm{Ap}(S, m)$. Hence $w(id) = id$ for all $i \in \left\{1, \dots, \frac{m}{d} - 1\right\}$ and consequently $k_{id} = 0$. □

Proposition 12. *If* $(a, m) = d \in S$, *then* $\mathrm{R}(S, a, m) = \mathrm{M}(a, m)$.

Proof. Recall that $x \in \mathrm{R}(S, a, m)$ if and only if $w(ax \bmod m) \leq x$. Let us suppose again that $w(i) = k_i m + i$ for all $i \in \{0, 1, \dots, m-1\}$. As $w(ax \bmod m) = w\left(d\left(\frac{a}{d}x \bmod \frac{m}{d}\right)\right)$ and $w(ax \bmod m) = k_{d(\frac{a}{d}x \bmod \frac{m}{d})} m + ax \bmod m$, by applying Lemma 11, we have that $w(ax \bmod m) = ax \bmod m$. Thus $x \in \mathrm{R}(S, a, m)$ if and only if $ax \bmod m \leq x$. This proves that $\mathrm{R}(S, a, m) = \mathrm{M}(a, m)$. □

Since (a, m) always belongs to $\mathbb{N}$, the previous proposition has as an immediate consequence that the set of all modular numerical semigroups coincides with the set of all rotations of $\mathbb{N}$, as is stated in the following corollary.

Corollary 13. *Let* a *and* b *be positive integers. Then* $\mathrm{M}(a, b) = \mathrm{R}(\mathbb{N}, a, b)$.

From Lemma 9 one may deduce easily the following result.

Lemma 14. *Let* S *and* T *be numerical semigroups containing the positive integer* m. *Let* $\mathrm{Ap}(S, m) = \{w(0), w(1), \dots, w(m-1)\}$ *and* $\mathrm{Ap}(T, m) = \{\tilde{w}(0), \tilde{w}(1), \dots, \tilde{w}(m-1)\}$. *Then* $S \subseteq T$ *if and only if* $\tilde{w}(i) \leq w(i)$ *for all* $i \in \{0, 1, \dots, m-1\}$.

Proposition 15. *Let* S *and* T *be numerical semigroups such that* $S \subseteq T$ *and let* $m \in S \setminus \{0\}$. *Then* $\mathrm{R}(S, a, m) \subseteq \mathrm{R}(T, a, m)$.

Proof. Suppose that $\mathrm{Ap}(S, m) = \{w(0), w(1), \dots, w(m-1)\}$ and that $\mathrm{Ap}(T, m) = \{\tilde{w}(0), \tilde{w}(1), \dots, \tilde{w}(m-1)\}$. If $x \in \mathrm{R}(S, a, m)$, then $w(ax \bmod m) \leq x$. By Lemma 14 we know that $\tilde{w}(ax \bmod m) \leq w(ax \bmod m) \leq x$, and therefore $x \in \mathrm{R}(T, a, m)$. □

Corollary 16. *One has:* $\mathrm{R}(S, a, m) \subseteq \mathrm{M}(a, m)$.

Proof. Since $S \subseteq \mathbb{N}$, by Proposition 15 we know that $\mathrm{R}(S, a, m) \subseteq \mathrm{R}(\mathbb{N}, a, m)$ and by Corollary 13 we have that $\mathrm{R}(\mathbb{N}, a, m) = \mathrm{M}(a, m)$. □

Next we show that the converse of Proposition 12 also holds, thus completing the proof of the result announced.

Theorem 17. *Let S be a numerical semigroup, a be a positive integer, $m \in S \setminus \{0\}$ and $d = (a, m)$. Then $\mathrm{R}(S, a, m) = \mathrm{M}(a, m)$ if and only if $d \in S$.*

Proof. As we pointed out above, in view of Proposition 12 we only have to prove necessity. Let $\mathrm{Ap}(S, m) = \{w(0), w(1), \ldots, w(m-1)\}$. If $\mathrm{R}(S, a, m) = \mathrm{M}(a, m)$, then from Proposition 2 we deduce that $ai \bmod m + (m + 1 - a)i \bmod m \in \mathrm{R}(S, a, m)$ for all $i \in \{0, 1, \ldots, m - 1\}$. Thus $w(a(ai \bmod m + (m + 1 - a)i \bmod m) \bmod m) \leq ai \bmod m + (m + 1 - a)i \bmod m$ and consequently $w(ai \bmod m) \leq ai \bmod m + (m + 1 - a)i \bmod m$. Since $w(ai \bmod m)$ is congruent with $ai \bmod m$ modulo m and $(m + 1 - a)i \bmod m \in \{0, 1, \ldots, m - 1\}$, we deduce that $w(ai \bmod m) = ai \bmod m$. It follows that $ai \bmod m \in S$ for all $i \in \{0, 1, \ldots, m - 1\}$. As $\left(\frac{a}{d}, \frac{m}{d}\right) = 1$, there exists $t \in \left\{1, \ldots, \frac{m}{d} - 1\right\}$ such that $\frac{a}{d}t \bmod \frac{m}{d} = 1$. Then $d = d\left(\frac{a}{d}t \bmod \frac{m}{d}\right) = at \bmod m \in S$. □

3. The Apéry set of a rotation

Recall that we have fixed some notation. Namely, the elements of $\mathrm{Ap}(S, m)$ and $\mathrm{Ap}(\mathrm{R}(S, a, m), m)$ are denoted by $w(i)$ and $\overline{w}(i)$ respectively, where $i \in \{0, 1, \ldots, m-1\}$.

Next result establishes a relationship between the elements of the Apéry sets $\mathrm{Ap}(S, m)$ and $\mathrm{Ap}(\mathrm{R}(S, a, m), m)$. It is then reformulated in a more convenient way in Theorem 19.

Lemma 18. *If $w(i) = k_i m + i$ for all $i \in \{0, 1, \ldots, m - 1\}$, then*

$$\overline{w}(i) = \begin{cases} k_{ai \bmod m} \cdot m + i & \text{if} \quad ai \bmod m \leq i, \\ (k_{ai \bmod m} + 1) \cdot m + i & \text{if} \quad ai \bmod m > i. \end{cases}$$

Proof. Let $x \in \mathbb{N}$ be such that $x \bmod m = i \in \{0, 1, \ldots, m - 1\}$. Then $x \in \mathrm{R}(S, a, m)$ if and only if $w(ai \bmod m) \leq x$, which is equivalent to $k_{ai \bmod m} \cdot m + (ai \bmod m) \leq x$. Thus $\overline{w}(i)$ is the least integer congruent with i modulo m that is greater than or equal to $k_{ai \bmod m} \cdot m + (ai \bmod m)$. The proposition is then easily deduced. □

Theorem 19. *If $i \in \{0, 1, \ldots, m - 1\}$, then*

$$\overline{w}(i) = w(ai \bmod m) + (m + 1 - a)i \bmod m.$$

Proof. From Lemma 18, and taking into account that $w(ai \bmod m) = k_{ai \bmod m} \cdot m + ai \bmod m$, we deduce that if $i \in \{0, 1, \ldots, m - 1\}$, then

$$\overline{w}(i) = w(ai \bmod m) + \begin{cases} i - ai \bmod m & \text{if} \quad ai \bmod m \leq i, \\ i - ai \bmod m + m & \text{if} \quad ai \bmod m > i. \end{cases}$$

The rest of the proof follows by Lemma 1. □

As we have seen above, by having a good description of the Apéry set of a numerical semigroup we can obtain important data of the given numerical semigroup. Theorem 19 will be used in the rest of this paper to take profit of this fact.

Example 20. Let $S = \langle 5, 7, 9\rangle$. We will use Theorem 19 to compute $\mathrm{R}(S, 2, 5)$ and $S = \langle 5, 7, 9\rangle$.

Since $\mathrm{Ap}(S, 5) = \{w(0) = 0, w(1) = 16, w(2) = 7, w(3) = 18, w(4) = 9\}$, we get that $\mathrm{Ap}(\mathrm{R}(S, 2, 5), 5) = \{\overline{w}(0) = 0, \overline{w}(1) = 11, \overline{w}(2) = 12, \overline{w}(3) = 18, \overline{w}(4) = 19\}$. Thus $\mathrm{R}(S, 2, 5) = \langle 5, 11, 12, 18, 19\rangle$.

Since $\mathrm{Ap}(S, 9) = \{w(0) = 0, w(1) = 10, w(2) = 20, w(3) = 12, w(4) = 22, w(5) = 5, w(6) = 15, w(7) = 7, w(8) = 17\}$, we get that $\mathrm{Ap}(\mathrm{R}(S, 6, 9), 9) = \{\overline{w}(0) = 0, \overline{w}(1) = 19, \overline{w}(2) = 20, \overline{w}(3) = 3, \overline{w}(4) = 22, \overline{w}(5) = 14, \overline{w}(6) = 6, \overline{w}(7) = 16, \overline{w}(8) = 17\}$. Thus $\mathrm{R}(S, 6, 9) = \langle 9, 19, 20, 3, 22, 14, 6, 16, 17\rangle = \langle 3, 14, 16\rangle$.

Theorem 17 suggests that the function assigning to each integer $a \in \{0, 1, \ldots, m-1\}$ the numerical semigroup $\mathrm{R}(S, a, m)$ is not injective in general. Next example shows, in particular, that this application not is injective even if we require $(a, m) = 1$.

Example 21. Let $S = \langle 5, 6, 7, 8, 9\rangle$. Then $\mathrm{Ap}(S, 5) = \{w(0) = 0, w(1) = 6, w(2) = 7, w(3) = 8, w(4) = 9\}$. Using Theorem 19 we get that both $\mathrm{Ap}(\mathrm{R}(S, 2, 5), 5)$ and $\mathrm{Ap}(\mathrm{R}(S, 4, 5), 5)$ are equal to $\{0, 11, 12, 8, 9\}$. Consequently $\mathrm{R}(S, 2, 5) = \mathrm{R}(S, 4, 5)$.

Remark 22. Recall that the Euler φ function is defined by $\varphi(n) = \#\{i \in \mathbb{N} \mid 1 \leq i \leq n \text{ and } (n, i) = 1\}$, for any positive integer n. Observe that we have the equality $\mathrm{R}(S, a, m) = \mathrm{R}(S, a \bmod m, m)$ and therefore $\#\{\mathrm{g}(\mathrm{R}(S, a, m)) \mid (a, m) = 1\} \leq \varphi(m)$. Example 21 shows that the previous bound is not attainable.

From Theorem 19 we deduce that $\max \mathrm{Ap}(\mathrm{R}(S, a, m)) \leq \max \mathrm{Ap}(S, m) + m - 1$. By applying Lemma 3 we get the following result.

Corollary 23. $\mathrm{g}(\mathrm{R}(S, a, m)) \leq \mathrm{g}(S) + m - 1$.

We intend now to continue the study of the Frobenius number and the singularity degree of $\mathrm{R}(S, a, m)$. The study for the general case will only be done in Section 5, since we need to study previously the quotients of a numerical semigroup by a positive integer, and this will be done in Section 4. But the case of co-prime rotations, that is, (a, m)-rotations with $(a, m) = 1$, is easier. We leave the result on the singularity degree for a corollary of Theorem 35, but we give here the result concerning the Frobenius number, since this result motivates an example and the reader may benefit from reading a simpler proof which contains the main ideas, although the result is not as general as possible.

Proposition 24. *If* $(a, m) = 1$, *then* $\mathrm{g}(S) \leq \mathrm{g}(\mathrm{R}(S, a, m)) \leq \mathrm{g}(S) + m - 1$.

Proof. By Corollary 23 it suffices to prove that $\mathrm{g}(S) \leq \mathrm{g}(\mathrm{R}(S, a, m))$. By Theorem 19 we know that $\overline{w}(i) = w(ai \bmod m) + (m + 1 - a)i \bmod m$ for all $i \in \{0, 1, \ldots, m-1\}$. As $(a, m) = 1$, then $\{w(0), w(1), \ldots, w(m-1)\} = \{w(ai \bmod m) \mid i \in \{0, 1, \ldots, m - 1\}\}$. Thus $\max \mathrm{Ap}(S, m) \leq \max \mathrm{Ap}(\mathrm{R}(S, a, m), m)$. Using Lemma 3 we get that $\mathrm{g}(S) \leq \mathrm{g}(\mathrm{R}(S, a, m))$. □

The following example shows that the upper bound given in previous proposition is attainable. The lower bound is clearly attainable, since if we take $a = 1$, we get $\mathrm{R}(S, 1, m) = S$.

Example 25. Let $S = \langle 3, 34\rangle$. Then $\mathrm{Ap}(S,3) = \{w(0) = 0, w(1) = 34, w(2) = 68\}$. By Lemma 3 we have $\mathrm{g}(S) = 65$. Applying now Theorem 19 we have $\mathrm{Ap}(\mathrm{R}(S,2,3),3) = \{\overline{w}(0) = 0, \overline{w}(1) = 70, \overline{w}(2) = 35\}$. By Lemma 3 we have $\mathrm{g}(S) = 67$.

4. The quotients of a numerical semigroup

Given a numerical semigroup and a positive integer p, let $\frac{M}{p} = \{x \in \mathbb{N} \mid px \in M\}$. Clearly $\frac{M}{p}$ is a numerical semigroup containing M. Furthermore $\frac{M}{p} = \mathbb{N}$ if and only if $p \in \mathbb{N}$. The semigroup $\frac{M}{p}$ is called *quotient numerical semigroup* of M by the integer p (see [5]). In this section d is a positive divisor of m.

Lemma 26. *Let $i \in \left\{0, \ldots, \frac{m}{d} - 1\right\}$. Then $w(id)$ is a multiple of d. Furthermore $\frac{w(id)}{d}$ is congruent with i modulo $\frac{m}{d}$.*

Proof. Since $w(id) = km + id$ for some $k \in \mathbb{N}$, $w(id)$ is a multiple of d and $\frac{w(id)}{d} = k\frac{m}{d} + i$. □

Observe that $\frac{m}{d} \in \frac{S}{d}$ and therefore it makes sense to talk about $\mathrm{Ap}\left(\frac{S}{d}, \frac{m}{d}\right)$. Next result shows how to obtain this set from $\mathrm{Ap}(S,m)$.

Theorem 27. *The set $\mathrm{Ap}\left(\frac{S}{d}, \frac{m}{d}\right)$ is obtained dividing by d the elements of $\mathrm{Ap}(S,m)$ that are multiples of d.*

Proof. Let $\ell \in \{0, \ldots, m-1\}$ and $w(\ell) \in \mathrm{Ap}(S,m)$. Then $w(\ell) = km + \ell$ for some $k \in \mathbb{N}$. As d is a divisor of m we deduce that $w(\ell)$ is a multiple of d if and only if ℓ is a multiple of d. Therefore $\left\{w(0), w(d), \ldots, w\left(d\left(\frac{m}{d} - 1\right)\right)\right\}$ is the set formed by the elements of $\mathrm{Ap}(S,m)$ that are multiples of d. Furthermore, from Lemma 26 we know that if $i \in \left\{0, \ldots, \frac{m}{d} - 1\right\}$, then $\frac{w(id)}{d}$ is congruent with i modulo $\frac{m}{d}$. To conclude the proof it suffices to show that $\frac{w(id)}{d}$ is the least element of $\frac{S}{d}$ that is congruent with i modulo $\frac{m}{d}$. Let $x \in \frac{S}{d}$ be such that x is congruent with i modulo $\frac{m}{d}$. Then $dx \in S$ and, applying Lemma 9 we have that $w(dx \bmod m) \leq dx$. Therefore $w(di) \leq dx$ and consequently $\frac{w(id)}{d} \leq x$. □

Example 28. Let $S = \langle 5, 6, 8\rangle$. Then $\mathrm{Ap}(S,6) = \{0, 13, 8, 15, 10, 5\}$. By the previous theorem we get that $\mathrm{Ap}\left(\frac{S}{2}, 3\right) = \{0, 4, 5\}$. Therefore $\frac{S}{2} = \langle 3, 4, 5\rangle$.

As an immediate consequence of Theorem 27, making use of Lemmas 6 and 3, we get the following corollary.

Corollary 29. *If* $\mathrm{Ap}(S,m) = \{0, k_1 m + 1, \ldots, k_{m-1} m + (m-1)\}$, *then:*

(1) $\mathrm{Ap}\left(\frac{S}{d}, \frac{m}{d}\right) = \left\{0, k_d \frac{m}{d} + 1, \ldots, k_{(\frac{m}{d}-1)d} \frac{m}{d} + \left(\frac{m}{d} - 1\right)\right\}$.

(2) $\#\mathrm{H}\left(\frac{S}{d}\right) = k_d + k_{2d} + \cdots + k_{(\frac{m}{d}-1)d}$.

(3) $\mathrm{g}\left(\frac{S}{d}\right) = \max\left\{0, k_d \frac{m}{d} + 1, \ldots, k_{(\frac{m}{d}-1)d} \frac{m}{d} + \left(\frac{m}{d} - 1\right)\right\} - \frac{m}{d}$.

5. Singularity degree and Frobenius number of a rotation

In this section we will obtain bounds for the Frobenius number and a formula for the singularity degree of a rotation in terms of the same invariants of the original semigroup. The following lemma exhibits an element of $\mathrm{R}(S,a,m)$ which proves out to be fundamental in this task. Recall that $d=(a,m)$.

Lemma 30. $\frac{m}{d}\in \mathrm{R}(S,a,m)$.

Proof. As $w\left(a\frac{m}{d} \bmod m\right)=w(0)=0$, we have that $w\left(a\frac{m}{d} \bmod m\right)\le \frac{m}{d}$ and therefore $\frac{m}{d}\in \mathrm{R}(S,a,m)$. □

As $\frac{m}{d}\in \mathrm{R}(S,a,m)$ it makes sense to talk about $\mathrm{Ap}\left(\mathrm{R}(S,a,m),\frac{m}{d}\right)$. Well, in this section we will assume that $\mathrm{Ap}\left(\mathrm{R}(S,a,m),\frac{m}{d}\right)=\left\{w'(0),w'(1),\dots,w'\left(\frac{m}{d}-1\right)\right\}$. This set is contained in $\mathrm{Ap}(\mathrm{R}(S,a,m),m)$, as shows the following lemma.

Lemma 31. *If $x\in \mathrm{Ap}\left(\mathrm{R}(S,a,m),\frac{m}{d}\right)$, then $x\in \mathrm{Ap}(\mathrm{R}(S,a,m),m)$.*

Proof. If $x-m\in \mathrm{R}(S,a,m)$ then $x-\frac{m}{d}\in \mathrm{R}(S,a,m)$, since $x-\frac{m}{d}=x-m+(d-1)\frac{m}{d}$ and $\frac{m}{d}\in \mathrm{R}(S,a,m)$. □

Now we are able to present a very convenient way to express the elements of $\mathrm{Ap}(\mathrm{R}(S,a,m),m)$. Notice that, in view of Theorem 17, the next result has Proposition 2 as an immediate consequence.

Theorem 32. *If $i\in\left\{0,\dots,\frac{m}{d}-1\right\}$, then*

$$w'(i)=w(ai \bmod m)+(m+1-a)i \bmod \frac{m}{d}.$$

Proof. Observe that using Lemma 31 and the definition of Apéry set one immediately concludes that $\mathrm{Ap}\left(\mathrm{R}(S,a,m),\frac{m}{d}\right)$ consists of the elements of $\mathrm{Ap}(\mathrm{R}(S,a,m),m)$ that subtracted by $\frac{m}{d}$ do not belong to $\mathrm{R}(S,a,m)$.

By Theorem 19 we know that $\overline{w}(j)=w(aj \bmod m)+(m+1-a)j \bmod m$ for every $j\in\{0,\dots,m-1\}$. Applying the definition of $\mathrm{R}(S,a,m)$ we have that $\overline{w}(j)-\frac{m}{d}\notin \mathrm{R}(S,a,m)$ if and only if $w\left(a\left(w(aj \bmod m)+(m+1-a)j \bmod m-\frac{m}{d}\right) \bmod m\right)> w(aj \bmod m)+(m+1-a)j \bmod m-\frac{m}{d}$. Observe that $w(aj \bmod m)+(m+1-a)j \bmod m$ modulo m is precisely $aj+(m+1-a)j$ modulo m and therefore we have that $w\left(a\left(w(aj \bmod m)+(m+1-a)j \bmod m-\frac{m}{d}\right) \bmod m\right)=w(aj \bmod m)$. Thus $\overline{w}(j)-\frac{m}{d}\notin \mathrm{R}(S,a,m)$ if and only if $w(aj \bmod m)>w(aj \bmod m)+(m+1-a)j \bmod m-\frac{m}{d}$ and this equivalent to $(m+1-a)j \bmod m<\frac{m}{d}$. Observe now that $(m+1-a)j \bmod m<\frac{m}{d}$ if and only if $(m+1-a)j \bmod m=(m+1-a)j \bmod \frac{m}{d}$. Consequently $\overline{w}(j)-\frac{m}{d}\notin \mathrm{R}(S,a,m)$ if and only if $\overline{w}(j)=w(aj \bmod m)+(m+1-a)j \bmod \frac{m}{d}$. As we have $aj \bmod m=d\left(\frac{a}{d}j \bmod \frac{m}{d}\right)=d\left(\frac{a}{d}\left(j \bmod \frac{m}{d}\right) \bmod \frac{m}{d}\right)=a\left(j \bmod \frac{m}{d}\right) \bmod m$ and $(m+1-a)j \bmod \frac{m}{d}=(m+1-a)\left(j \bmod \frac{m}{d}\right) \bmod \frac{m}{d}$, we can say that $\overline{w}(j)-\frac{m}{d}\notin \mathrm{R}(S,a,m)$ if and only if $\overline{w}(j)=w\left(a\left(j \bmod \frac{m}{d}\right) \bmod m\right)+(m+1-a)\left(j \bmod \frac{m}{d}\right) \bmod \frac{m}{d}$. Consequently, the elements of $\mathrm{Ap}(\mathrm{R}(S,a,m),m)$ that subtracted by $\frac{m}{d}$ do not belong to $R(S, a, m)$ are those of the form $w(ai \bmod m) + (m+1-a)i \bmod \frac{m}{d}$ with $i \in \left\{0, \ldots, \frac{m}{d} - 1\right\}$. □

Example 33. Let $S = \langle 5, 7, 9\rangle$. We will use the preceding theorem to compute $R(S, 6, 9)$. By Example 20 we know that $\mathrm{Ap}(S, 9) = \{w(0) = 0, w(1) = 10, w(2) = 20, w(3) = 12, w(4) = 22, w(5) = 5, w(6) = 15, w(7) = 7, w(8) = 17\}$. Using Theorem 32 we have that $\mathrm{Ap}(R(S, 6, 9), 3) = \{0, 16, 14\}$. Thus $R(S, 6, 9) = \langle 3, 14, 16\rangle$.

Next we get bounds for the Frobenius number of $R(S, a, m)$.

Corollary 34. $d\mathrm{g}\left(\frac{S}{d}\right) + (d-1)\frac{m}{d} \le \mathrm{g}(R(S, a, m)) \le d\mathrm{g}\left(\frac{S}{d}\right) + m - 1$.

Proof. By Theorem 32 we know that $w'(i) = w\left(d\left(\frac{a}{d}i \bmod \frac{m}{d}\right)\right) + (m+1-a)i \bmod \frac{m}{d}$ for all $i \in \{0, \ldots, \frac{m}{d} - 1\}$. We observe that $w\left(d\left(\frac{a}{d}i \bmod \frac{m}{d}\right)\right)$ is an element of $\mathrm{Ap}(S, m)$ that is a multiple of d. Applying then Theorem 27 we have the inequalities $d\left(\max \mathrm{Ap}\left(\frac{S}{d}, \frac{m}{d}\right)\right) \le \max \mathrm{Ap}\left(R(S, a, m), \frac{m}{d}\right) \le d\left(\max \mathrm{Ap}\left(\frac{S}{d}, \frac{m}{d}\right)\right) + \frac{m}{d} - 1$. If we apply now Lemma 3 we obtain that $d\left(\mathrm{g}\left(\frac{S}{d}\right) + \frac{m}{d}\right) \le \mathrm{g}(R(S, a, m)) + \frac{m}{d} \le d\left(\mathrm{g}\left(\frac{S}{d}\right) + \frac{m}{d}\right) + \frac{m}{d} - 1$. Consequently $d\mathrm{g}\left(\frac{S}{d}\right) + (d-1)\frac{m}{d} \le \mathrm{g}(R(S, a, m)) \le d\mathrm{g}\left(\frac{S}{d}\right) + m - 1$. □

Notice that since $\frac{S}{1} = S$, Proposition 24 is an immediate consequence of Corollary 34. Observe also that by Example 25 the bounds are attainable. Now comes the announced result that relates the singularity degrees of a rotation and a quotient of S.

Theorem 35. $\#\mathrm{H}(R(S, a, m)) = d\,\#\mathrm{H}\left(\dfrac{S}{d}\right) + \dfrac{m + 1 - d - (a-1, m)}{2}$.

Proof. Let us suppose that $\mathrm{Ap}(S, m) = \{k_0 m + 0, k_1 m + 1, \ldots, k_{m-1}m + (m-1)\}$. Then by Lemma 18 we know that $\overline{w}(i) = \overline{k}_{ai \bmod m} m + i$ where

$$\overline{k}_{ai \bmod m} = \begin{cases} k_{ai \bmod m} & \text{if} \quad ai \bmod m \le i, \\ k_{ai \bmod m} + 1 & \text{if} \quad ai \bmod m > i. \end{cases}$$

By Lemma 6 we know that

$$\#\mathrm{H}(R(S, a, m)) = \sum_{i=1}^{m-1} \overline{k}_{ai \bmod m}$$

and by Proposition 8 that

$$\sum_{i=1}^{m-1} \overline{k}_{ai \bmod m} = \sum_{i=1}^{m-1} k_{ai \bmod m} + \frac{m + 1 - d - (a-1, m)}{2}.$$

Observe that $ai \bmod m = a\left(i \bmod \frac{m}{d}\right) \bmod m$. Thus

$$\sum_{i=1}^{m-1} k_{ai \bmod m} = d\sum_{i=1}^{\frac{m}{d}-1} k_{d\left(\frac{a}{d}i \bmod \frac{m}{d}\right)} = d\left(k_d + \cdots + k_{\left(\frac{m}{d}-1\right)d}\right).$$

Applying (2) of Corollary 29 we have that $k_d + \cdots + k_{\left(\frac{m}{d}-1\right)d} = \#\mathrm{H}\left(\frac{S}{d}\right)$ and the result follows. □

Observing that $\frac{S}{1} = S$ we get the following corollary.

Corollary 36. *If* $(a, m) = 1$, *then*

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

A proof of this result could have given without using quotients. Notice that as $(a, m) = 1$, the function $\sigma : \{1, \ldots, m-1\} \to \{1, \ldots, m-1\}$ defined by $\sigma(i) = ai \bmod m$ is a bijection. From Lemma 18 we could then deduce that $\mathrm{Ap}(\mathrm{R}(S, a, m), m) = \{0, \overline{k}_{\sigma(1)}m + 1, \ldots, \overline{k}_{\sigma(m-1)}m + (m-1)\}$, where

$$\overline{k}_{\sigma(i)} = \begin{cases} k_{\sigma(i)} & \text{if} \quad \sigma(i) \le i, \\ k_{\sigma(i)} + 1 & \text{if} \quad \sigma(i) > i. \end{cases}$$

The result would then follow by using Lemma 6 and Proposition 8.

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] J. L. Ramírez Alfonsín, The Diophantine Frobenius problem, Forschungsintitut für Diskrete Mathematik, Bonn, Report N0.00893 (2000).

[4] J. C. Rosales and P. A. García-Sánchez, “Finitely generated commutative monoids”, Nova Science Publishers, New York, 1999.

[5] J. C. Rosales, P. A. García-Sánchez, J. I. García-García and J. M. Urbano-Blanco, Proportionally modular Diophantine inequalities, J. Number Theory **103** (2003), 281-294.

[6] J. C. Rosales, P. A. García-Sánchez and J. M. Urbano-Blanco, Modular Diophantine inequalities and numerical semigroups, Pacific J. Math., to appear in Vol 218 (2005).

[7] E. S. Selmer, On a linear diophantine problem of Frobenius, J. Reine Angew. Math. **293/294** (1977), 1-17.

E-mail address: mdelgado@fc.up.pt

Centro de Matemática, Universidade do Porto, Rua do Campo Alegre 687, 4169-007 Porto, Portugal

E-mail address: jrosales@ugr.es

Departamento de Álgebra, Universidad de Granada, E-18071 Granada, Spain