MODULAR DIOPHANTINE INEQUALITIES AND SOME OF THEIR INVARIANTS

J. C. ROSALES

Departamento De Algebra, Universidad De Granada, E-18071 Granada, Spain
E-mail address: jrosales@ugr.es

(Received 7 May 2004; after final revision 4 June 2004; accepted 29 August 2005)

Given two positive integers \(a\) and \(b\), \(a \mod b\) denotes the remainder of the division of \(a\) by \(b\). A modular Diophantine inequality is an expression of the form \(ax \mod b \leq x\) for some positive integers \(a\) and \(b\). The set \(S(a, b)\) of integer solutions of this inequality is a numerical semigroup, that is, it is a subset of \(\mathbb{N}\) (\(\mathbb{N}\) denotes the set of nonnegative integers) closed under additions, \(0 \in S(a, b)\) and its complement in \(\mathbb{N}\) has finitely many elements. It is well known (see for instance [7]) that every numerical semigroup is finitely generated, and thus there exist positive integers \(n_1, \ldots, n_e\) such that \(S(a, b) = \langle n_1, \ldots, n_e \rangle = \{a_1 n_1 + \ldots + a_e n_e \mid a_1, \ldots, a_e \in \mathbb{N}\}\).

This paper continues the study of modular Diophantine inequalities initiated in [9, 10]. In Section 1, we describe an algorithmic procedure to compute a finite system of generators of \(S(a, b)\). The key result of this section is Theorem 1, which associates to \(S(a, b)\) a full affine semigroup \(A(a, b)\) so that for any system of generators \(\{(x_1, y_1), \ldots, (x_e, y_e)\}\) we have that \(\{x_1 + y_1, \ldots, x_e + y_e\}\) is a system of generators of \(S(a, b)\). These facts together with the concept of modular permutation will allow us in Section 2 to calculate a minimal system of generators for \(A(a, b)\) and consequently an upper bound for the embedding dimension of \(S(a, b)\) (the cardinality of a minimal system of generators of \(S(a, b)\)).

In the literature one can find several invariants of a numerical semigroup. The Frobenius number, the degree of singularity and type are some of them. These invariants are tightly related to the knowledge of the Apéry set of an element in the semigroup. In Section 3, and more precisely, in Theorem 19 we describe the Apéry set of \(S(a, b)\) with respect to the element \(b/\gcd(a-1, b)\) and this will yield information on the above mentioned invariants. Finally, all these results will enable us to give in Section 4 a way to construct systems of generators of symmetric numerical semigroups with Frobenius number previously chosen.

1. A SYSTEM OF GENERATORS FOR \(S(a, b)\)

Let \(a\) and \(b\) be positive integers. Since the Diophantine inequalities \(ax \mod b \leq x\) and \((a \mod b) x \mod b \leq x\) have the same integer solutions, we assume in from now on that \(a < b\).

The author is supported by the project BFM2000-1469 and wants to thank P. A. García-Sánchez for his comments and suggestions.
Let $x, y, z$ be integers. We write $x \equiv y \mod z$ to indicate that $x - y$ is a multiple of $z$. With this notation, we introduce the following result that is crucial in the rest of the paper.

**Theorem 1** — Let $a < b$ be positive integers. Then

$$S(a, b) = \{x + y \mid (x, y) \in \mathbb{N}^2 \text{ and } x(a - 1) + ya \equiv 0 \mod b\}.$$  

**Proof:** If $s \in S(a, b)$, then $as \mod b = x \leq s$. Set $y = s - x$. Clearly, $as - x \equiv 0 \mod b$ and thus $x(a - 1) + ya \equiv 0 \mod b$. Conversely, $a(x + y) \mod b = ((a - 1)x + ay + x) \mod b = x \mod b \leq x \leq x + y$ and thus $x + y \in S(a, b)$. \hfill \Box

Let $\mathbb{Z}$ be the set of integers, $r$ a positive integer and $H$ a subgroup of $\mathbb{Z}^r$. Then

$H \cap \mathbb{N}^r$ is a submonoid of $\mathbb{N}^r$. These semigroups, known as full-semigroups (see [4]), are finitely generated, because they are minimally generated (see [7]) by the set of minimal elements of

$H \cap \mathbb{N}^r \setminus \{(0, \ldots, 0)\}$ with respect to the usual partial order on $\mathbb{N}^r$ ($x \leq y$ if $y - x \in \mathbb{N}^r$).

If $a < b$ are positive integers, we denote by

$$A(a, b) = \{S(x, y) \in \mathbb{N}^2 \mid (a - 1)x + ay \equiv 0 \mod b\}.$$  

This set is a full-affine semigroup, because $A(a, b) = \{(x, y) \in \mathbb{Z}^2 \mid (a - 1)x + ay \equiv 0 \mod b\}$

$\cap \mathbb{N}^2$.

Let $p : \mathbb{N}^2 \to \mathbb{N}$ be the map defined by $p(x, y) = x + y$. In view of Theorem 1, $S(a, b) = p(A(a, b))$. As $p$ is a semigroup homomorphism, we get the following result.

**Proposition 2** — Let $a < b$ be two positive integers. If $\{(x_1, y_1), \ldots, (x_e, y_e)\}$ is a system of generators of $A(a, b)$, then $\{x_1 + y_1, \ldots, x_e + y_e\}$ is a system of generators of $S(a, b)$.

Our next goal is to find a procedure to obtain in an easy and efficient way a system of generators of $A(a, b)$. With this in mind we introduce the following notation.

Given a positive integer $n$, we denote the set $\{0, \ldots, n - 1\}$ by $\mathbb{Z}_n$. Clearly, $(\mathbb{Z}_n, +, \cdot)$ is a ring with the operations $x + y = x + y \mod n$ and $x \cdot y = xy \mod n$. If $a < b$ are positive integers, $d = \gcd(a, b)$ and $d' = \gcd(a - 1, b)$, define
\[ H(a,b) = \{(x, y) \in \mathbb{Z}_{b/d'} \times \mathbb{Z}_{b/d} : (a-1)x + ay \equiv 0 \mod b\}. \]

This set is a subgroup of \( (\mathbb{Z}_{b/d'} \times \mathbb{Z}_{b/d}, +) \) and it is also a finite subset of \( \mathbb{N}^2 \). Given a rational number \( q \), set \( \lfloor q \rfloor = \max\{z \in \mathbb{Z} : z \leq q\} \).

**Proposition 3** — Let \( a < b \) be positive integers, \( d = \gcd\{a, b\} \) and \( d' = \gcd\{a - 1, b\} \). If \( (x, y) \in A(a, b) \), then there exist \( \lambda, \mu \in \mathbb{N} \) and \( (h_1, h_2) \in H(a, b) \) such that \( (x, y) = \lambda (b/d', 0) + \mu (0, b/d) + (h_1, h_2) \).

**Proof:** Let \( \alpha_1 = b/d' \) and \( \alpha_2 = b/d \). If \( (x, y) \in A(a, b) \), then \( (x \mod \alpha_1, y \mod \alpha_2) \in H(a, b) \) and \( (x, y) = \lfloor \frac{x}{\alpha_1} \rfloor (\alpha_1, 0) + \lfloor \frac{y}{\alpha_2} \rfloor (0, \alpha_2) + (x \mod \alpha_1, y \mod \alpha_2) \).

As an immediate consequence we obtain the following.

**Corollary 4** — Let \( a < b \) be positive integers, \( d = \gcd\{a, b\} \) and \( d' = \gcd\{a - 1, b\} \). Then the semigroup \( A(a, b) \) is generated by \{\((b/d', 0), (0, b/d)\) \( \cup H(a, b) \).

The next result can be deduced from [8]. We include its proof since no explicit demonstration is given there.

**Proposition 5** — Let \( a < b \) be positive integers, \( d = \gcd\{a, b\} \) and \( d' = \gcd\{a -1, b\} \). Then

1. if \( (x, y) \in H(a, b) \setminus \{(0, 0)\} \), then \( x \neq 0 \) and \( y \neq 0 \),

2. there exists \( t \in \{1, \ldots, b/d - 1\} \) such that \((a-1)d + at \equiv 0 \mod b\),

3. \( H(a, b) \) is the subgroup of \( \mathbb{Z}_{b/d'} \times \mathbb{Z}_{b/d} \) generated by \{\((d, t)\)\}.

**Proof:** (1) We show that if \( (0, y) \in H(a, b) \), then \( y = 0 \). If \( (0, y) \in H(a, b) \), then \( y \in \{0, \ldots, b/d - 1\} \) and thus \((a-1)0 + ay \equiv 0 \mod b\). This implies that \( ay \) is a common multiple of \( a \) and \( b \). However, the least common multiple of \( a \) and \( b \) is \( ab/d \). This leads to \( y = 0 \). Analogously, one proves that if \( (x, 0) \in H(a, b) \), then \( x = 0 \).

(2) Observe that \((a-1)d + at \equiv 0 \mod b\) if and only if \((a-1) + (a/d)t \equiv 0 \mod (b/d)\). The existence of \( t \) is ensured because \( \gcd\{a/d, b/d\} = 1 \).
(3) If \((x, y) \in H(a, b)\), then \((a - 1) x + ay \equiv 0 \mod b\), whence there exists \(l \in \mathbb{N}\) such that \((a - 1)x = lb - ay\). Since \(d\) divides \(lb - ay\) and \(\gcd(d, a - 1) = 1\), we have that \(d\) divides \(x\). Thus, there exists \(k \in \mathbb{N}\) such that \(x = kd\). As \(H(a, b)\) is a group, \((x, y) - k(d, t) \in H(a, b)\) and its first coordinate is zero, which in view of 1) implies that \((x, y) - k(d, t) = (0, 0)\).

To conclude this section we give an example in which we make use of the results shown so far.

Example 6 — Let us compute a system of generators of \(S(9, 30)\) (or equivalently, we are going to find the set of all nonnegative integer solutions to the inequality \(9x \mod 30 \leq x\)). By using Corollary 4 and the remark after Theorem 1, we deduce that \(A(9, 30)\) is generated by

\[
\operatorname{Minimals}_\leq \{ (15, 0), (0, 10) \} \cup H(9, 30) \setminus \{ (0, 0) \}.
\]

As \(8 \times 3 + 9 \times 4 \equiv 0 \mod 30\), Proposition 5 tells us that \(H(9, 30)\) is the subgroup of \(\mathbb{Z}_{15} \times \mathbb{Z}_{10}\) generated by \((3, 4)\). Hence, \(H(9, 30) = \{ (0, 0), (3, 4), (6, 8), (9, 2), (12, 6) \}\). This implies that \(A(9, 30) = \langle (15, 0), (0, 10), (3, 4), (9, 2) \rangle\). Finally, by Proposition 2 we have that \(S(9, 30) = \langle 15, 10, 7, 11 \rangle\).

2. Minimal Generators of \(A(a, b)\) and Modular Permutations

Along this section (in order to be brief) we will assume that \(a < b\) are positive integers, \(d = \gcd(a, b)\), \(d' = \gcd(a - 1, b)\) and

\[
H'(a, b) = \left\{ (x, y) \in \left( \mathbb{Z}_b \times \mathbb{Z}_{bd'} \right)^2 \mid \frac{a - 1}{d'} x + \frac{a}{d} y \equiv 0 \mod \frac{b}{dd'} \right\}.
\]

Note that \(b\) is a multiple of \(dd'\) because \(\gcd(a, a - 1) = 1\).

Proposition 7 — \(H(a, B) = \{ (dx, d' y) \mid (x, y) \in H'(a, b) \} \).

Proof : The reader will not find any difficulties in showing that \((x, y) \in H'(a, b)\) if and only if \((dx, d' y) \in H'(a, b)\). The proof is complete once we realize that as \(\gcd(a - 1, a) = 1\), we have that if \((x, y) \in H(a, b)\), then \(x\) is a multiple of \(d\) (this has been used above) and \(y\) is a multiple of \(d'\).
Note that if $dd' = b$, then $H'(a, b) = \{(0, 0)\}$ and consequently $H(a, b) = \{(0, 0)\}$. By Corollary 4, we have that $A(a, b) = \langle (b/d', 0), (0, b/d) \rangle$. As an immediate consequence of Proposition 2, we have the following.

**Corollary 8** — If $dd' = b$, then $S(a, b) = \langle b/d', b/d \rangle$.

**Example 9** — We compute the system of generators of the semigroup $S(15, 42)$. Note that $d = 3$ and $d' = 14$. Hence $b = dd'$ and $S(15, 42) = \langle 3, 14 \rangle$.

From Corollary 8 one easily deduces [10, Corollary 32] as we show next.

**Corollary 10** — Let $S$ be a numerical semigroup minimally generated by the positive integers $n_1, n_2$. Then there exist positive integers $a < b$ such that $S = S(a, b)$.

**Proof**: Since $\gcd\{n_1, n_2\} = 1$, there exist positive integers $u, v$ such that $un_1 - vn_2 = 1$. Note that $\gcd\{un_1, n_1 n_2\} = n_1$ and $\gcd\{u_1 - 1, n_1 n_2\} = \gcd\{vn_2, n_1 n_2\} = n_2$. Hence by Corollary 8, we conclude that $S(un_1, n_1 n_2) = \langle n_1, n_2 \rangle$.

**Lemma 11** — If $dd' \neq b$ and $p = \left(\frac{a}{d}\right)^{-1} \left(-\frac{a-1}{d'}\right) \mod \frac{b}{dd'}$, then $H'(a, b)$ is the subgroup of $\left(\frac{\mathbb{Z}}{b/d'}\right)$ generated by $\{(1, p)\}$.

**Proof**: Observe that $\frac{a-1}{d'} + \frac{a}{d} \cdot p = 0 \mod \frac{b}{dd'}$, if and only if $p = \left(\frac{a}{d}\right)^{-1} \left(-\frac{a-1}{d'}\right) \mod \frac{b}{dd'}$. Hence $(1, p) \in H'(a, b)$. Following an argument similar to the one used in Proposition 5 one easily concludes the proof.

As an immediate consequence of Lemma 11 and Proposition 7 we obtain the following result.

**Proposition 12** — Under the hypothesis of Lemma 11,

$$H(a, b) = \left\{ \left( kd, \left( kd \mod \frac{b}{dd'} \right) \right) \mid k \in \{0, \ldots, \frac{b}{dd'} - 1\} \right\}.$$  

If $p = 1$, then $\text{Minimals}_{S}(H(a, b) \setminus \{(0,0)\}) = \{(d, d')\}$. Hence by Corollary 4 and the remark after Theorem 1, we have that $A(a, b) = \left\langle \left(\frac{b}{d'}, 0\right), \left(0, \frac{b}{d}\right), (d, d') \right\rangle$.
Corollary 13 — Under the hypothesis of Lemma 11, if $p = 1$, then $S(a, b) = \langle \left( \frac{b}{d}, \frac{b}{d'} \right), d, d' \rangle$.

Example 14 — By Corollary 13, as $p = (3^{-1}(-4)) \mod 7 = 1$, we have that $S(9, 42) = \langle 21, 14, 5 \rangle$.

Corollary 15 — Let $n_1, n_2, u$ and $v$ be positive integers such that $un_1 - vn_2 = 1$. Then

$$S(u n_1, (u + v) n_1 n_2) = \langle (u + v) n_2, (u + v) n_1, n_1 + n_2 \rangle.$$ 

PROOF: It suffices to point out that $\gcd\{u n_1, (u + v) n_1 n_2\} = n_1$ and that $\gcd\{u n_1 - 1, (u + v) n_1 n_2\} = n_2$, and then apply Corollary 13.

Let $S_n$ be the symmetric group of degree $n$, that is, the set of all one-to-one maps from $\{1, ..., n\}$ into itself. Following the notation in [9], we will say that a permutation

$$\sigma = \begin{pmatrix} 1 & 2 & ... & n \\ \sigma(1) & \sigma(2) & ... & \sigma(n) \end{pmatrix} \in S_n$$

is modular if there exists a positive integer $k$ such that $\sigma(i) = (ki) \mod (n + 1)$, for each $i \in \{1, ..., n\}$. If $x$ and $y$ are positive integers such that $\gcd\{x, y\} = 1$, we denote by $\sigma_{x,y}$ the modular permutation of $S_{y-1}$ defined by

$$\sigma_{x,y}(i) = (xi) \mod y.$$ 

Given $\sigma \in S_n$, set

$$I(\sigma) = \{i \in \{1, ..., n\} | \sigma(i) \leq \sigma(j) \text{ for all } j \in \{1, ..., i\}\}.$$
**Theorem 16** — Let $a < b$ be positive integers, $d = \gcd(a, b)$ and $d' = \gcd(a - l, b)$. If $dd' \neq b$ and $p = \left( \frac{a}{d} \right)^{-1} \left( \frac{-a-1}{d'} \right) \mod \frac{b}{dd'}$, then $A(a, b)$ is minimally generated by

$$\{ \left( \frac{b}{dd'}, 0 \right), \left( 0, \frac{b}{d} \right) \} \cup \left\{ \left( dk, d' \sigma_{p, \frac{b}{dd'}} (k) \right) | k \in I \left( \sigma_{p, \frac{b}{dd'}} \right) \right\}$$

**Proof**: As $\gcd \left( p, \frac{b}{dd'} \right) = 1$, we have that $\sigma_{p, \frac{b}{dd'}}$ is a permutation. Since $\sigma_{p, \frac{b}{dd'}}(k) = kp \mod \frac{b}{dd'}$. In view of Proposition 12, we deduce that

$$\text{Minimals}_{S} (H (a, b) \setminus \{(0, 0)\}) = \left\{ \left( dk, d' \sigma_{p, \frac{b}{dd'}} (k) \right) | k \in I \left( \sigma_{p, \frac{b}{dd'}} \right) \right\}.$$

The proof now follows from Corollary 4 and the remark after Theorem 1.

It is a well known fact that every numerical semigroup has a unique minimal system of generators (see for instance [7]). The cardinality of this set is known as the embedding dimension of $S$ and it is denoted by $e(S)$. As a consequence of Proposition 2 and Theorem 16 we obtain a bound for $e(S(a, b))$.

**Corollary 17** — Under the hypothesis of Theorem 16,

$$e(S(a, b)) \leq \# I \left( \sigma_{p, \frac{b}{dd'}} \right) + 2.$$

($\#A$ denotes the cardinality of the set $A$).

**Example 18** — Let us compute a system of generators for $S(56, 455)$. In this setting $d = 7$, $d' = 5$, $\frac{b}{dd'} = 13$ and $p = (8^{-1} (-11)) \mod 13 = 10$. Since $\sigma_{10, 13} (i + 1) = (\sigma_{10, 13} (i) + 10) \mod 13$, one can easily obtain that

$$\sigma_{10, 13} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 10 & 7 & 4 & 1 & 11 & 8 & 5 & 2 & 12 & 9 & 6 & 3 \end{pmatrix}.$$ 

Hence $I (\sigma_{10, 13}) = \{1, 2, 3, 4\}$. By Theorem 16, $A(56, 455)$ is minimally generated by $\{(91, 0), (0, 65), (7 \times 1, 5 \times 10), (7 \times 2, 5 \times 7), (7 \times 3, 5 \times 4), (7 \times 4, 5 \times 1)\}$. By Proposition 2, we have that $S(56, 455) = \{91, 65, 57, 49, 41, 33\}$.

Note that in the above example the bound given in Corollary 17 is reached.
3. **THE APÉRY SET OF** $S(a, b)$

Given a numerical semigroup $S$ and $n \in S \setminus \{0\}$, the Apéry set of $S$ in $n$ (see [1]) is $Ap(S, n) = \{x \in S \mid x - n \in S\}$. It is well known (and easy to prove) that $Ap(S, n)$ has $n$ elements and that $Ap(S, n) = \{0, w(1), \ldots, w(n-1)\}$, where $w(i)$ is the least element in $S$ congruent with $i$ modulo $n$. For $A, B \subseteq \mathbb{N}$, set $A + B = \{a + b \mid a \in A, b \in B\}$.

If $\sigma$ belongs to $S_n$, then it makes no sense to speak about $\sigma(0)$. However, in order to simplify the notation, in the sequel we will assume that $\sigma(0) = 0$.

**Theorem 19** — Let $a < b$ be positive integers, $d = \gcd(a, b)$ and $d' = \gcd(a - 1, b)$. If $dd' \neq b$, let $p = \left(\begin{array}{c} a \\ d \end{array}\right)^{-1} \left(\begin{array}{c} -a - 1 \\ d' \end{array}\right) \mod \frac{b}{dd'}$. Then

$$Ap\left(S(a, b), \frac{b}{d'}\right) = \left\{dk + d'\sigma_{p, \frac{b}{dd'}}(k) \mid k \in \left\{0, \ldots, \frac{b}{dd'} - 1\right\}\right\} + \left\{0, \frac{b}{d}, 2\frac{b}{d}, \ldots, (d - 1)\frac{b}{d}\right\}.$$  

**Proof:** Let $B = \left\{dk + d'\sigma_{p, \frac{b}{dd'}}(k) \mid k \in \left\{0, \ldots, \frac{b}{dd'} - 1\right\}\right\} + \left\{0, \frac{b}{d}, 2\frac{b}{d}, \ldots, (d - 1)\frac{b}{d}\right\}$. Note that $\#B \leq \frac{b}{dd'} \cdot d = \frac{b}{d'}$. This in order to prove the statement it suffices to show that for every $s \in S(a, b)$ there exists $\lambda \in \mathbb{N}$ and $w \in B$ such that $s = \lambda \frac{b}{d'} + w$. This follows from Propositions 3, 12 and 2.

If $S$ is a numerical semigroup, then $\mathbb{N} \setminus S$ has finitely many elements. The largest integer not in $S$ is the Frobenius number of $S$, denoted by $g(S)$. In [9], the problem of finding a formula for $g(S(a, b))$ is left open. It is a well known fact that for any numerical semigroup and every $n \in S \setminus \{0\}$, $g(S) = \max(\text{Ap}(S, n)) - n$ (see for instance [7]). As we know how are the elements of $Ap\left(S(a, b), \frac{b}{d'}\right)$, this yields the following result.

**Corollary 20** — Under the hypothesis of Theorem 19,

$$g(S(a, b)) = \max\left\{dk + d'\sigma_{p, \frac{b}{dd'}}(k) \mid k \in \left\{0, \ldots, \frac{b}{dd'} - 1\right\}\right\}$$
\[ + (d - 1) \frac{b}{d} - \frac{b}{d'}. \]

**Example 21.** Let us compute the Frobenius number of \( S(9, 30) \). Note that \( b = 30, a = 9, d = 3 \) and \( d' = 2 \). Hence \( \frac{b}{d'} = 15, \frac{b}{d} = 10, \frac{b}{dd'} = 5 \) and \( p = (3^{-1} (-4)) \mod 5 = 2 \). Since

\[ \sigma_{5, 2} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}, \]

by Theorem 19 we know that

\[ Ap(S(9, 30), 15) = \{0, 3 \times 1 + 2 \times 2, 3 \times 2 + 2 \times 4, 3 \times 3 + 2 \times 1, 3 \times 4 + 2 \times 3\} + \{0, 10, 20\} = \{0, 7, 14, 11, 18, 10, 17, 24, 21, 28, 20, 27, 34, 31, 38\}. \]

Hence \( g(S(9, 30)) = 38 - 15 = 23 \).

Given a numerical semigroup \( S \), the cardinality of the set \( \mathcal{H}(S) = \mathbb{N} \setminus S \) is an important invariant known as the gender (see [5]) or degree of singularity (see [2]) of \( S \). In [11] the following formula is given for any numerical semigroup \( S \) and \( n \in S \setminus \{0\} \):

\[ \# \mathcal{H}(S) = \left( \frac{1}{n} \sum_{w \in Ap(S, n)} w \right) - \frac{n - 1}{2}. \]

From this it is straightforward to prove the following result.

**Corollary 22 ([9, Theorem 12])** — Under the hypothesis of Theorem 19,

\[ \# \mathcal{H}(S, b) = \frac{b + 1 d - d'}{2}. \]

Given a numerical semigroup \( S \) define

\[ Pg(S) = \{x \in \mathbb{Z} \setminus S \mid n + s \in S \text{ for all } s \in S \setminus \{0\}\}. \]

The cardinality of the set \( Pg(S) \) is another important invariant of the numerical semigroup \( S \), known as the type of \( S \) and denoted by \( t(S) \) (see for instance [2]). We define in \( S \) the following order relation \( a \leq S b \) if \( b - a \in S \). Then by [6, Lemma 10], we can assert that if \( n \in S \setminus \{0\} \) and \( \{w_1, \ldots, w_t\} = \text{Maximals } S (Ap(S, n)) \), then \( Pg(S) = \{w_1 - n, \ldots, w_t - n\} \). It is well known (and easy to prove) that if \( w, w' \in Ap(S, n) \) and \( w - w' \in S \), then \( w - w' \in Ap(S, n) \).

**Example 23** — We compute the type of \( S(9, 30) \) by using the remark given above. Recall from Example 21 that

\[ Ap(S(9, 30), 15) = \{0, 7, 10, 11, 14, 17, 18, 20, 21, 24, 27, 28, 31, 34, 38\}. \]
Hence Maximals $\leq_{S(9, 30)} (Ap (S (9, 30), 15)) = \{34, 38\}$. Therefore $P_g(S(9, 30)) = \{19, 23\}$ and $t(S(9, 30)) = 2$.

Given a permutation $\sigma \in S_n$, define

$$J(\sigma) = \{i \in \{1, \ldots, n\} \mid \sigma(j) \leq \sigma(i) \text{ for all } j \in \{i, \ldots, n\}\}.$$  

Observe that if $(x_1, y_1), (x_2, y_2) \in A(a, b)$ and $(x_1, y_1) - (x_2, y_2) \in \mathbb{N}^2$, then $(x_1, y_1) - (x_2, y_2) \in A(a, b)$.

**Proposition 24** — Under the hypothesis of Theorem 19,

$$t(S(a, b)) \leq \#J\left(\frac{b}{d}, \frac{b}{d}\right).$$

**Proof:** Let $w \in Ap\left(S(a, b), \frac{b}{d}\right) \setminus \{0\}$. By Theorem 19, we know that there exists

$$k \in \left\{1, \ldots, \frac{b}{d}, 1\right\} \text{ and } \lambda \in \{0, \ldots, d - 1\} \text{ such that } w = dk + d' \sigma_{\frac{b}{dd'}}(k) + \lambda \frac{b}{d}.$$  

In order to prove this proposition, it suffices to show that if $w \in \text{Maximals } \leq_{S(a, b)} \left(Ap\left(S(a, b), \frac{b}{d}\right)\right)$, then $k \in J\left(\frac{b}{d}, \frac{b}{d}\right)$ and $\lambda = d - 1$. If $\lambda < d - 1$, then by Theorem 19, $w' = dk + d' \sigma_{\frac{b}{dd'}}(k) + (d - 1) \frac{b}{d} \in \left(Ap\left(S(a, b), \frac{b}{d}\right)\right)$ and $w - w' = (d - 1 - \lambda) \frac{b}{d} \in \{0\}$. Hence $w \notin \text{Maximals } \leq_{S(a, b)} \left(Ap\left(S(a, b), \frac{b}{d}\right)\right)$.

If $k \notin J\left(\frac{b}{d}, \frac{b}{d}\right)$, then there exists $\bar{k} \in \left\{k + 1, \ldots, \frac{b}{d}, 1\right\}$ such that $\sigma(\bar{k}) > \sigma(k)$. Note that by Proposition 12 and Corollary 4, we know that

$$\left(dk, d' \sigma_{\frac{b}{dd'}}(k)\right), \left(d\bar{k}, d' \sigma_{\frac{b}{dd'}}(\bar{k})\right) \in A(a, b).$$  

Moreover,

$$\left(d\bar{k}, d' \sigma_{\frac{b}{dd'}}(\bar{k})\right) \left(dk, d' \sigma_{\frac{b}{dd'}}(k)\right)$$  

$- \left(dk, d' \sigma_{\frac{b}{dd'}}(k)\right) \in \mathbb{N}^2$ and thus it also belongs to $A(a, b)$. Let $w' = dk + d' \sigma_{\frac{b}{dd'}}(k) + \lambda \frac{b}{d}$.

Then by Theorem 19 we know that $w' \in Ap\left(S(a, b), \frac{b}{d}\right)$ and from Theorem 1 we have that

$$w' - w \in S(a, b) \setminus \{0\}. \text{ Hence } w \notin \text{Maximals } \leq_{S(a, b)} \left(Ap\left(S(a, b), \frac{b}{d}\right)\right).$$

**Example 25** — In Example 18, one gets $J(\sigma_{10, 13}) = (9, 10, 11, 12)$. By Proposition 24, $t(S(56, 455)) \leq 4$. 

4. A FAMILY OF SYMMETRIC NUMERICAL SEMIGROUPS

A kind of semigroup of particular interest is that of symmetric numerical semigroups, which are those numerical semigroups with type one. Given a numerical semigroup \( S \), the least positive integer belonging to \( S \) is the multiplicity of \( S \) and it is denoted by \( m(S) \). If \( S \) is minimally generated by \( \{n_1 < n_2 < \ldots < n_e\} \), then clearly \( m(S) = n_1 \), the least minimal generator of \( S \).

We recall now a couple of known results that will be needed later.

**Lemma 26** ([9, Proposition 29]) — Let \( 2 \leq a < b \) be positive integers such that \( \gcd\{a, b\} = \gcd\{a - 1, b\} = 1 \). Then \( b = g(S(a, b)) + m(S(a, b)) \) and \( b \) is the greatest minimal generator of \( S(a, b) \).

**Lemma 27** ([9, Corollary 33]) — Let \( a < b \) be two positive integers. Then \( S(a, b) \setminus \{b\} \) is a symmetric numerical semigroup if and only if \( \gcd\{a, b\} = \gcd\{a - 1, b\} = 1 \).

In the literature there are several characterizations of symmetric numerical semigroups. The most extended is the following (which can be found for instance in [3]): a numerical semigroup is symmetric if and only if for every \( x \in \mathbb{Z} \setminus S \) we have that \( g(S) - x \in S \).

**Lemma 28** — Let \( S \) be a numerical semigroup with minimal system of generators \( \{n_1 < n_2 < \ldots < n_e\} \) and \( e \geq 3 \). If \( n_e = g(S) + n_1 \) and \( S \setminus \{n_e\} \) is a symmetric numerical semigroup, then \( S \setminus \{n_e\} \) is minimally generated by \( \{n_1, n_2, \ldots, n_{e-1}\} \).

**Proof**: It suffices to show that \( n_e + 1, n_e + 2, \ldots, n_e + n_1 \in \langle n_1, \ldots, n_{e-1} \rangle \). As \( n_e + 1, \ldots, n_e + (n_1 - 1) \in Ap(S, n_e) \), we have that \( n_e + 1, \ldots, n_e + (n_1 - 1) \in \langle n_1, \ldots, n_{e-1} \rangle \). Besides, by hypothesis \( n_e = g(S) + n_1 \), which implies that \( g(S \setminus \{n_e\}) = n_e \). Since \( n_2 - n_1 \in S \) (\( n_1 \) and \( n_2 \) are minimal generators), we have that \( n_2 - n_1 \in S \setminus \{n_e\} \), and thus \( n_e - (n_2 - n_1) = n_e + n_1 - n_2 \in S \setminus \{n_e\} \) (this is due to the fact that \( S \setminus \{n_e\} \) is symmetric). Hence there exist \( a_1, \ldots, a_e \in \mathbb{N} \) such that \( n_e + n_1 - n_2 = a_1 n_1 + a_2 n_2 + \ldots + a_e n_e \). We deduce that \( a_e = 0 \), since otherwise \( n_1 \) would not be a minimal generator. This leads to \( n_e + n_1 \in \langle n_1, \ldots, n_{e-1} \rangle \).

**Theorem 29** — Let \( 2 \leq t < b \) be two positive integers such that \( \gcd\{t, b\} = \gcd\{t + 1, b\} = 1 \). Then the semigroup generated by \( \{k + \sigma_{t, b}(k) \mid k \in \{1, \ldots, b - 1\}\} \) is a symmetric numerical semigroup with Frobenius number \( b \). Moreover \( e(S) \leq \# I(\sigma_{t, b}) \).
PROOF : By Lemma 27, it suffices to show that \( S = S(a, c) \setminus \{c\} \) for some positive integers \( a < c \) such that \( \gcd(a, c) = \gcd(a - 1, c) = 1 \). Set \( c = b \) and \( a = (t + 1)^{-1} \mod b \). Then \( \gcd(a, b) = 1 \) and \( (a - 1) + at \equiv 0 \mod b \). As \( \gcd(t, b) = 1 \), from the last congruence we deduce that \( \gcd(a - 1, b) = 1 \). By Theorem 19, we know that \( S(a, b) \) is generated by \( \{k + \sigma_{t,b}(k) \mid k \in \{1, \ldots, b - 1\}\} \cup \{b\} \), and in view of Lemma 26, we know that \( b = g(S(a, b)) + m(S(a, b)) \) and that \( b \) is the largest minimal generator of \( S(a, b) \). Moreover, since \( t \geq 2 \), we deduce that \( e(S(a, b)) \geq 3 \), because if there were only one minimal generator less than \( b \), then by using that \( \{b, \rightarrow\} \subseteq S(a, b) \) (the arrow means that all the integers greater than \( b \) are in the set) this would force the other generator to be 2. However, \( k + \sigma_{t,b}(k) = 2 \), implies \( k = 1 \) and \( t = 1 \), in contradiction with \( t \geq 2 \).

By using now Lemmas 27 and 28, we deduce that \( S = S(a, b) \setminus \{b\} \) is a symmetric numerical semigroup with Frobenius number \( b \). Finally, \( e(S) \leq \# I(\sigma_{t,b}) \) follows from Theorem 16 and Proposition 2.

\[ \square \]

**Example 30** : We construct a symmetric numerical semigroup with Frobenius number 13. Take \( t = 8 \) and \( b = 13 \) and let us use Theorem 29.

\[
\sigma_{8,13} = \begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\
8 & 3 & 11 & 6 & 1 & 9 & 4 & 12 & 7 & 2 & 10 & 5
\end{pmatrix}.
\]

\( I(\sigma_{8,3}) = \{1, 2, 5\} \) and thus \( S = \langle 9, 5, 6 \rangle \) is a symmetric numerical semigroup with Frobenius number 13.

**REFERENCES**


