MODULAR DIOPHANTINE INEQUALITIES AND NUMERICAL SEMIGROUPS

J. C. Rosales, P. A. García-Sánchez and J. M. Urbano-Blanco
MODULAR DIOPHANTINE INEQUALITIES AND NUMERICAL SEMIGROUPS

J. C. ROSALES, P. A. GARCÍA-SÁNCHEZ AND J. M. URBANO-BLANCO

We study the set of integer solutions to the modular diophantine inequality $ax \mod b \leq x$.

Introduction

Given $x \in \mathbb{Q}$, we set $\lfloor x \rfloor = \min \{ z \in \mathbb{Z} \mid z \geq x \}$ and $\lceil x \rceil = \max \{ z \in \mathbb{Z} \mid z \leq x \}$, as usual. Given integers $m, n$ with $n > 0$, we set $m \mod n = m - n \lfloor m/n \rfloor$ and $m \mod (-n) = m \mod n$. A modular diophantine inequality is an expression of the form $ax \mod b \leq x$ with $a, b$ integers such that $b \neq 0$. Since $ax \mod b \geq 0$, the set $S$ of solutions to such an inequality is contained in the set $\mathbb{N}$ of nonnegative integers. $S$ is a numerical semigroup, that is, $S$ is closed under addition, $0 \in S$ and $\mathbb{N} \setminus S$ is finite. Not every numerical semigroup arises from a modular diophantine inequality, and Section 2 presents a procedure for testing numerical semigroups for this property. Theorem 12 is crucial for obtaining this algorithm, and thus Section 1 is devoted to it. One of the main consequences of this theorem is that if the inequalities $ax \mod b \leq x$ and $cx \mod d \leq x$ have the same solutions, then

$$b - (a, b) - (a-1, b) = d - (c, d) - (c-1, d),$$

where $(x, y)$ denotes the greatest common divisor of the integers $x$ and $y$.

A numerical semigroup $S$ is said to be modular with modulus $b$ and factor $a$ if $S = \{ x \in \mathbb{N} \mid ax \mod b \leq x \}$. The preceding remark ensures that $b - (a, b) - (a-1, b)$ is an invariant of $S$, which we call the weight of $S$ and denote by $w(S)$.

If $S$ is a numerical semigroup, the largest integer not in $S$ is called the Frobenius number of $S$ and is denoted by $g(S)$. This integer has been widely studied; see for instance [Brauer 1942; Brauer and Shockley 1962; Johnson 1960; Selmer 1977; Sylvester 1884; Curtis 1990; Davison 1994; Djawadi and Hofmeister 1996]. In this direction it is worth highlighting [Ramírez Alfonsín 2000; ≥ 2005], where a review of this problem is given, with many references. In the literature one can also find a large number of publications devoted to the study of one-dimensional analytically

Supported by the project BFM2000-1469.


379
irreducible local domains via their value semigroups, which are numerical semigroups; see, for instance, [Apéry 1946; Barucci et al. 1997; Bertin and Carbonne 1977; Delorme 1976; Fröberg et al. 1987; Kunz 1970; Teissier 1973; Watanabe 1973]. As a consequence of this study, some interesting kinds of numerical semigroups arise, such as symmetric and pseudo-symmetric numerical semigroups. In Section 1 we prove that a modular numerical semigroup \( S \) is symmetric if and only if \( w(S) = g(S) \), and pseudo-symmetric if and only if \( g(S) = w(S) + 1 \). Sections 3 and 4 are devoted to modular numerical semigroups with modulus equal to their weight plus two and three, respectively. We show that those of weight plus two are obtained from a symmetric numerical semigroup by adjoining its Frobenius number to it, and that those with weight plus three arise from a pseudo-symmetric numerical semigroup by adding to it its Frobenius number and this number divided by two.

In Section 5 we study those modular numerical semigroups \( S \) such that the factor of \( S \) divides the modulus. For these numerical semigroups we can explicitly give formulas for the multiplicity, the minimal generator set, the Apéry set and the Frobenius number, so the case \( a | b \) is now well understood.

Section 6 addresses the problem of computing the Frobenius number in the complementary case \( a \nmid b \), solving it when \((a-1)(a - (b \mod a)) < b\). We have not been able to solve the general case.

### 1. Modular numerical semigroups

Let \( a \) and \( b \) be integers such that \( b \neq 0 \). Since \( ax \mod b = (a \mod b)x \mod b \) and \( ax \mod b = ax \mod (-b) \), in order to study the solutions of \( ax \mod b \leq x \), we can assume that \( b \) is a positive integer and that \( 0 \leq a < b \).

**Proposition 1.** The set of integer solutions of a modular diophantine inequality is a numerical semigroup.

**Proof.** Let \( a \) and \( b \) be two integers such that \( 0 \leq a < b \) and let \( S = \{ x \in \mathbb{N} \mid ax \mod b \leq x \} \). Clearly \( 0 \in S \), and if \( x \) is an integer greater than or equal to \( b \), then \( x \in S \). Hence \( \mathbb{N} \setminus S \) is finite. For \( x, y \in S \), we have \( a(x + y) \mod b \leq ax \mod b + ay \mod b \leq x + y \), whence \( x + y \in S \), so \( S \) is closed under addition. \( \square \)

A numerical semigroup \( S \) arising as in the proposition is said to be *modular*. The modular semigroup with modulus \( b \) factor \( a \) will be denoted by \( S(a, b) \); thus \( S(a, b) = \{ x \in \mathbb{N} \mid ax \mod b \leq x \} \). When we write \( S(a, b) \) we will generally assume tacitly that \( a \) and \( b \) are integers with \( 0 \leq a < b \).

**Example 2.** \( S(2, 3) = S(2, 4) = \{ 0, 2, 3, \rightarrow \} \), where \( \rightarrow \) means that all the elements beyond 3 are in the set. Thus \( a \) and \( b \) don’t have to be unique.
Let $S$ be a modular numerical semigroup with modulus $b$. Suppose $x$ and $b$ are both in $S$ if and only if $b+1-a)x$ mod $b \leq x$. The converse follows by interchanging $a$ with $b+1-a$.

**Lemma 3.** Let $a$ and $b$ be integers such that $0 \leq a < b$. Then $ax$ mod $b \leq x$ if and only if $(b+1-a)x$ mod $b \leq x$.

**Proof.** If $ax$ mod $b \leq x$, there exist $q, r \in \mathbb{N}$ such that $ax = qb + r$ with $0 \leq r \leq x$. Hence $(b+1-a)x = (b+1)x - ax = bx - qbx + r$ and $(b+1-a)x$ mod $b \leq x - r \leq x$. The converse follows by interchanging $a$ with $b+1-a$.

**Lemma 4.** Let $S$ be a modular numerical semigroup with modulus $b \geq 2$. Then there exists a positive integer $a$ such that $a \leq \frac{1}{2}(b+1)$ and $S = S(a, b)$.

**Proof.** Write $S = S(a, b)$ with $0 \leq a < b$. By Lemma 3, $S = S(b+1-a, b)$, so if $a > \frac{1}{2}(b+1)$ we can replace $a$ by $b+1-a \leq \frac{1}{2}(b+1)$. Also if $a = 0$ we can replace it by $a = 1$, since $S = \mathbb{N}$ for both these values of $a$.

**Lemma 5.** Let $a$ and $b$ be integers such that $0 \leq a < b$ and let $x \in \mathbb{N}$. Then

$$a(b-x) \mod b = \begin{cases} 0 & \text{if } ax \mod b = 0, \\ b - (ax \mod b) & \text{if } ax \mod b \neq 0, \end{cases}$$

and $ax$ mod $b > x$ implies that $a(b-x)$ mod $b < b - x$.

**Corollary 6.** If $S = S(a, b)$ and $x \in \mathbb{N} \setminus S$, then $b - x \in S$.

Given a subset $A$ of $\mathbb{N}$, we denote by $H(A)$ the complement $\mathbb{N} \setminus A$, and by $\langle A \rangle$ the submonoid of $\mathbb{N}$ generated by $A$ (the set of finite sums of elements of $A$).

**Remark 7.** If $S = S(a, b) \neq \mathbb{N}$ for positive $a$ and $b$, then $b-1 \notin H(S)$, since otherwise $b - (b-1) = 1$ would be an element of $S$. Moreover $x \in S$ for all integers $x \geq b$. Therefore the Frobenius number $g(S)$ is at most $b-2$.

We now characterize the case $g(S) = b-2$. If $g(S) = b-2$, Corollary 6 implies that $b - (b-2) = 2 \in S$. Hence $b$ is odd and $S = \langle 2, b \rangle$. In addition, since $2 \in S$, $2a$ mod $b \leq 2$ and this leads to $2a > b$, whence $a > \frac{1}{2}b$. But Lemma 4 says we can take $a \leq \frac{1}{2}(b+1)$, which then means $a = \frac{1}{2}(b+1)$. Hence $S = S(\frac{1}{2}(b+1), b)$. Conversely, if $S = S(\frac{1}{2}(b+1), b)$ with $b$ odd, it is easy to check that $S = \langle 2, b \rangle$ and thus $g(S) = b-2$.

**Example 8.** Suppose $b \geq 2$ and $S = S(2, b)$. Then $S = \{0, \lfloor \frac{1}{2}(b+1) \rfloor \}$, for clearly $\{b, \rightarrow \} \subseteq S$. Now take $0 < x < b$. Then $x \in S$ if and only if $2x$ mod $b \leq x$. However, $2x$ mod $b = 2x$ if and only if $2x < b$, and thus in this case $x \notin S$. If $2x \geq b$, then $2x$ mod $b = 2x - b \leq x$, whence $x \in S$.

**Lemma 9.** Let $S = S(a, b)$ and let $x$ be an integer such that $0 \leq x \leq b$. Then $x$ and $b-x$ are both in $S$ if and only if $ax$ mod $b \in \{0, x\}$.
Lemma 10. Let $a$ and $b$ be positive integers and $x$ an integer such that $0 \leq x < b$.

1. $ax \mod b = 0$ if and only if $x$ is a multiple of $b/(a, b)$.
2. $ax \mod b = x$ if and only if $x$ is a multiple of $b/(b, a-1)$.

Lemma 11. Let $S = S(a, b)$ with $0 < a < b$. Let $\alpha = (b, a-1)$ and $\beta = (b, a)$, and let $x$ be an integer such that $0 \leq x < b$. Then

$$\{x, b-x\} \subset S \iff x \in \left\{0, \frac{b}{\alpha}, \frac{b}{\alpha} \cdots (\alpha-1) \frac{b}{\alpha}, \frac{b}{\beta}, \frac{b}{\beta} \cdots (\beta-1) \frac{b}{\beta}, b\right\} =: X.$$  

The cardinality of $X$ is $\alpha + \beta$.

Proof. The equivalence is just Lemmas 9 and 10 put together. To show there is no duplication in the elements of $X$ as written, note that $(\alpha, \beta) = 1$. If $sb/\alpha = tb/\beta$ for some $s, t \in \mathbb{N}$, then $s\beta = t\alpha = k\alpha \beta$ for some $k \in \mathbb{N}$. Hence $s = k\alpha$ and $t = k\beta$. □

Theorem 12. Let $S = S(a, b)$ for some integers $0 \leq a < b$. Then

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

Here as usual $\#$ denotes cardinality.

Proof. Let $\alpha$, $\beta$ and $X$ be as in Lemma 11. By Corollary 6 and Lemma 11, for $0 \leq x \leq b$, at most one of $x, b-x$ lies in $H(S)$, and it’s exactly one unless $x \in X$. Thus $\# H(S) = \frac{1}{2}(b+1 - \# X) = \frac{1}{2}(b+1 - \alpha - \beta)$. □

Example 13. If $p$ is an odd prime, $\# H(S(a, p)) = \frac{1}{2}(p-1)$ for all $a$ with $1 < a < p$.

As an immediate consequence of Theorem 12 we obtain:

Corollary 14. Suppose $S(a, b) = S(c, d)$. Then

$$b - (a, b) - (a-1, b) = d - (c, d) - (c-1, d).$$  

Example 15. The converse of Corollary 14 is false. For instance, $(4, 5, 6) = S(3, 12) \neq S(2, 10) = (5, 6, 7, 8, 9)$.

Recall that we have defined the weight of $S = S(a, b)$ as $w(S) := b - (a, b) - (a-1, b)$; by Theorem 12, this number equals $2 \# H(S) - 1$, and so is an invariant of $S$. Note that $w(\mathbb{N}) = -1$. If $S \neq \mathbb{N}$, we can choose $a, b$ with $2 \leq a < b$; hence $(a, b) + (a-1, b) \leq \frac{1}{2}b + \frac{1}{2}b < b$, so $w(S) \geq 1$. Thus, like the Frobenius number, the
weight of a modular numerical semigroup is at least 1, except for the case $S = \mathbb{N}$, where $w(S) = g(S) = -1$.

Theorem 12 and the inequality $\# H(S) \geq \frac{1}{2}(g(S) + 1)$, valid for any numerical semigroup $S$ (see [Fröberg et al. 1987], for instance), yield:

**Corollary 16.** If $S$ is a modular numerical semigroup, then $w(S)$ is odd and greater than or equal to $g(S)$. \hfill $\square$

In view of this, modular numerical semigroups $S$ with $w(S) = g(S)$ and $g(S)$ odd, or with $w(S) = g(S) + 1$ and $g(S)$ even, have minimal possible weight with respect to their Frobenius numbers. The next result characterizes this kind of numerical semigroup, but before proving it we need to recall some concepts.

A numerical semigroup $S$ is **symmetric** if $x \in \mathbb{N} \setminus S$ implies $g(S) - x \in S$. It is straightforward to prove that a symmetric numerical semigroup has odd Frobenius number. A numerical semigroup is **pseudo-symmetric** if $g(S)$ is even and $x \in \mathbb{N} \setminus S$ implies that either $x = g(S)/2$ or $g(S) - x \in S$. A numerical semigroup $S$ is symmetric if and only if $\# H(S) = \frac{1}{4}(g(S) + 1)$, and pseudo-symmetric if and only if $\# H(S) = \frac{1}{2}(g(S) + 2)$; see [Fröberg et al. 1987], for instance.

A numerical semigroup is **irreducible** if it cannot be expressed as the intersection of two numerical semigroups containing it properly. In [Rosales and Branco 2003] it is shown that $S$ is irreducible if and only if $S$ is symmetric or pseudo-symmetric (depending on the parity of $g(S)$).

**Corollary 17.** Let $S$ be a modular numerical semigroup.

1. $S$ is symmetric if and only if $w(S) = g(S)$.
2. $S$ is pseudo-symmetric if and only if $w(S) = g(S) + 1$.

**Proof.** $S$ is symmetric if and only if $\# H(S) = \frac{1}{2}(g(S) + 1)$. By Theorem 12, $\# H(S) = \frac{1}{2}(w(S) + 1)$, whence $S$ is symmetric if and only if $g(S) = w(S)$. The proof of (2) is analogous. \hfill $\square$

**Example 18.** If $b$ is an odd integer, there exists a modular numerical semigroup $S$ with $w(S) = b$. It suffices to take $S = S(2, b+2)$, since $w(S(2, b+2)) = b + 2 - (2, b + 2) - (1, b + 2) = b + 2 - 1 - 1 = b$.

**2. Determining whether a numerical semigroup is modular**

In this section we give a procedure for deciding whether a given numerical semigroup is a modular numerical semigroup, and if so to express it in the form $S(a, b)$.

**Lemma 19.** Let $S$ be a modular numerical semigroup with modulus $b$ and $S \neq \mathbb{N}$. Then $b \leq 12 \# H(S) - 6$.

**Proof.** As we saw right after Example 15, if $a \geq 2$ we have $(a, b) + (a-1, b) \leq \frac{5}{6}b$. By Theorem 12, $\# H(S) \geq \frac{1}{2}(b + 1 - \frac{5}{6}b)$ and thus $b \leq 12 \# H(S) - 6$. \hfill $\square$
For a numerical semigroup $S$, the multiplicity of $S$, denoted by $m(S)$, is the least positive integer in $S$. Here is an immediate consequence of Lemma 11:

**Lemma 20.** For $S = S(a, b)$,

$$b - m(S) \in S \iff m(S) = \min \left\{ \frac{b}{(a, b)}, \frac{b}{(a-1, b)} \right\}.$$ 

**Lemma 21.** Let $S$ be a modular numerical semigroup with modulus $b$. Then

$$b \geq g(S) + m(S).$$

*Proof.* Since 1, 2, …, $m(S) - 1$ are not in $S$, Corollary 6 ensures that $b - m(S) + 1, \ldots, b - 1$ are. But $\{b, m(S)\} \subset S$, so $\{b - m(S) + 1, \ldots\} \subset S$. This implies that $g(S) \leq b - m(S)$. □

**Lemma 22.** For $S = S(a, b)$,

$$b = g(S) + m(S) \iff m(S) \neq \min \left\{ \frac{b}{(a, b)}, \frac{b}{(a-1, b)} \right\}.$$ 

*Proof.* Follows from Lemmas 20 and 21. □

Now we have all the ingredients to give the algorithm announced at the start of this section, to decide whether a numerical semigroup is of the form $S(a, b)$, and if so, produce such a pair $(a, b)$ (or all such pairs with $a \leq \frac{1}{2}(b + 1)$, if the algorithm is not stopped after the first pair is found).

**Algorithm 23.** Given a numerical semigroup $S$ distinct from $\mathbb{N}$:

1. Compute $\# H(S)$, $g(S)$ and $m(S)$.
2. Set $b = g(S) + m(S)$.
3. For every $a \in A := \left\{ a \in \mathbb{N} \middle| \begin{align*} 2 \leq a &\leq \frac{1}{2}(b + 1), \\
&b = 2 \# H(S) + (a, b) + (a-1, b) - 1, \\
m(S) &< \min\{b/(a, b), b/(a-1, b)\} \end{align*} \right\}$

compute $S(a, b)$; if $S = S(a, b)$, return this answer and stop.
4. Compute $B = \{b \in (k \cdot m(S) \mid k \in \mathbb{N}) \mid 2 \# H(S) + 1 \leq b \leq 12 \# H(S) - 6\}$.
5. For every $b \in B$

for every $a \in A_b := \left\{ a \in \mathbb{N} \middle| \begin{align*} 2 \leq a &\leq \frac{1}{2}(b + 1), \\
&b = 2 \# H(S) + (a, b) + (a-1, b) - 1, \\
m(S) = \min\{b/(a, b), b/(a-1, b)\} \end{align*} \right\}$

compute $S(a, b)$; if $S = S(a, b)$, return this answer and stop.
6. Return “$S$ is not modular”.
We briefly justify the correctness of Algorithm 23. In Steps (2) and (3) we check whether \( S \) is a modular numerical semigroup with modulus \( g(S) + m(S) \), and the correct working of these steps relies on Lemmas 4 and 22 and Theorem 12. If \( S \) is not a modular numerical semigroup with modulus \( g(S) + m(S) \), Lemma 22 gives \( m(S) = \min\{b/(a, b), b/(a−1, b)\} \). This implies that \( m(S) \) divides \( b \). Theorem 12 states that \( b = 2 \# H(S) + (a, b) + (a−1, b)−1 \), so \( b \geq 2 \# H(S) + 1 \); at the same time \( b \leq 12 \# H(S) - 6 \) by Lemma 19. Therefore Steps (4) and (5) cover the case \( b \neq g(S) + m(S) \).

**Example 24.** Let \( S = \langle 3, 5 \rangle \). Then \( \# H(S) = 4 \), \( g(S) = 7 \) and \( m(S) = 3 \). In Step (2) we get \( b = 10 \). Step (3) yields \( A = \{2, 3, 4\} \), then \( S(2, 10) = \langle 5, 6, 7, 8, 9 \rangle \), \( S(3, 10) = \langle 4, 5, 7 \rangle \), and \( S(4, 10) = \langle 3, 5 \rangle = S \), so the algorithm returns \( S = S(4, 10) \).

**Example 25.** Let \( S = \langle 3, 8, 10 \rangle \). In this case \( \# H(S) = 5 \), \( g(S) = 7 \) and \( m(S) = 3 \). In Step (2) we obtain \( b = 10 \) and in Step (3), \( A = \emptyset \). The only nonempty set \( A_b \) with \( b \in B \) is \( A_{15} = \{5\} \). Since \( S \neq S(5, 15) = \langle 3, 7, 11 \rangle \), the algorithm returns No.

**Example 26.** Let \( S = \langle 10, 11, 12 \rangle \). Then \( \# H(S) = 25 \), \( g(S) = 49 \) and \( m(S) = 10 \). In Step (2) we obtain \( b = 59 \) and \( A \) is empty. Computing \( B \), we obtain

\[
B = \{60, 70, 80, 90, 100, 110, 120, 130, 140, 150, 160, 170, 180, 190, 200, 210, 220, 230, 240, 250, 260, 270, 280, 290\}.
\]

The only nonempty set \( A_b \) with \( b \in B \) is \( A_{60} = \{6\} \). It turns out that \( S = S(6, 60) \).

**Remark 27.** If the input to Algorithm 23 is known to be symmetric, the procedure can be improved, because if \( S = S(a, b) \) is symmetric then \( b \) must be equal to \( g(S) + (a, b) + (a−1, b) \) (note that \( g(S) = g(S) \) by Corollary 17). A similar argument applies to the pseudo-symmetric case.

**Remark 28.** The intersection \( \bigcap_{i=1}^{n} S(a_i, b_i) \) of \( n \geq 1 \) modular numerical semigroups is a numerical semigroup; it need not be modular, as can be seen from Example 25, since we can write \( \langle 3, 8, 10 \rangle = \langle 3, 4 \rangle \cap \langle 3, 5 \rangle = S(3, 8) \cap S(4, 10) \).

Nor can every numerical semigroup be written as such an intersection: for instance, \( \langle 7, 8, 10, 13 \rangle \) is a symmetric, hence irreducible, numerical semigroup; thus it cannot be an intersection of modular numerical semigroups other than by being itself a modular numerical semigroup. Algorithm 23 says that it is not.

### 3. Modular numerical semigroups whose modulus is its weight plus two

We now study modular numerical semigroups \( S = S(a, b) \) whose modulus \( b \) equals \( w(S)+2 \). Since \( b = w(S)+(a, b)+(a−1, b) \geq w(S)+2 \), the condition \( b = w(S)+2 \) is equivalent to \( (a, b) = (a−1, b) = 1 \) (so \( b \) is odd), and it characterizes modular numerical semigroups whose moduli are minimal with respect to their weights.
Every numerical semigroup $S$ is finitely generated (as an additive monoid). This is easy to see — for instance, start with two relatively prime $r, s \in S$ and then adjoin all elements of $S \cap \{0, 1, \ldots, rs - 1\}$ as yet unaccounted for. Among all generating sets one can of course choose one that is minimal, say $\mathcal{M}(S)$. A minute’s thought shows that $\mathcal{M}(S)$ is characterized by containing exactly those nonzero elements of $S$ that cannot be expressed as a sum of two nonzero elements of $S$:

$$\mathcal{M}(S) = (S \setminus \{0\}) \setminus ((S \setminus \{0\}) + (S \setminus \{0\})),$$

In particular, $\mathcal{M}(S)$ is unique. We set $e(S) = \#\mathcal{M}(S)$ and call this number the embedding dimension of $S$; the elements of $\mathcal{M}(S)$ are called minimal generators.

**Proposition 29.** Let $S = S(a, b)$ with $2 \leq a < b$ and $(a, b) = (a-1, b) = 1$. Then

1. $b = g(S) + m(S),$
2. $\# \mathcal{H}(S) = \frac{1}{2}(g(S) + m(S) - 1),$
3. $b$ is the largest minimal generator of $S$.

**Proof.** (1) We already know that $b-1 \in S$ when $2 \leq a < b$. Hence $m(S) \neq b$. Using Lemma 22, we get $b = g(S) + m(S)$.

(2) Immediate from Theorem 12.

(3) First we prove that $b$ is a minimal generator of $S$. Assume to the contrary that $b = x + y$ with $x, y \in S \setminus \{0\}$. Then $ax \mod b \leq x$ and $ay \mod b \leq y$, and thus $(ax \mod b) + (ay \mod b) \leq x + y = b$. Since $a(x + y) \mod b = ab \mod b = 0$, we deduce that $(ax \mod b) + (ay \mod b) \in \{0, b\}$. Thus either $ax \mod b = x$ and $ay \mod b = y$, or $ax \mod b = 0$ and $ay \mod b = 0$. These two cases contradict the two halves of Lemma 10.

To see that $b$ is the largest minimal generator, take $x \in S$ with $x > b$. By applying (1) we obtain $x > g(S) + m(S)$, which implies that $x - m(S) > g(S)$; this forces $x - m(S) \in S$. Thus $x = m(S) + (x - m(S))$ cannot be a minimal generator of $S$. □

Proposition 29 allows us to relate the modular numerical semigroups in question with unitary extensions of symmetric numerical semigroups or UESY-semigroups in short. A numerical semigroup $S$ is a UESY-semigroup if there exists a symmetric numerical semigroup $S'$ such that $S' \subset S$ and $\#(S \setminus S') = 1$. In [Rosales ≥ 2005b] this condition is shown to be equivalent to the existence of a symmetric numerical semigroup $S'$ such that $S = S' \cup \{g(S')\}$. The following result also appears there.

**Proposition 30.** Let $S$ be a numerical semigroup, $S \neq \mathbb{N}$. The following conditions are equivalent:

1. $S$ is a UESY-semigroup.
2. $\# \mathcal{H}(S) = \frac{1}{2}(g(S) + m(S) - 1)$ and $g(S) + m(S)$ is a minimal generator of $S$. □
A pseudo-Frobenius number [Rosales and Branco 2002] of a numerical semigroup $S$ is an integer $x \notin S$ such that $x + s \in S$ for all $s \in S \setminus \{0\}$. The set of pseudo-Frobenius numbers of $S$ is denoted by $Pg(S)$, and its cardinality, called the type of $S$, is denoted by $t(S)$. Clearly $g(S) \in Pg(S)$. Moreover $S$ is symmetric if and only if $Pg(S) = \{g(S)\}$, and $S$ is pseudo-symmetric if and only if $Pg(S) = \{g(S), \frac{1}{2}g(S)\}$; see [Barucci et al. 1997; Fröberg et al. 1987], for instance.

In [Rosales $\geq$ 2005b] it is proved that if $S$ is a UESY-semigroup distinct from $\mathbb{N}$, then $t(S) = e(S) - 1$. This, plus Propositions 29 and 30, gives:

**Corollary 31.** Let $S = S(a, b)$ be such that $2 \leq a < b$ and $(a, b) = (a - 1, b) = 1$. Then $t(S) = e(S) - 1$ and there exists a symmetric numerical semigroup $S'$ such that $S = S' \cup \{g(S')\}$. \(\square\)

**Theorem 32.** Let $S = S(a, b)$. Then $b = w(S) + 2$ if and only if $S$ is a UESY-semigroup and $b$ is a minimal generator of $S$.

*Proof.* If $b = w(S) + 2 = b - (a, b) - (a - 1, b) + 2$, we deduce $(a, b) = (a - 1, b) = 1$. Corollary 31 then says that $S$ is a UESY-semigroup, and Proposition 29 that $b$ is a minimal generator of $S$.

Conversely, if $b$ is a minimal generator of $S$ it equals $g(S) + m(S)$, by Lemma 21 and the fact, shown in the proof of Proposition 29, that a minimal generator of $S$ cannot exceed $g(S) + m(S)$. If $S$ is a UESY, then $\#H(S) = \frac{1}{2}(g(S) + m(S) - 1)$ by Proposition 30 and $\#H(S) = \frac{1}{2}(w(S) + 1)$ by Theorem 12. Thus $b = w(S) + 2$. \(\square\)

**Corollary 33.** Let $S$ be a modular numerical semigroup with modulus $b$. Then $b = w(S) + 2$ if and only if $S \setminus \{b\}$ is a symmetric numerical semigroup. Therefore, if $b$ is a prime integer, $S \setminus \{b\}$ is a symmetric numerical semigroup.

*Proof.* If $b = w(S) + 2$, Theorem 32 says $b$ is a minimal generator of $S$, so $S' = S \setminus \{b\}$ is a numerical semigroup with $g(S') = b$. By Corollary 6, $S'$ is symmetric.

Conversely, if $S \setminus \{b\}$ is a symmetric numerical semigroup, then $S$ is a UESY-semigroup with $b$ as a minimal generator. Now Theorem 32 gives $b = w(S) + 2$.

Finally, $b$ prime implies $(a, b) = (a - 1, b) = 1$, so $w(S) = b - 2$. \(\square\)

**Corollary 34.** Let $b \geq 3$ be an integer. Then $b$ is prime if and only if $b$ is the largest minimal generator of $S(a, b)$ for every $a$ such that $2 \leq a \leq \sqrt{b}$.

*Proof.* If $b$ is prime Proposition 29 applies; this proves one direction. Conversely, suppose $b$ is not a prime — say $b = ac$ with integers $a, c \geq 2$ and $a \leq \sqrt{b}$. For $S = S(a, b)$, we have $ac \mod b = 0$ and thus $c \in S$. But then $b = ac$ cannot be a minimal generator of $S$. \(\square\)

4. Modular numerical semigroups whose modulus is its weight plus three

We now study modular numerical semigroups $S = S(a, b)$ such that $b = w(S) + 3$; this condition is equivalent to $(a, b) + (a - 1, b) = 3$. There are two cases:
\begin{itemize}
  \item \((a, b) = 1\) and \((a - 1, b) = 2\).
  \item \((a, b) = 2\) and \((a - 1, b) = 1\).
\end{itemize}

In both situations \(b\) must be even and by Corollary 6 we deduce that \(\frac{1}{2}b \in S\).

Let \(S\) be a numerical semigroup with minimal generating set \(\{n_1, \ldots, n_p\}\). We say that \(x \in S\) has a unique expression if the equality \(x = a_1n_1 + \cdots + a pn_p\), with \(a_1, \ldots, a_p \in \mathbb{N}\), determines \(a_1, \ldots, a_p\) uniquely.

**Proposition 35.** Let \(S = S(a, b)\) be such that \(2 \leq a < b\) and \((a, b) + (a - 1, b) = 3\).

1. \(m(S) \neq \frac{1}{2}b\) \(\iff\) \(S \neq \{0, \frac{1}{2}b, \rightarrow\}\) \(\iff\) \(b = g(S) + m(S) \iff\) \(#H(S) = \frac{g(S) + m(S) - 2}{2}\).

2. \(\frac{1}{2}b\) is a minimal generator of \(S\).

3. \(b\) has a unique expression in \(S\).

**Proof.** (1) Follows easily from Corollary 6, Lemma 22 and Theorem 12.

(2) Suppose \(x + y = \frac{1}{2}b\) with \(x, y \in S\). Then \(ax \mod b \leq x\) and \(ay \mod b \leq y\), whence \(ax \mod b + ay \mod b \leq x + y = \frac{1}{2}b\). Thus \(\frac{1}{2}ab \mod b = a(x + y) \mod b = ax \mod b + ay \mod b\). We must show that \(x = 0\) or \(y = 0\). We distinguish two cases. If \((a, b) = 2\), then \(\frac{1}{2}ab \mod b = 0\), so \(ax \mod b = 0\) and \(ay \mod b = 0\); then Lemma 10 shows that both \(x\) and \(y\) are multiples of \(\frac{1}{2}b\), which leads to the desired conclusion. Similarly, if \((a - 1, b) = 2\), then \(\frac{1}{2}ab \mod b = \frac{1}{2}b\), so \(ax \mod b = x\) and \(ay \mod b = y\); Lemma 10 again shows that \(x\) and \(y\) are multiples of \(\frac{1}{2}b\).

(3) We prove that if \(x, y \in S \setminus \{0\}\) are such that \(x + y = b\), then \(x = y = \frac{1}{2}b\). Arguing as in the proof of Proposition 29(3), we see that either \((ax \mod b, ay \mod y) = (x, y)\) or \(ax \mod b = ay \mod y = 0\). Lemma 10 implies that \(x\) and \(y\) are both multiples of \(\frac{1}{2}b\), and since \(x \neq 0 \neq y\), we conclude that \(x = y = \frac{1}{2}b\).

Paralleling what we did in Section 3 for the case \(b = w(S) + 2\), we can use Proposition 35 to relate modular numerical semigroups such that \(b = w(S) + 3\) with a previous studied class of numerical semigroups. A numerical semigroup \(S\) is called a **PESPY-semigroup** if there exists a pseudo-symmetric numerical semigroup \(S'\) such that \(S = S' \cup \left\{\frac{1}{2}g(S'), g(S')\right\}\) (the two additional elements are the pseudo-Frobenius numbers of \(S'\); see [Barucci et al. 1997; Fröberg et al. 1987]).

Numerical semigroups of the form \(\{0, x, \rightarrow\}\) with \(x\) a positive integer are called **intervals**. The following result appears in [Rosales \(\geq 2005a\)].

**Proposition 36.** Let \(S\) be a numerical semigroup that is not an interval. The following conditions are equivalent:

1. \(S\) is a PESPY-semigroup.

2. \(#H(S) = \frac{1}{2}(g(S) + m(S) - 2)\), \(\frac{1}{2}(g(S) + m(S))\) is a minimal generator of \(S\) and \(g(S) + m(S)\) is an element of unique expression of \(S\).
The next result is an immediate consequence of Propositions 35 and 36.

**Corollary 37.** Let \( S = S(a, b) \) be such that \( 2 \leq a < b \), \((a, b) + (a-1, b) = 3 \) and \( S \) is not an interval. Then \( S \) is a PEPSY-semigroup.

In [Rosales \( \geq 2005a \)] it is proved that if \( S \) is a PEPSY-semigroup that is not an interval, then \( t(S) = e(S) - 1 \). Thus:

**Corollary 38.** Let \( S = S(a, b) \) be such that \( 2 \leq a < b \), \((a, b) + (a-1, b) = 3 \) and \( S \) is not an interval. Then \( t(S) = e(S) - 1 \).

**Remark 39.** Among numerical semigroups, interval semigroups have maximal embedding dimension relative to multiplicity: \( e(S) = m(S) \). For any numerical semigroup with maximal embedding dimension, \( t(S) = m(S) - 1 = e(S) - 1 \) (see [Barucci et al. 1997], for instance). Hence the assumption “\( S \) is not an interval” can be dropped from Corollary 38.

**Theorem 40.** Assume that \( S = S(a, b) \) is not an interval. Then \( b = w(S) + 3 \) if and only if \( S \) is a PEPSY-semigroup, \( \frac{1}{2}b \) is a minimal generator of \( S \) and \( b \) has a unique expression in \( S \).

**Proof.** Necessity follows from Corollary 37 and Proposition 35. Sufficiency: Lemma 21 says that \( b \geq g(S) + m(S) \). If \( b > g(S) + m(S) \), then \( m(S) + (b - m(S)) \) and \( \frac{1}{2}b + \frac{1}{2}b \) are distinct expressions for \( b \) in \( S \) (\( m(S) \neq \frac{1}{2}b \) since otherwise \( S \) is an interval, by Corollary 6). Therefore \( b = g(S) + m(S) \). By Proposition 36, we know that \( \# H(S) = \frac{1}{2}(g(S) + m(S) - 2) \) and Theorem 12 ensures that \( \# H(S) = \frac{1}{2}(w(S) + 1) \), whence \( b = g(S) + m(S) = w(S) + 3 \).

**Corollary 41.** Let \( S \) be a modular numerical semigroup with modulus \( b \). Then \( b = w(S) + 3 \) if and only if \( S \setminus \left\{ \frac{1}{2}b, b \right\} \) is a pseudo-symmetric numerical semigroup. Therefore, if \( b = 2p \) and \( a < p \) for some positive prime \( p \), then \( S \setminus \left\{ \frac{1}{2}b, b \right\} \) is a pseudo-symmetric numerical semigroup.

**Proof.** Suppose \( b = w(S) + 3 \). By Theorem 40, \( \frac{1}{2}b \) is a minimal generator of \( S \) and \( b \) has a unique expression in \( S \). This implies that \( S' = S \setminus \left\{ \frac{1}{2}b, b \right\} \) is a numerical semigroup, and clearly \( g(S') = b \). Using Corollary 6 we can easily deduce that \( S' \) is pseudo-symmetric.

Conversely, if \( S \setminus \left\{ \frac{1}{2}b, b \right\} \) is a pseudo-symmetric numerical semigroup, then \( S \) is a PEPSY-semigroup by definition, \( \frac{1}{2}b \) is a minimal generator of \( S \) and \( b = \frac{1}{2}b + \frac{1}{2}b \) is the unique expression of \( b \) in \( S \). Thus \( b = w(S) + 3 \) by Theorem 40.

5. When the factor divides the modulus

We next focus on numerical semigroups of the form \( S = S(a, ab) \), where we may as well assume \( a, b > 1 \). First a general definition: given a numerical semigroup
Corollary 45. Let $S$ and $n \in S \setminus \{0\}$, the Apéry set of $n$ in $S$ [Apéry 1946] is
\[
\text{Ap}(S, n) = \{ s \in S \mid s - n \notin S \}.
\]
This set always has $n$ elements $w(0) = 0$, $w(1)$, $\ldots$, $w(n-1)$, where $w(i)$ is the least element congruent to $i$ modulo $n$. Note also that $x \in \mathbb{Z}$ is an element of $S$ if and only if $x \geq w(x \mod n)$. Consequently
\[
(*) \quad g(S) = \max(\text{Ap}(S, n)) - n.
\]
The following result is a consequence of [Rosales 1996, Lemma 3.3] and gives a characterization of Apéry sets which will be useful later.

**Lemma 42.** Let $m > 0$ be an integer and let $X = \{0 = w(0), w(1), \ldots, w(m-1)\}$ be a subset of $\mathbb{N}$ such that $i < w(i) \equiv i \mod m$ for all $i \in \{1, \ldots, m-1\}$. Let $S$ be the submonoid of $\mathbb{N}$ generated by $X \cup \{m\}$. Then $S$ is a numerical semigroup with multiplicity $m$. Moreover, $\text{Ap}(S, m) = X$ if and only if for all $i, j \in \{1, \ldots, m-1\}$ there exist $k \in \{0, \ldots, m-1\}$ and $t \in \mathbb{N}$ such that $w(i) + w(j) = w(k) + tm$. \hfill \Box

Getting back to $S = S(a, ab)$, with $a, b > 1$, we will give a description of the particular Apéry set $\text{Ap}(S, m(S))$ in terms of $a, b$, and this will lead to an explicit formula for the Frobenius number of $S$. We also show how the minimal generating set for such numerical semigroups can be computed from $a$ and $b$ as well as the corresponding sets of pseudo-Frobenius numbers.

**Lemma 43.** $m(S(a, ab)) = b$.

**Proof.** Let $S = S(a, ab)$ and let $x \in \{1, \ldots, b-1\}$. Then $ax < ab$ and thus $ax \mod ab = ax > x$, whence $x \notin S$. Clearly $b \in S$ and consequently $m(S) = b$. \hfill \Box

**Theorem 44.** $\text{Ap}(S(a, ab), b) = \{0, k_1 b + 1, k_2 b + 2, \ldots, k_{b-1} b + b-1\}$, where $k_i = [(a-1)i/b]$ for all $i \in \{1, \ldots, b-1\}$.

**Proof.** Let $S'$ be the semigroup generated by $\{b, k_1 b + 1, \ldots, k_{b-1} b + b-1\}$. Since $k_i \geq 1$ for all $i \in \{1, \ldots, b-1\}$ we have $m(S') = b$. Clearly $k_1 \leq \cdots \leq k_{b-1}$ and $k_i + k_j \geq k_{i+j}$ for all $i, j \in \{1, \ldots, b-1\}$ with $2 \leq i + j \leq b-1$. Using Lemma 42, we deduce that $\text{Ap}(S', b) = \{0, k_1 b + 1, \ldots, k_{b-1} b + b-1\}$. Recall that $x \in \mathbb{Z}$ belongs to $S'$ if and only if $x \geq k_x \mod b + x \mod b$, since this latter number is the element in $\text{Ap}(S', b)$ that is congruent to $x$ modulo $b$. So, for $x$ an integer we have $x \in S' \iff [x/b] \geq k_x \mod b \iff [x/b] \geq [(a-1)(x \mod b)/b] \iff [x/b] \geq (a-1)(x \mod b)/b \iff [x/b] \geq (a-1)(x \mod b) \iff x - (x \mod b) \geq (a-1)(x \mod b) \iff a(x \mod b) \leq x \iff ax \mod ab \leq x$. Thus $S' = S(a, ab)$. \hfill \Box

Using this result and equality $(*)$ with $n = m(S)$, we obtain:

**Corollary 45.** $g(S(a, ab)) = [(b-1)(a-1)/b] b - 1$. 
Let \( S \)

\[(ii) \text{ Let } i, k \text{ is a minimal generator of } S. \]

which is impossible in view of (†), since

\[\{i \mid (a-1)i \equiv 0 \mod b \} \ni \{i \mid (a-1)i \equiv 0 \mod b \}. \]

Thus

\[\text{Proof.} \]

\[(iii) \text{ We next turn our attention to the minimal generating set } \{a_0 < a_1 < \ldots < a_n\} \text{ of } S(a, ab). \]

We know that \( n_0 = b \), by Lemma 43; our goal is to describe the remaining minimal generators.

**Lemma 46.** Let \( x \) and \( y \) be positive integers. Then \( \lceil x/y \rceil \) if and only if \( x \equiv 0 \mod b \) or \( y \equiv 0 \mod b \) or \( (x \mod b) + (y \mod b) > b \). \( \square \)

**Remark 47.** If \( S \) is any numerical semigroup and \( m \in S \setminus \{0\} \), then \( S \) is generated by

\[X = (Ap(S, m) \setminus \{0\}) \cup \{m, w(1), \ldots, w(m-1)\}, \]

and the minimal generating set of \( S \) is \( X \setminus (X + X) \). Now, in the case of \( S = S(a, ab) \), Theorem 44 says that \( Ap(S, b) = \{0, k_1b+1, \ldots, ak_{b-1}b+b-1\} \), with \( k_i = \lceil (a-1)i/b \rceil \) for all \( i \in \{1, \ldots, b-1\} \). Thus \( k_i b + t \) is a minimal generator of \( S \) if and only if \( k_i \neq k_i + k_{i-t} \) for all \( i \in \{1, \ldots, t-1\} \).

**Lemma 48.** Let \( S = S(a, ab) \) with \( a, b > 1 \), set \( k_i = \lceil (a-1)i/b \rceil \) for all \( i \in \{1, \ldots, b-1\} \) and take \( t \in \{1, \ldots, b-1\} \).

(i) If \( t < b/(a-1) \), then \( k_i b + t \) is a minimal generator of \( S \) if and only if \( (a-1)i \mod b < (a-1)i \mod b \) for all \( i \in \{1, \ldots, t-1\} \).

(ii) If \( t > b/(a-1) \), then \( k_i b + t \) is not a minimal generator of \( S \).

(iii) If \( t = b/(a-1) \), then \( k_i b + t \) is a minimal generator of \( S \).

**Proof.** Using Lemma 46 and Remark 47, we see that \( k_i b + t \) is a minimal generator of \( S \) if and only if \( (a-1)i \equiv 0 \mod b \) and \( (a-1)i \mod b + (a-1)(t-i) \mod b \leq b \) for all \( i \in \{1, \ldots, t-1\} \). Observe that

\[(\dagger) \quad \frac{b}{(a-1, b)} = \frac{\lcm(a-1, b)}{(a-1)} = \min \{i \mid (a-1)i \mod b = 0\}. \]

(i) From the foregoing we deduce that if \( t < b/(a-1, b) \), then \( k_i b + t \) is a minimal generator of \( S \) if and only if \( (a-1)i \mod b + (a-1)(t-i) \mod b \leq b \) for all \( i \in \{1, \ldots, t-1\} \). If \( (a-1)i \mod b \) \( (a-1)(t-i) \mod b \leq b \), then \( (a-1)t \mod b = 0 \), which is impossible in view of (†), since \( t < b/(a-1, b) \). Hence \( k_i b + t \) is a minimal generator of \( S \) if and only if for all \( i \in \{1, \ldots, t-1\} \) one has \( (a-1)i \mod b + (a-1)(t-i) \mod b \leq b \), which is equivalent to \( (a-1)i \mod b + (a-1)(t-i) \mod b = (a-1)t \mod b \). Since \( (a-1)(t-i) \mod b \neq 0 \), we conclude that \( k_i b + t \) is a minimal generator of \( S \) if and only if \( (a-1)i \mod b < (a-1)t \mod b \) for all \( i \in \{1, \ldots, t-1\} \).

(ii) Let \( i = b/(a-1, b) \). Then \( (a-1)i \equiv 0 \mod b \) and in view of Lemma 46 we get \( k_i + k_{i-t} = k_t \), which implies that \( k_i b + b \) is not a minimal generator of \( S \).
(iii) In this setting \((a-1)t \mod b = 0\) and \((a-1)i \mod b \neq 0\) for all \(i \in \{1, \ldots, t-1\}\). Hence for every \(i \in \{1, \ldots, t-1\}\) one gets \((a-1)i \mod b+(a-1)(t-i) \mod b = b\), and by Lemma 46 we deduce that \(k_i \neq k_i+k_{t-i}\) for any \(i \in \{1, \ldots, t-1\}\). Therefore \(k_i b + t\) is a minimal generator of \(S\).

Lemma 48 yields an explicit description of the minimal generating set of \(S\):

**Theorem 49.** Let \(S = S(a, ab)\) with \(a, b > 1\), and set \(k_i = \lceil (a-1)i/b \rceil\) for \(i \in \{1, \ldots, b-1\}\).

1. If \((b, a-1) = 1\), the minimal generating set of \(S\) is \(\{b, k_t b+t_1, \ldots, k_t b+t_r\}\), where \(\{t_1, \ldots, t_r\} = \{t \in \{1, \ldots, b-1\} \mid (a-1)i \mod b < (a-1)t \mod b \text{ for all } i \in \{1, \ldots, t-1\}\}\).

2. If \((b, a-1) \neq 1\), let \(t_{r+1} = b/(b, a-1)\). Then the minimal generating set of \(S\) is \(\{b, k_t b+t_1, \ldots, k_t b+t_r, k_{t_{r+1}} b + t_{r+1}\}\), where \(\{t_1, \ldots, t_r\} = \{t \in \{1, \ldots, t_{r+1}-1\} \mid (a-1)i \mod b < (a-1)t \mod b \text{ for all } i \in \{1, \ldots, t-1\}\}\).

**Example 50.** Let \(S = S(5, 35)\). Applying Theorem 49(1) with \(a = 5\) and \(b = 7\), we see that \(\{t_1, \ldots, t_r\} = \{1, 3, 5\}\) (observe that 1 is always in \(\{t_1, \ldots, t_r\}\)), and that \(S\) is minimally generated by \(\{7, 8, 17, 26\}\).

**Example 51.** Let \(S = S(5, 30)\). Applying Theorem 49(2) with \(a = 5\) and \(b = 6\), we see that \(t_{r+1} = 3\), \(\{t_1, \ldots, t_r\} = \{1\}\), and \(S\) is minimally generated by \(\{6, 7, 15\}\).

**Corollary 52.** Let \(S = S(a, ab)\) with \(a, b > 1\). Set \(k_i = \lceil (a-1)i/b \rceil\) for \(i \in \{1, \ldots, b-1\}\), and

\[
    t = \begin{cases} 
        \min \{x \in \mathbb{N} \mid (a-1)x \equiv b-1 \mod b\} & \text{if } (b, a-1) = 1, \\
        b/(b, a-1) & \text{if } (b, a-1) \neq 1.
    \end{cases}
\]

Then \(k_i b + t\) is the greatest minimal generator of \(S\).

**Corollary 53.** Let \(a \geq 3\) and let \(b\) be a positive integer. Then \(e(S(a, ab)) \geq \lfloor b/(a-1) \rfloor + 1\).

**Proof.** The integer \(b\) is always a minimal generator of \(S(a, ab)\). Also, if \((a-1)t \leq b\), then by Lemma 48, \(k_i b + t\) is a minimal generator of \(S\).

**Pseudo-Frobenius numbers.** For any numerical semigroup \(S\), we define an order \(\leq_S\) on \(S\) as follows: \(a \leq_S b\) if \(b-a \in S\). Given a subset \(A\) of \(S\), denote by \(\operatorname{Max}_{\leq_S} A\) the set of maximal elements of \(A\) with respect to \(\leq_S\). The following result appears in [Rosales and Branco 2002].

**Lemma 54.** Let \(S\) be any numerical semigroup with multiplicity \(m\). If \(\operatorname{Max}_{\leq_S} (\mathbb{A}p(S, m)) = \{w_{i_1}, \ldots, w_{i_r}\}\),

the pseudo-Frobenius numbers of \(S\) (page 387) are precisely \(w_{i_1} - m, \ldots, w_{i_r} - m\).
Note that if \( w, w' \in \text{Ap}(S, m) \) and \( w - w' \in S \), this forces \( w - w' \) to be in \( \text{Ap}(S, m) \) as well. Hence
\[
\text{Max}_{\leq S}(\text{Ap}(S, m)) = \{ w \in \text{Ap}(S, m) \mid w + w' \notin \text{Ap}(S, m) \text{ for all } 0 \neq w' \in \text{Ap}(S, m) \}.
\]

Let \( S = S(a, ab) \) with \( a, b > 1 \). Our aim is to compute the set \( \text{Max}_{\leq S}(\text{Ap}(S, b)) \) and thus, in view of Lemma 54, the pseudo-Frobenius set \( \text{Pg}(S) \).

**Remark 55.** By Theorem 44, \( k_i b + i \notin \text{Max}_{\leq S}(\text{Ap}(S, b)) \) if and only if there exists \( j \in \{1, \ldots, b-1\} \) such that \( i + j \leq b-1 \) and \( k_i + k_j = k_{i+j} \). Minimal generators are \( \leq S \)-minimal elements of \( \text{Ap}(S, b) \), which is why the condition just stated is similar (dual) to the one presented on the previous page for minimal generators.

**Theorem 56.** Let \( a \) and \( b \) be two integers greater than one, and let \( S = S(a, ab) \). Let \( k_i = \lfloor (a-1)i/b \rfloor \) for \( i \in \{1, \ldots, b-1\} \). Then \( k_i b + i \in \text{Max}_{\leq S}(\text{Ap}(S, b)) \) if and only if one of the following conditions hold:

1. \((a-1)i \equiv 0 \mod b \) and \( i = b-1 \),
2. \((a-1)i \not\equiv 0 \mod b \) and for all \( t \in \{i+1, \ldots, b-1\} \), either \((a-1)i \mod b < (a-1)t \mod b \) or \((a-1)i \mod b = (a-1)t \mod b = 0 \).

**Proof.** Assume that \((a-1)i \equiv 0 \mod b \) and \( i < b-1 \). Then by Lemma 46, we deduce that \( k_i + k_1 = k_{i+1} \) and thus \( k_i b + i \notin \text{Max}_{\leq S}(\text{Ap}(S, b)) \). If \((a-1)i \not\equiv 0 \mod b \), then by Lemma 46 we have \( k_i b + i \in \text{Max}_{\leq S}(\text{Ap}(S, b)) \) if and only if for all \( t \in \{i+1, \ldots, b-1\} \) we have \((a-1)(t-i) \equiv 0 \mod b \) and \((a-1)i \mod b < (a-1)(t-i) \mod b \leq b \). If \((a-1)i \mod b + (a-1)(t-i) \mod b < b \), then \((a-1)i \mod b + (a-1)(t-i) \mod b = (a-1)t \mod b \) and thus \((a-1)i \mod b < (a-1)t \mod b \). If \((a-1)i \mod b + (a-1)(t-i) \mod b = b \), then \((a-1)t \mod b = 0 \).

To prove the converse, assume \( k_i b + i \not\in \text{Max}_{\leq S}(\text{Ap}(S, b)) \). Then there exists \( t \in \{i+1, \ldots, b-1\} \) such that \( k_i + k_{i+1} = k_t \). By using Lemma 46, we deduce that \((a-1)i \equiv 0 \mod b \) or \((a-1)(t-i) \equiv 0 \mod b \) or \((a-1)i \mod b + (a-1)(t-i) \mod b > b \). If \((a-1)i \equiv 0 \mod b \), then \( i \) must be equal to \( b-1 \), but this is impossible since \( t \in \{i+1, \ldots, b-1\} \). If \((a-1)(t-i) \equiv 0 \mod b \), then \((a-1)i \mod b = (a-1)t \mod b \), which is also impossible by hypothesis. Finally if \((a-1)i \mod b + (a-1)(t-i) \mod b > b \), then \((a-1)i \mod b = (a-1)i \mod b + (a-1)(t-i) \mod b - b < (a-1)i \mod b \), leading again to a contradiction. \(\Box\)

**Example 57.** Let \( S = S(5, 30) \). Applying Theorem 56 we get \( \text{Max}_{\leq S}(\text{Ap}(S, 6)) = \{29\} \), which by Lemma 54 means that \( \text{Pg}(S) = \{23\} \). Thus \( S(5, 30) \) is symmetric.

**Proposition 58.** Let \( S = S(a, ab) \) with \( a, b > 1 \).

1. \( S \) is symmetric if and only if \((a-1, b) + (a-1) \mod b = b \).
2. \( S \) is pseudo-symmetric if and only if \((a-1, b) + (a-1) \mod b = b + 1 \).
Proof. (1) Combining Corollaries 45 and 17(1), we see that \( S \) is symmetric if and only if \( \lceil (b-1)(a-1)/b \rceil b - 1 = ab - a - (a-1, b) \). The left-hand side can be written as \( (a-1 - [(a-1)/b]) b - 1 = (a-1)b - [(a-1)/b]b - 1 = ab - b - (a-1 - (a-1) \mod b) - 1 \). Thus \( S \) is symmetric if and only if \( (a-1) \mod b + (a-1, b) = b \).

(2) As above, but this time using Corollary 17(2).

**Corollary 59.** Let \( k \) be a positive integer and let \( b \) be a multiple of \( k \). Then \( S(b - k + 1 + bn, (b - k + 1 + bn)b) \) is symmetric for all \( n \in \mathbb{N} \).

The pseudo-symmetric case is completely different:

**Corollary 60.** \( S(a, ab) \) is not pseudo-symmetric for any choice of \( a, b > 1 \).

Proof. Set \( q = [(a-1)/b] \) and choose \( u, v \in \mathbb{Z} \) such that \( (a-1, b) = u(a-1) + vb \).

If \( S(a, ab) \) is pseudo-symmetric, we have \( (a-1, b) + (a-1) \mod b = b + 1 \), hence \( u(a-1) + vb + (a-1) - qb = b + 1 \), or yet \( (u + 1)(a-1) + (v - q - 1)b = 1 \). But this implies \( (a-1, b) = 1 \) and hence \( 1 + (a-1) \mod b = b + 1 \), an impossibility.

Some families. We now present some families of numerical semigroups of the form \( S(a, ab) \) with \( a, b > 1 \) such that \( (a-1, b) = 1 \). For these families we can compute the minimal generating set and pseudo-Frobenius numbers explicitly. As a consequence of Theorems 49 and 56 one gets:

**Proposition 61.** Let \( S = S(a, ab) \) with \( a, b > 1 \) and \( (a-1, b) = 1 \). Set \( k_i = \lceil (a-1)i/b \rceil \) for \( i \in \{1, \ldots, b-1\} \) and take \( t \in \{1, \ldots, b-1\} \).

1. \( k, b + t \) is a minimal generator of \( S \) if and only if \( (a-1)i \mod b < (a-1)t \mod b \) for all \( i \in \{1, \ldots, t-1\} \).

2. \( k, b + t \in \text{Max}_{\leq t}(\text{Ap}(S, b)) \) if and only if \( (a-1)t \mod b < (a-1)i \mod b \) for all \( i \in \{t+1, \ldots, b-1\} \).

Let \( S_n \) be the symmetric group in \( n \) elements \( \{1, \ldots, n\} \), and for \( k \) relatively prime to \( n + 1 \), define the permutation \( \sigma_{k,n+1} \in S_n \) by \( \sigma(i) = ki \mod (n + 1) \) for \( i = 1, \ldots, n \). Such a permutation is called modular. Next, given any permutation \( \sigma \in S_n \), set

\[
E(\sigma) = \{ t \in \{1, \ldots, n\} \mid \sigma(i) < \sigma(t) \text{ for all } i \in \{1, \ldots, t-1\} \},
\]

\[
T(\sigma) = \{ t \in \{1, \ldots, n\} \mid \sigma(t) < \sigma(i) \text{ for all } i \in \{t+1, \ldots, n\} \}.
\]

With this notation we can rewrite Proposition 61 as follows.

**Corollary 62.** Let \( S = S(a, ab) \) with \( a, b > 1 \) and \( (a-1, b) = 1 \). Then

\[
\text{e}(S) = \#E(\sigma_{a-1, b}) + 1 \quad \text{and} \quad \text{t}(S) = \#T(\sigma_{a-1, b}).
\]

The minimal generating set of \( S \) is \( \{b\} \cup \{ \lceil (a-1)i/b \rceil b + i \mid i \in E(\sigma_{a-1, b}) \} \), and

\[
\text{Max}_{\leq t}(\text{Ap}(S, b)) = \{ \lceil (a-1)i/b \rceil b + i \mid i \in T(\sigma_{a-1, b}) \}.
\]
Example 63. Let $S = S(6, 42)$. Apply Corollary 62 with $a = 6$ and $b = 7$. Clearly $\sigma_{5,7} = (154623)$, $E(\sigma_{5,7}) = \{1, 4\}$ and $T(\sigma_{5,7}) = \{3, 6\}$. Hence $e(S) = 3$ and $t(S) = 2$. The set $\{7, [(5 \times 1)/7]7 + 1, [(5 \times 4)/7]7 + 4\} = \{7, 8, 25\}$ is a minimal generating set of $S$ and $\Max_{\leq S}(Ap(S, 7)) = \{(5 \times 3)/7]7 + 3, [(5 \times 6)/7]7 + 6\} = \{24, 41\}$.

Corollary 64. Let $S = S((b-1) + bn, ((b-1) + bn)b)$ with $n \in \mathbb{N}$ and $b \geq 5$ odd. Then $S$ is minimally generated by $\{b, (n + 1)b + 1, \lfloor b - \frac{1}{2} + n \frac{b+1}{2} \rfloor b + \frac{b+1}{2}\}$, and

$$\Max_{\leq S}(Ap(S, b)) = \{\lfloor b - \frac{1}{2} + n \frac{b-1}{2} \rfloor b + \frac{b-1}{2}, ((b-2) + n(b-1)b) + b-1\}.$$  

Proof. Since $(b - 2 + bn, b) = (b - 2, b) = 1$, we can apply Corollary 62. By inspection we see that $E(\sigma_{b-2,b}) = \{1, (b-1)/2\}$ and $T(\sigma_{b-2,b}) = \{(b-1)/2, b-1\}$. We can conclude the proof using Corollary 62, taking into account that

$$\left\lfloor \frac{(b-2) + bn}{b} \right\rfloor = n + 1, \quad \left\lfloor \frac{(b-2) + bn}{b} \right\rfloor = \frac{b-1}{2} + n \frac{b+1}{2}, \quad \text{and}$$

$$\left\lfloor \frac{(b-2) + bn}{b} \right\rfloor = (b-2) + n(b-1). \quad \Box$$

Corollary 65. Let $b$ be an integer greater than or equal to two and let $n \in \mathbb{N}$. Then $S = S((n + 1)b, (n + 1)b^2)$ is minimally generated by $\{b, (n + 1)b + 1\}$ and $\Max_{\leq S}(Ap(S, b)) = \{(n + 1)(b-1)b + b-1\}$.

Proof. Use Corollary 62 and the fact that $\sigma_{(n+1)b-1,b} = \sigma_{b-1,b}$ swaps $i$ and $b-i$. $\Box$

Corollary 66. Let $S = S(2 + nb, (2 + nb)b)$ with $n \in \mathbb{N}$ and $b \geq 2$. Then $S$ is minimally generated by

$$X = \{b, (n + 1)b + 1, (2n + 1)b + 2, \ldots, ((b-1)n + 1)b + b-1\}$$

and $\Max_{\leq S}(Ap(S, b)) = X \setminus \{b\}$.

Proof. Use Corollary 62 and the fact that $\sigma_{1+nb,b} = \sigma_{1,b}$ is the identity. $\Box$

Corollary 67. Let $S = S(3 + nb, (3 + nb)b)$ with and $n \in \mathbb{N}$ $b \geq 3$ odd. Then $S$ is minimally generated by $\{b, (n + 1)b + 1, (2n + 1)b + 2, \ldots, \lfloor \frac{b+1}{2} + n \rfloor + 1\}$ and

$$\Max_{\leq S}(Ap(S, b)) = \{\lfloor \frac{b+1}{2} + n \rfloor + 2 b + \frac{b+1}{2}, \ldots, ((b-1)n + 2)b + b-1\}.$$  

Proof. By considering $\sigma_{2+bn,b} = \sigma_{2,b}$ we see that $E(\sigma_{2,b}) = \{1, \ldots, \frac{1}{2}(b-1)\}$ and $T(\sigma_{2,b}) = \{\frac{1}{2}(b+1), \ldots, b-1\}$. Using Corollary 62, the proof follows easily from

$$\left\lfloor \frac{(2 + bn)i}{b} \right\rfloor b = \begin{cases} (ni + 1)b + i & \text{if } i \leq \frac{1}{2}(b-1), \\ (ni + 2)b + i & \text{if } i \geq \frac{1}{2}(b+1). \end{cases} \Box$$
6. The Frobenius number in other special cases

In Section 5 we studied \( S(a, b) \) with \( a \mid b \). We now give some partial results for the Frobenius number in the complementary case, \( a \nmid b \). We are able to find the number when \( (a-1)(a - (b \mod a)) < b \). We use without further comment the fact that, for \( q \) a rational number and \( x \) a positive integer, \( x < [q] \) implies \( x < q \).

**Lemma 68.** Let \( S = S(a, b) \) with \( 0 < a < b \) and \( b \mod a \neq 0 \). Then

\[
g(S(a, b)) \leq b - \lfloor b/a \rfloor.
\]

**Proof.** Let \( x \) be a positive integer. If \( x < \lfloor b/a \rfloor \), then \( x < b/a \) and thus \( ax \mod b = ax > x \). Hence \( x \notin S \) and in view of Corollary 6, this leads to \( b - x \in S \). As \( y \in S \) for all \( y \geq b \), we conclude that \( g(S) \leq b - \lfloor b/a \rfloor \).

**Lemma 69.** Let \( a \) and \( b \) be positive integers such that \( a < b \) and \( b \mod a \neq 0 \). Then \( a \lfloor b/a \rfloor \mod b = a - (b \mod a) \).

**Proposition 70.** Let \( a \) and \( b \) be positive integers such that \( a < b \) and \( b \mod a \neq 0 \). Then \( g(S(a, b)) = b - \lfloor b/a \rfloor \) if and only if \( (a-1)(a - (b \mod a)) < b \).

**Proof.** Let \( S = S(a, b) \). From Lemma 68 we deduce that \( g(S) = b - \lfloor b/a \rfloor \) if and only if \( b - \lfloor b/a \rfloor \notin S \), or in other words, \( a(b - \lfloor b/a \rfloor) \mod b > b - \lfloor b/a \rfloor \). This by Lemma 69 is equivalent to \((b \mod a - a) \mod b > b - \lfloor b/a \rfloor \), and this condition holds if and only if \( b + (b \mod a) - a > b - \lfloor b/a \rfloor - 1 \). Hence \( g(S) = b - \lfloor b/a \rfloor \) if and only if \( \lfloor b/a \rfloor + 1 + (b \mod a) > a \), or equivalently \( (b - (b \mod a))/a + 1 + (b \mod a) > a \), and this holds if and only if \( b > (a-1)(a - (b \mod a)) \).

**Corollary 71.** Let \( a \) and \( b \) be positive integers such that \( a < b, b \mod a \neq 0 \) and \( (a-1)(a - (b \mod a)) < b \). Then \( m(S(a, b)) = \lfloor b/a \rfloor \).

**Proof.** Let \( S = S(a, b) \). By Proposition 70, we know that \( g(S) = b - \lfloor b/a \rfloor \). Thus \( b - \lfloor b/a \rfloor \notin S \) and thus by Corollary 6, \( \lfloor b/a \rfloor = b - (\lfloor b/a \rfloor) \in S \). Besides, if \( x \) is a positive integer such that \( x < \lfloor b/a \rfloor \), then \( x < b/a \), whence \( ax \mod b = ax > x \) and thus \( x \notin S \). Therefore \( m(S) = \lfloor b/a \rfloor \).

Though we have given an explicit formula for \( g(S(a, b)) \) for several cases, we have not been able to find such a formula for arbitrary positive integers \( a \) and \( b \). We propose this as an open question.

**Problem 1.** Find a formula for \( g(S(a, b)) \) with \( a \) and \( b \) positive integers.

**Acknowledgments**

We thank J. I. García-García and the referee for their comments and suggestions.
References


J. C. ROSALES  
DEPARTAMENTO DE ÁLGEBRA  
UNIVERSIDAD DE GRANADA  
E-18071 GRANADA  
SPAIN  
jrosales@ugr.es

P. A. GARCÍA-SÁNCHEZ  
DEPARTAMENTO DE ÁLGEBRA  
UNIVERSIDAD DE GRANADA  
E-18071 GRANADA  
SPAIN  
pedro@ugr.es

J. M. URBANO-BLANCO  
DEPARTAMENTO DE ÁLGEBRA  
UNIVERSIDAD DE GRANADA  
E-18071 GRANADA  
SPAIN  
jurbano@ugr.es