

IRREDUCIBLE NUMERICAL SEMIGROUPS HAVING TOMS DECOMPOSITION

M. A. Moreno and E. Pardo

Department of Mathematics, University of Cádiz, Puerto Real (Cádiz), Spain

J. Nicola

Department of Mathematics, University of Geneva, Geneva, Switzerland

In this article we prove that if S is an irreducible numerical semigroup and S is generated by an interval or S has multiplicity 3 or 4, then it enjoys Toms decomposition. We also prove that if a numerical semigroup can be expressed as an expansion of a numerical semigroup generated by an interval, then it is irreducible and has Toms decomposition.

Key Words: Numerical semigroup; Toms decomposition.

2000 Mathematics Subject Classification: Primary 06F05; Secondary 46L80.

1. INTRODUCTION

In the last 30 years, K -theory provided invariants in order to classify C^* -algebras. The interest has been also focussed on determining the range of these invariants. In this line, one of the questions was to find a simple C^* -algebra A whose ordered K_0 -group fails unperforation property.

This question was answered in the affirmative by Villadsen (1998). Subsequent refinements, due to Rørdam and Villadsen (1998) and Elliott and Villadsen (2000), allowed to restrict the K -theoretical scope, by constructing a simple C^* -algebra A such that $(K_0(A), K_0(A)^+) \cong (\mathbb{Z}, S)$, where $S \subseteq \mathbb{Z}^+$ is a submonoid such that $\mathbb{Z}^+ \setminus S$ is a finite set. The natural representation problem is then whether it is possible to find such an algebra for any such monoid S . In this direction, Toms (2003) gives techniques for constructing a simple C^* -algebra with stable rank one whose ordered K_0 -group is isomorphic to \mathbb{Z} with positive cone

$$S = \frac{1}{L} \left(\bigcap_{i=1}^N \langle q_i, m_i \rangle \right) \cap \mathbb{Z}, \quad (*)$$

where q_1, \dots, q_N are prime numbers, m_1, \dots, m_N are natural numbers with $\text{g.c.d.}(q_i, m_i) = 1$, and $L \in \mathbb{N}$ with $\text{g.c.d.}(q_i, L) = \text{g.c.d.}(m_i, L) = 1$. The obvious

Received July 18, 2005; Revised April 26, 2006. Communicated by Facchini.

Address correspondence to E. Pardo, Department of Mathematics, University of Cádiz, Apartado 40, 11510 Puerto Real (Cádiz), Spain; Fax: 34-956016288; E-mail: enrique.pardo@uca.es

question, posed by Toms, in order to give complete answer to the representation problem (as well as for the structural knowledge of numerical semigroups), is whether any submonoid $S \subset \mathbb{Z}^+$ with $\mathbb{Z}^+ \setminus S$ finite should be of this particular form (*).

Toms (2002) showed that the answer is affirmative for 2-generated numerical semigroups. In a recent work (Moreno et al., 2005), the authors and H. Thomas proved that the answer to Toms' question is negative, and in fact that there exist infinitely many numerical semigroups which do not entail a Toms decomposition. Instead, the same work shows that the blocks $\frac{1}{L}\langle q_i, m_i \rangle \cap \mathbb{Z}$ appearing in the decomposition (*) satisfy interesting regularities (of geometrical nature), so that it is an interesting question to state whether concrete families of numerical semigroups have Toms decomposition.

In this article, we show that irreducible numerical semigroups lying in some largely studied classes (e.g., numerical semigroups generated by intervals) has Toms decompositions, and we give explicit expressions of such decompositions.

Let us summarize the contents of this article. In Section 2 we will establish basic results on numerical semigroups and we will present the connection with Toms' question. In Section 3, we present a kind of semigroups, the numerical semigroups generated by intervals, we characterize irreducibility for this family, and we prove that these semigroups have Toms decomposition. In Section 4 we present other families of semigroups having the same decomposition properties.

2. NUMERICAL SEMIGROUPS AND TOMS DECOMPOSITION

In this section we provide the necessary definitions and results related to numerical semigroups, to make clear the connection between them and Toms' question.

A *numerical semigroup* is a subset of S of \mathbb{Z}^+ closed under addition, such that $0 \in S$ and S generates \mathbb{Z} as a group. By definition (see Rosales and García-Sánchez, 1999), $\mathbb{Z}^+ \setminus S$ is a finite set. We refer to the greatest integer not in S as the *Frobenius number* of S (also called the *Conductor* of S) and we denote it by $C(S)$.

We say that a numerical semigroup is *irreducible* if it cannot be expressed as an intersection of two numerical semigroups containing it properly. It is known (Rosales and Branco, 2003) that S is irreducible if and only if S is maximal in the set of all numerical semigroups with Frobenius number $C(S)$. By Barucci et al. (1997) and Fröberg and Gottlieb (1987), the class of irreducible semigroups with odd (respectively even) Frobenius number is the same as the class of symmetric (respectively pseudo-symmetric) numerical semigroups. Also, every numerical semigroup with two generators is irreducible. The essential point is that every numerical semigroup S admits a decomposition $S = S_1 \cap S_2 \cap \dots \cap S_n$ with S_i irreducible for all i (see Rosales and Branco, 2002).

We know (see Barucci et al., 1997 and Rosales and García-Sánchez, 1999), that a numerical semigroup S has a unique minimal system of generators $\{n_1 < n_2 < \dots < n_p\}$. We refer to the numbers n_1 and p as the *multiplicity* and *embedding dimension* of S and denote them by $m(S)$ and $\mu(S)$, respectively. Moreover, if S is a irreducible numerical semigroup, $m(S)$ and $\mu(S)$ are linked (Rosales and Branco, 2003, Proposition 6). Notice that, if S is a irreducible numerical semigroup and $S = \langle n_1, n_2, \dots, n_k \rangle$ is written with the minimal number of generators, then there

exists an upper bound for n_k . Since n_k has to be smaller than the Frobenius number of $\langle n_1, n_2 \rangle$ then $n_k < n_1 n_2 - n_1 - n_2$. Moreover, by Rosales and Branco (2003, Proposition 6), when the upper bound k is larger than 4, we have $k \leq n_1 - 1$.

To check the irreducibility of a numerical semigroup with a minimal set of generators of large cardinality is not always easy. We recall a definition that furnishes a helpful device in this context. Let S be a numerical semigroup and $n \in S \setminus \{0\}$. For any $1 \leq i \leq n$, denote by $w(i)$ the smallest element of S congruent with $i - 1$ modulo n . Notice that this means $w(i) = \min(S \cap (i - 1 + n\mathbb{Z}))$. We denote by $Ap(S, n) = \{0 = w(1), \dots, w(n)\}$ the Apéry set of n in S . By Rosales and García-Sánchez (1999) we know that $Ap(S, n) = \{x \in S : x - n \notin S\}$ and $w(n) = C(S) + n$.

Definition 2.1. Given a numerical semigroup S , we say that S has a *Toms decomposition* provided that there exist $L, q_i, m_i \in \mathbb{Z}^+$ pairwise coprime, with q_i prime for $i \in \{1, \dots, N\}$, such that

$$S = \frac{1}{L} \left(\bigcap_{i=1}^N \langle q_i, m_i \rangle \right) \cap \mathbb{Z}.$$

Next result states that a Toms decomposition is, in fact, an intersection of building blocks of the form $\frac{1}{L} \langle q_i, m_i \rangle$ sharing a common L .

Lemma 2.2. *With the notation of Definition 2.1, we have*

$$\frac{1}{L} \left(\bigcap_{i=1}^N \langle q_i, m_i \rangle \right) \cap \mathbb{Z} = \bigcap_{i=1}^N \left(\frac{1}{L} \langle q_i, m_i \rangle \cap \mathbb{Z} \right).$$

Toms (2002) proves any numerical semigroup with two generators has a Toms decomposition. Concretely, we have the following result.

Lemma 2.3 (Toms, 2002, Lemma 3.3.1). *Let m and k be coprime positive integers. Then there exists a prime q and a positive integer L coprime to both m and q such that*

$$\frac{1}{L} \langle m, q \rangle \cap \mathbb{Z} = \langle m, k \rangle.$$

The idea of the proof is the following: Consider the sequence of integers $a_n = -m + nk$, and let n_0 be a positive integer such that a_{n_0} is positive. Then, a_{n_0} is coprime to k , and the sequence $\{a_n : a_n > 0\}$ is arithmetic; in particular, this sequence contains infinitely many primes. Choose a positive integer L such that a_L is both prime and greater than $mk - m - k$, and set $q = a_L$. Then, the result holds.

Thus, Toms' question has to be proved for numerical semigroups with more than two generators. Moreover, intertwining Toms' (2002) argument with the following result, we are allowed, given S a numerical semigroup, to look for a triple of positive pairwise coprime integers q, m, L such that $S = \frac{1}{L} \langle m, q \rangle \cap \mathbb{Z}$, without paying attention to q being prime or not.

Lemma 2.4. *If L, K, m and q are positive integers, then*

$$\frac{1}{L} \left(\frac{1}{K} \langle m, q \rangle \cap \mathbb{Z} \right) \cap \mathbb{Z} = \frac{1}{LK} \langle m, q \rangle \cap \mathbb{Z}.$$

Then, it suffices to find L_1, q_1, m three pairwise coprime positive integers such that $S = \frac{1}{L_1} \langle m, q_1 \rangle \cap \mathbb{Z}$, to get a Toms building block if q_1 is not prime. To show, look at $\langle m, q_1 \rangle$. By using the proof of Lemma 2.3 we outlined above, chose n_0 so that a_{n_0} is prime, and greater than both L_1 and $m q_1 - m - q_1$. Then, define $q_2 = a_{n_0}$, $L_2 = n_0$. Hence, q_2 is prime, q_2, m, L_2 are pairwise coprime, q_2 is coprime to L_1 , and $\langle m, q_1 \rangle = \frac{1}{L_2} \langle m, q_2 \rangle \cap \mathbb{Z}$. Thus, we apply Lemma 2.4 to end the argument.

In the particular case of an irreducible numerical semigroup S , if there exists a Toms decomposition $S = \bigcap_{i=1}^N (\frac{1}{L_i} \langle q_i, m_i \rangle \cap \mathbb{Z})$, then clearly

$$S = \frac{1}{L} \langle q, m \rangle \cap \mathbb{Z},$$

for $L, q, m \in \mathbb{Z}^+$, pairwise coprime and q prime.

Notice that having Toms decomposition for irreducible numerical semigroups does not guarantee decomposition for arbitrary numerical semigroups, since it is not clear whether for any such a decomposition there exists L , coprime to each $q_1, \dots, q_N, m_1, \dots, m_N$, such that $\bigcap_{i=1}^N (\frac{1}{L_i} \langle q_i, m_i \rangle \cap \mathbb{Z}) = \frac{1}{L} (\bigcap_{i=1}^N \langle q_i, m_i \rangle) \cap \mathbb{Z}$.

3. NUMERICAL SEMIGROUPS GENERATED BY INTERVALS

In this section, we present the semigroups generated by intervals of non-negative integers, that is to say, semigroups of the form

$$S = \langle a, a + 1, \dots, a + x \rangle = \left\{ \sum_{i=0}^x n_i (a + i) : n_i \in \mathbb{Z}^+ \right\} \subseteq \mathbb{Z}^+.$$

Note that if $x \geq a$, then $S = \{a, a + 1, \dots\} = a + \mathbb{Z}^+ = \langle a, a + 1, \dots, 2a - 1 \rangle$; thus we may assume that $x \leq a - 1$. For such semigroups, García-Sánchez and Rosales (1999) computed the Frobenius number and gave a characterization of the numerical semigroups generated by intervals that are symmetric.

Notation 3.1. $[a]$ will denote the least integer greater than or equal to a .

The next result characterizes which numerical semigroups generated by intervals are irreducible.

Proposition 3.2. *Let $S = \langle a, a + 1, \dots, a + t \rangle$ be a numerical semigroup generated by an interval with a, t both integers, $a \geq 3, t \geq 2$. For $t = a - 1, \langle 3, 4, 5 \rangle$ is the only irreducible semigroup generated by an interval. If $2 \leq t \leq a - 2$, then S is irreducible if and only if t divides $a - 2$.*

Proof. Let us consider $S = \langle a, a + 1, \dots, a + t \rangle, a \geq 3, t \geq 2$. If $t \geq a$, S is not written with minimal number of generators. If $t = a - 1$, then $S = \mathbb{Z}^+ \setminus \{1, \dots, a - 1\}$

with $C(S) = a - 1$, and the only irreducible case with $t = a - 1$ is $\langle 3, 4, 5 \rangle = \mathbb{Z}^+ \setminus \{1, 2\}$ with Frobenius number $C(S) = 2$; indeed $\langle 3, 4, 5 \rangle$ is obviously maximal in the set of all numerical semigroups with Frobenius number 2, and according to Rosales and Branco (2003, Theorem 1), $\langle 3, 4, 5 \rangle$ is irreducible. For any other numerical semigroup S such that $t = a - 1$, we consider $S' = S \cup \{C(S) - 1\} = S \cup \{a - 2\}$. First, S' contains strictly S as $a - 2$ does not belong to S ; secondly S' has the same Frobenius number as S , namely, $C(S') = C(S) = a - 1$, as 1 is not in S' . Thus S is not maximal in the set of all numerical semigroups with Frobenius number $C(S)$, and consequently S is not irreducible.

In particular we have proved that if $a \geq 4$ and $S = \langle a, a + 1, \dots, a + t \rangle$ is irreducible, then $2 \leq t \leq a - 2$. Now we will show the second part of the statement. We start by proving that if S is irreducible, then t divides $a - 2$. To see this, observe that S has the following structure:

$$\begin{aligned} &\langle a, a + 1, \dots, a + t \rangle \\ &= \{0, [a, a + 1, \dots, a + t], \dots, [2a, 2a + 1, \dots, 2(a + t)], \dots, \\ &\quad [(x - 1)a, \dots, (x - 1)(a + t)], \dots, [C(S) + 1, xa, xa + 1, \dots, x(a + t)], \dots\}, \end{aligned}$$

where x is an integer greater than or equal to 2, and the sequences between brackets consists of consecutive numbers. According to the above argument, $C(S) - 1$ must be contained in S if S is irreducible. This only occurs when the last gap in S consists only of the integer $C(S)$, i.e., $C(S) - 1 = (x - 1)(a + t) = xa - 2$.

The latter yields $x(a + t) - xa = a + t - 2$, and further $x = 1 + \frac{a-2}{t}$. Thus, as x is an integer, t must to divide $a - 2$.

Conversely, suppose that t divides $a - 2$. By García-Sánchez and Rosales (1999, Corollary 5), $C(S) = \lceil \frac{a-1}{t} \rceil a - 1$. Then, as $\frac{a-1}{t} = \frac{a-2}{t} + \frac{1}{t}$, we get $\lceil \frac{a-1}{t} \rceil a = (\frac{a-2}{t} + 1)a$, which is an even number if $a \geq 3$. Thus, $C(S)$ is odd. By García-Sánchez and Rosales (1999, Theorem 6), S symmetric, whence S is irreducible, as desired. \square

The proof of Proposition 3.2 also establishes the following result.

Corollary 3.3. *If $S = \langle a, a + 1, \dots, a + t \rangle$ is irreducible, then $C(S) = (a - 1) + a \frac{a-2}{t}$.*

Note that this number is odd whatever a and t are such that t divides $a - 2$.

Now, we get the main result of this section, showing that irreducible numerical semigroups generated by an interval enjoy Toms decompositions.

Theorem 3.4. *Let $S = \langle a, a + 1, a + 2, \dots, a + t \rangle$, with a, t positive integers such that $a \geq 4$, $2 \leq t \leq a - 2$ and t divides $a - 2$. Then S has Toms decomposition. More concretely, the following identities hold:*

- (1) *If a is odd, then $S = \frac{1}{t} \langle a, a + t \rangle \cap \mathbb{Z}$;*
- (2) *If a is even and t is odd, then $S = \frac{1}{t} \langle a, a + t \rangle \cap \mathbb{Z}$;*
- (3) *If both a and t are even, then $S = \frac{1}{\frac{a}{t}-1+1} \langle a, C(S)(t - 1) + (a + t) \rangle \cap \mathbb{Z}$.*

Proof. (1) If a is odd, we have $\text{g.c.d.}(a, t) = \text{g.c.d.}(a, a + t) = \text{g.c.d.}(a + t, t) = 1$. As

$$a + i = \frac{(t - i)a + i(a + t)}{t} \quad \text{with } i \in \{0, \dots, t\},$$

we have $S \subseteq \frac{1}{t}\langle a, a + t \rangle \cap \mathbb{Z}$.

For the reverse inclusion, by Rosales and Branco (2003, Theorem 1), we will see that $C(S) \notin \frac{1}{t}\langle a, a + t \rangle \cap \mathbb{Z}$. Suppose that $C(S) \in \frac{1}{t}\langle a, a + t \rangle \cap \mathbb{Z}$. If we denote $\eta = C(S) - a$. Then there exists $\alpha', \beta' \in \mathbb{Z}^+$ such that

$$a + \eta = \frac{\alpha'a + \beta'(a + t)}{t}.$$

Now, we write $\beta' = ka + \beta$, with $k \in \mathbb{Z}^+$ and $0 \leq \beta \leq a - 1$. If we replace α' by $\alpha = \alpha' + k(a + t)$ and β' by β , then

$$a + \eta = \frac{\alpha a + \beta(a + t)}{t}, \quad (3.1)$$

where $\alpha, \beta \in \mathbb{Z}^+$ with $0 \leq \beta \leq a - 1$ and $\alpha \geq 0$. Therefore

$$t(a + \eta) = \alpha a + \beta(a + t), \quad (3.2)$$

whence $\eta t \equiv \beta t \pmod{a}$. As $\text{g.c.d.}(t, a) = 1$, we have $\eta \equiv \beta \pmod{a}$, and so $\eta = \beta + an$ for some $n \geq 0$. Thus, Corollary 3.3 and the restriction $0 \leq \beta \leq a - 1$ imply that $n = \frac{a-2}{t} - 1$, and so $\beta = a - 1$. Substituting in (3.2) we get

$$a(a - 2) + t(a - 1) = \alpha a + (a - 1)(a + t),$$

so that $\alpha = -1$, contradicting the assumption.

(2) If a is even and t is odd, we have $\text{g.c.d.}(a, t) = \text{g.c.d.}(a, a + t) = \text{g.c.d.}(t, a + t) = 1$. Suppose that $\text{g.c.d.}(a, t) = d$. Then d would divide t , but then d would also divide $a - 2$, since S is irreducible, which would result in $d = 1$ or $d = 2$. However $d = 2$ is a contradiction, since t is odd. Thus, $\text{g.c.d.}(a, t) = 1$. Now the proof of case (1) give us the desired result.

(3) If both a and t are even, we will prove that

$$S = \frac{1}{a(t-1)+1} \langle a, C(S)(t-1) + a + t \rangle \cap \mathbb{Z}.$$

We denote $L = a(t - 1) + 1$ and $q = C(S)(t - 1) + a + t$. We have that $\text{g.c.d.}(L, a) = 1$. Notice that by Corollary 3.3

$$q = \left(a - 1 + a \frac{a-2}{t} \right) (t - 1) + a + t = a \left((a - 2) \frac{t-1}{t} + t \right) + 1.$$

Thus, $\text{g.c.d.}(a, q) = 1$.

As $t(q - L(\frac{a-2}{t} + 1)) = a(t - 1) + 2$, we have that $tq = L(a - 1 + t) + 1$, and therefore $\text{g.c.d}(L, q) = 1$.

Now, we will prove that

$$S = \langle a, a + 1, \dots, a + t \rangle = \frac{1}{a(t - 1) + 1} \langle a, C(S)(t - 1) + (a + t) \rangle \cap \mathbb{Z}$$

holds. First, we will show that the identity

$$a + \eta = \frac{\alpha_\eta a + \beta_\eta (C(S)(t - 1) + (a + t))}{a(t - 1) + 1} \tag{3.3}$$

holds for $\eta = 0, 1, \dots, t$ and a related couple of non-negative integers α_η, β_η . Notice that, if we define $\beta_\eta = \eta$, then (3.3) is equivalent to

$$\begin{aligned} \alpha_\eta &= \frac{(a(t - 1) + 1)(a + \eta) - \eta((a - 1 + a\frac{a-2}{t})(t - 1) + a + t)}{a} \\ &= \eta \left(\frac{a - 2}{t} + 1 \right) + a(t - \eta - 1) + 1. \end{aligned}$$

For $\eta = 0, 1, \dots, t - 1$, α_η is obviously a non-negative integer; and $\eta = t$ yields $\alpha_t = a - 2 + t - a + 1 = t - 1 > 0$. Thus,

$$\langle a, a + 1, \dots, a + t \rangle \subseteq \frac{1}{a(t - 1) + 1} \langle a, C(S)(t - 1) + (a + t) \rangle \cap \mathbb{Z}.$$

Now, by Rosales and Branco (2003, Theorem 1), we only need to check that

$$C(S) \notin \frac{1}{a(t - 1) + 1} \langle a, C(S)(t - 1) + (a + t) \rangle \cap \mathbb{Z}.$$

So, we will see that (3.3) fails for $\eta = a\frac{a-2}{t} - 1$, whenever α_η, β_η are both non-negative integers. Writing (3.3) as

$$(a(t - 1) + 1)(a + \eta) = \alpha_\eta a + \beta_\eta \left(\left(a - 1 + a\frac{a - 2}{t} \right) (t - 1) + a + t \right), \tag{3.4}$$

and reducing this identity modulo a , one has that $\eta \equiv \beta_\eta \pmod{a}$. An analog argument to that of case (1), using Corollary 3.3 and the condition $0 \leq \beta_\eta \leq a - 1$, ensure that $\beta_\eta = a - 1$. Substituting the value of β_η in (3.4) and multiplying by t , we get first

$$\begin{aligned} &(a(t - 1) + 1)(ta + a(a - 2) - t) \\ &= t\alpha_\eta a + (a - 1)((ta - t + a(a - 2))(t - 1) + at + t^2), \end{aligned}$$

that give us

$$ta + a(a - 2) - t = t\alpha_\eta a - (ta - t + a(a - 2))(t - 1) + (a - 1)(at + t^2),$$

and thus

$$ta + a^2 - 2a - t = t\alpha_\eta a + 2at - t + a^2 - 2a,$$

whence

$$ta = t\alpha_\eta a + 2at.$$

Hence,

$$\alpha_\eta = \frac{ta - 2ta}{at} = -\frac{at}{at} = -1,$$

contradicting the assumption. Thus, the result holds. \square

Remark 3.5. It can be check easily that $S = \langle 3, 4, 5 \rangle = \frac{1}{2}\langle 3, 5 \rangle \cap \mathbb{Z}$.

Example 3.6. We have:

- (1) $S = \langle 6, 7, 8 \rangle = \frac{1}{7}\langle 6, 25 \rangle \cap \mathbb{Z}$;
- (2) $T = \langle 14, 15, 16, 17 \rangle = \frac{1}{29}\langle 14, 239 \rangle \cap \mathbb{Z}$;
- (3) $V = \langle 11, 12, 13, 14 \rangle = \frac{1}{3}\langle 11, 14 \rangle \cap \mathbb{Z}$;
- (4) $W = \langle 4, 5, 6 \rangle = \frac{1}{7}\langle 4, 19 \rangle \cap \mathbb{Z}$.

Remark 3.7. The semigroups (2) and (3) in Examples 3.6 have q prime, whereas $\langle 6, 25 \rangle$ needs to be transformed using Toms (2002, Lemma 3.3.1). A prime number q_S is required, such that $q_S = -6 + 25L_S$, where $q_S \geq C(\langle 6, 25 \rangle) = 119$, L_S is coprime to 6, and both q and L_S are coprime to 7. The least value of q_S fulfilling these conditions is $q_S = 269$, with a related $L_S = 11$. Thus, by Lemmas 2.3 and 2.4,

$$S = \langle 6, 7, 8 \rangle = \frac{1}{7} \left(\frac{1}{11} \langle 6, 269 \rangle \right) \cap \mathbb{Z} = \frac{1}{77} \langle 6, 269 \rangle \cap \mathbb{Z}.$$

4. OTHER EXAMPLES HAVING TOMS DECOMPOSITION

In this section we will show that the Toms decomposition holds for some kinds of irreducible numerical semigroup with multiplicity 3 and 4, and these appearing as expansions of numerical semigroups generated by an interval.

We begin characterizing when an expansion of a numerical semigroup generated by an interval is irreducible.

Proposition 4.1. *Let a odd, $a \geq 5$ and $x > 0$. Then $S = \langle a, x + a, 2x + a, \dots, (a - 2)x + a \rangle$ is an irreducible numerical semigroup if and only if $\text{g.c.d.}(a, x) = 1$.*

Proof. Let $S = \langle a, x + a, 2x + a, \dots, (a - 2)x + a \rangle$. Then, $\text{g.c.d.}(a, x) = 1$ is a necessary condition for S to be written with a minimal number of generators. To see

this, assume per absurdum that $a = pq$ and $x = kq$ for some positive integers k, p and q , where $k \geq 2$ and $p, q \geq 3$. Then

$$S = \langle pq, (k + p)q, (2k + p)q, \dots, ((pq - 2)k + p)q \rangle.$$

As $1 < p < pq - 2$, then the sequence $p, k + p, 2k + p, \dots, (pq - 2)k + p$ contains $pk + p$ and hence $a = pq$ divides the generator $p(k + 1)q$, which contradicts $\mu(S) = a - 1$.

To prove the converse, we assume that $\text{g.c.d.}(a, x) = 1$ and first show that the Frobenius number of S is $C(S) = (a - 1)x + a$. To see this, let us show that $(a - 1)x + a$ does not belong to S , but every $n \in S$ such that $n > (a - 1)x + a$ is in S . Assume at first that $(a - 1)x + a$ is in S . Then there exist $\alpha_0, \dots, \alpha_{a-2}$, all non-negative integers, such that

$$(a - 1)x + a = a\alpha_0 + (x + a)\alpha_1 + \dots + ((a - 2)x + a)\alpha_{a-2}. \tag{4.1}$$

That is

$$(a - 1)x + a = x(\alpha_1 + 2\alpha_2 + \dots + (a - 2)\alpha_{a-2}) + a \sum_{i=0}^{a-2} \alpha_i.$$

Assume that $\sum_{i=0}^{a-2} \alpha_i = k > 1$. Then $x(a - 1 - (\alpha_1 + 2\alpha_2 + \dots + (a - 2)\alpha_{a-2})) = (k - 1)a$, but $\text{g.c.d.}(a, x) = 1$ ensures that a divides $a - 1 - (\alpha_1 + 2\alpha_2 + \dots + (a - 2)\alpha_{a-2})$ and consequently $\alpha_1 + 2\alpha_2 + \dots + (a - 2)\alpha_{a-2} \leq -1$, which is absurd. Hence, as $\sum_{i=0}^{a-2} \alpha_i \leq 0$ is absurd as well, $\sum_{i=0}^{a-2} \alpha_i = 1$, which means that exactly one of the α_i is 1 and every other 0. But then (4.1) does not hold. Thus $(a - 1)x + a \notin S$.

Let us now consider $n = (a - 1)x + t, t \geq a + 1$. If $t > 2a$, then n can be expressed as $(a - 1)x + r + ak$, with $r \in \{a + 1, a + 2, \dots, 2a\}$ and k a positive integer. And $t = 2a$ yields $(a - 1)x + 2a = 2(\frac{a-1}{2}x + a) \in S$, as a is odd and $2 \leq \frac{a-1}{2} < a - 2$. Hence it suffices to show that $(a - 1)x + t$ belongs to S for $t \in \{a + 1, \dots, 2a - 1\}$.

Look at the generators of S . As x is coprime with a , each of the $a - 1$ generators belongs to different congruence classes modulo a , and the missing class is $-x$ (the one corresponding to $(a - 1)x + a$, the Frobenius number of S). Now let us consider $(a - 1)x + t \equiv t - x \pmod{a}$. For $t \in \{a + 1, \dots, 2a - 1\}$, $t - x$ runs through each congruence class modulo a , except precisely class $-x$. Hence $(a - 1)x + t$ belongs to the same congruence class modulo a as one of the generators, and is greater than this generator. Denote by ψ the suitable generator. Then $(a - 1)x + t = \psi + a\zeta$, for some $\zeta \in \mathbb{Z}^+$. Thus $C(S) = (a - 1)x + a$.

Let us now show that S is irreducible. Observe that $C(S)$ is odd. We will prove $w(i) + w(a - i + 1) = w(a)$ for $i \in \{1, \dots, a\}$, and by Rosales and Branco (2003, Proposition 3), S is an irreducible numerical semigroup.

We begin proving that

$$Ap(S, a) = \{0, x + a, 2x + a, \dots, (a - 2)x + a, (a - 1)x + 2a\}.$$

To see this, observe that $w(1) = 0$ as a is the least element in S , and $w(a) = C(S) + a$, according to a result given by Rosales and García-Sánchez (1999,

Proposition 10.4). By definition of $Ap(S, a)$ (see Section 2), we have to check that $w(i) - a \notin S$ for $i = 2, \dots, a - 1$. As $w(i) = (i - 1)x + a$, then $w(i) - a = (i - 1)x$. Let $j = i - 1$ and assume that $jx \in S$ for $j = 1, 2, \dots, a - 2$. Then there exists $\beta_0, \dots, \beta_{j-1}$, all non-negative integers, such that $jx = a\beta_0 + (x + a)\beta_1 + \dots + ((j - 1)x + a)\beta_{j-1}$ (we exclude $jx + a, \dots, (a - 2)x + a$, as they are greater than jx) and further $(j - \sum_{k=1}^{j-1} \beta_k k)x = a \sum_{k=0}^{j-1} \beta_k$. As $\text{g.c.d.}(a, x) = 1$, a divides $j - \sum_{k=1}^{j-1} \beta_k k$, which is impossible, since

$$j - \sum_{k=1}^{j-1} \beta_k k < j \leq a - 2. \quad (4.2)$$

Thus

$$\begin{aligned} Ap(S, a) &= \{0 = w(1), x + a = w(2), \dots, (a - 2)x + a \\ &= w(a - 1), (a - 1)x + 2a = w(a)\} \end{aligned}$$

and, as $w(i) - a = (i - 1)x$ and $w(a) = (a - 1)x + 2a$, the identity $w(i) + w(a - i + 1) = w(a)$ holds, so that S is irreducible.

Finally, we observe that S is written with a minimal number of generators. Assume that some of them—say $lx + a$ for some $l \in \{1, \dots, a - 2\}$ —is a positive integer combination of the remaining generators. Provided that a is the smallest element in S , it is a necessary generator, and only those smaller than $lx + a$ take part in this combination. Then, there exists $\gamma_0, \dots, \gamma_{l-1}$, non-negative integers, such that $lx + a = a\gamma_0 + (x + a)\gamma_1 + \dots + ((l - 1)x + a)\gamma_{l-1}$, and further $(l - \sum_{k=1}^{l-1} \gamma_k k)x = a(\sum_{k=0}^{l-1} \gamma_k - 1)$. As $\text{g.c.d.}(a, x) = 1$, we get the same contradiction as (4.2). \square

The next result shows that the irreducible numerical semigroups with multiplicity 3, as well as those appearing as expansions of a numerical semigroup generated by an interval, have Toms decomposition.

Theorem 4.2.

- (1) If x is a strictly positive integer and x not a multiple of 3, then $S = \langle 3, x + 3, 2x + 3 \rangle$ has Toms decomposition

$$S = \frac{1}{x + 2} \langle x + 3, 2x + 3 \rangle \cap \mathbb{Z}.$$

- (2) Let $S = \langle a, x + a, 2x + a, \dots, (a - 2)x + a \rangle$, a numerical semigroup where $\text{g.c.d.}(a, x) = 1$, a is odd, $a \geq 5$ and $x > 0$. Then S has Toms decomposition

$$S = \frac{1}{a - 2} \langle a, (a - 2)x + a \rangle \cap \mathbb{Z}.$$

Proof. (1) By Rosales and Branco (2003, Theorem 7), the only irreducible numerical semigroup with $\mu(S) = m(S) = 3$ is $S = \langle 3, x + 3, 2x + 3 \rangle$, where x is a strictly positive integer such that x is not multiple of 3. Let $k = 3$, $m = x + 3$, and $q = 2x + 3$, and let us implement $L = \frac{q+m}{k} = \frac{(2x+3)+(x+3)}{3} = x + 2$. Then, m and

L are obviously coprime. Also, L and q are coprime, as any nontrivial common factor would divide $1 = 2L - q$. Assume that p divides both m and q for some p prime; then p divides $3 = 2m - q$, which entails $p = 3$ and contradicts $3 \nmid x$. Thus $\text{g.c.d.}(m, q) = 1$. We will prove now that

$$\frac{1}{x+2} \langle x+3, 2x+3 \rangle \cap \mathbb{Z} = \langle 3, x+3, 2x+3 \rangle.$$

As,

$$3 = \frac{(2x+3) + (x+3)}{x+2},$$

$$x+3 = \frac{1}{x+2} ((x+2)(x+3) + 0 \cdot (2x+3)),$$

and

$$2x+3 = \frac{1}{x+2} (0 \cdot (x+3) + (x+2)(2x+3)),$$

we have $\frac{1}{x+2} \langle x+3, 2x+3 \rangle \cap \mathbb{Z} \supseteq \langle 3, x+3, 2x+3 \rangle$.

To see the converse, assume that $\frac{a(x+3)+b(2x+3)}{x+2}$ is an integer for a, b both non-negative integers; assume furthermore that $a \geq b$. Then

$$\frac{a(x+3) + b(2x+3)}{x+2} = b \frac{(x+3) + (2x+3)}{x+2} + \frac{(a-b)(x+3)}{x+2} = 3b + \frac{(a-b)(x+3)}{x+2}.$$

As $\text{g.c.d.}(x+2, x+3) = 1$, there exists $d \in \mathbb{Z}^+$ such that $d = \frac{a-b}{x+2}$ and consequently $\frac{a(x+3)+b(2x+3)}{x+2} = 3b + d(x+3)$.

A similar argument with $b \geq a$ shows that, for some $g \in \mathbb{Z}^+$,

$$\frac{a(x+3) + b(2x+3)}{x+2} = 3a + g(2x+3).$$

Thus, $\frac{1}{x+2} \langle x+3, 2x+3 \rangle \cap \mathbb{Z} \subseteq \langle 3, x+3, 2x+3 \rangle$ and reciprocal inclusion yields

$$\frac{1}{x+2} \langle x+3, 2x+3 \rangle \cap \mathbb{Z} = \langle 3, x+3, 2x+3 \rangle,$$

completing the proof.

(2) Let us denote by T the numerical semigroup $\frac{1}{a-2} \langle a, (a-2)x+a \rangle \cap \mathbb{Z}$. As a is odd, $a-2, a$ and $(a-2)x+a$ are pairwise coprime and both a and $(a-2)x+a$ belong to T . To check that the remaining generators of S are in T , it is enough to find two suitable non-negative integers φ, χ such that the equation $kx+a = \frac{1}{a-2}(\varphi a + \chi((a-2)x+a))$ holds for each $k \in \{1, \dots, a-3\}$. Choose $\chi = k$, whence the identity reduces to $a-2 = \varphi + k$. As k runs increasingly from 1 to $a-3$, there exists a related φ running decreasingly from $a-3$ to 1. Thus $T \supseteq S$.

The converse is easy to prove, checking that $C(S) \notin T$. Assume per absurdum that $C(S) \in T$. Then there exist \varkappa, ϱ both non-negative integers such that

$$(a-1)x + a = \frac{\varkappa a + \varrho((a-2)x + a)}{a-2}. \quad (4.3)$$

We deduce that $\varrho < a-1$. As (4.3) is $(a-2)((a-1) - \varrho)x + ((a-2) - \varrho)a = \varkappa a$, a must divide $(a-2)((a-1) - \varrho)x$, which is impossible as $\text{g.c.d.}(a, x) = 1$ and $a > a-1 - \varrho$ for $\varrho < a-1$. Thus $C(S) \notin T$ and $S = T$. \square

As a consequence, we obtain an expression of Toms decomposition for other families of numerical semigroups, as follows.

Corollary 4.3. *If x is a strictly positive integer then $S = \langle 3, 3x+2, 6x+1 \rangle$ has Toms decomposition $S = \frac{1}{3x+1} \langle 3x+2, 6x+1 \rangle \cap \mathbb{Z}$.*

Proof. By assumption, $3x-1$ is a strictly positive integer, and it is not multiple of 3. Then, the result holds by part (1) of Theorem 4.2. \square

Example 4.4. We have:

- (1) $S = \langle 3, 5, 7 \rangle = \frac{1}{4} \langle 5, 7 \rangle \cap \mathbb{Z}$;
- (2) If $S = \langle 5, x+5, 2x+5, 3x+5 \rangle$ with $\text{g.c.d.}(5, x) = 1$ and $x > 0$, then $S = \frac{1}{3} \langle 5, 3x+5 \rangle \cap \mathbb{Z}$.

Notice that no such identity has been found for $S = \langle a, x+a, 2x+a, \dots, (a-2)x+a \rangle$, where $\text{g.c.d.}(a, x) = 1$ and a is even.

Next result shows that the irreducible numerical semigroups with multiplicity 4 have Toms decomposition.

Proposition 4.5. *Let $S = \langle 4, x+2, x+4 \rangle$, where x is an odd integer greater than or equal to 3. Then $S = \frac{2}{(x+3)} \langle x+2, x+4 \rangle \cap \mathbb{Z}$.*

Proof. By Rosales and Branco (2003, Theorem 9), S is an irreducible numerical semigroup, and $m(S) = 4$. Now, the proof is analog to that of Theorem 4.2(1), by fixing $k = 4$, $m = x+2$, $q = x+4$ and

$$L = \frac{q+m}{k} = \frac{(x+4) + (x+2)}{4} = \frac{x+3}{2} \in \mathbb{Z}^+. \quad \square$$

Example 4.6. We have $\langle 4, 7, 9 \rangle = \frac{1}{4} \langle 7, 9 \rangle \cap \mathbb{Z}$.

ACKNOWLEDGMENTS

Part of this work was done during a visit of the second author to the Departamento de Matemáticas de la Universidad de Cádiz (Spain), through a grant of the Erasmus-Socrates Program of the European Community. His contribution is

contained in his Master Degree Thesis, done under the supervision of E. Pardo in Fall 2004. The second author thanks the host center for its warm hospitality.

The first and third authors were partially supported by the DGI and European Regional Development Fund, jointly, through Project MTM2004-00149, by PAI III grant FQM-298 of the Junta de Andalucía. The third author is also partially supported by the Comissionat per Universitats i Recerca de la Generalitat de Catalunya. The second author is partially supported by an Erasmus–Socrates grant of the European Community.

REFERENCES

- Barucci, V., Dobbs, D. E., Fontana, M. (1997). Maximality properties in numerical semigroups and applications to one-dimensional analytically irreducible local domains. *Memoirs Amer. Math. Soc.* 598:X+78 pp.
- Elliott, G., Villadsen, J. (2000). Perforated ordered K_0 -groups. *Canad. J. Math.* 52(6):1164–1191.
- Fröberg, R., Gottlieb, G., Häggkvist, R. (1987). On numerical semigroups. *Semigroup Forum* 35:63–83.
- García-Sánchez, P. A., Rosales, J. C. (1999). Numerical semigroups generated by intervals. *Pacific J. Math.* 191(1):75–83.
- Moreno, M. A., Nicola, J., Pardo, E., Thomas, H. (2005). Numerical semigroups that cannot be written as an intersection of d -squashed semigroups. To appear in *Canadian Mathematical Bulletin*.
- Rosales, J. C., García-Sánchez, P. A. (1999). *Finitely Generated Commutative Monoids*. New York: Nova Science Publishers.
- Rosales, J. C., Branco, M. B. (2002). Decomposition of a numerical semigroup as an intersection of irreducible numerical semigroups. *Bull. Belg. Math. Soc. Simon Stevin* 9(3):373–381.
- Rosales, J. C., Branco, M. B. (2003). Irreducible numerical semigroups. *Pacific J. Math.* 209(1):131–143.
- Rørdam, M., Villadsen, J. (1998). On the ordered K_0 -group of universal free product C^* -algebras. *K-Theory* 15:307–322.
- Toms, A. (2002). On strongly perforated K_0 -groups of simple C^* -algebras.
- Toms, A. (2003). Strongly perforated K_0 -groups of simple C^* -algebras. *Canad. Math. Bull.* 46(3):457–472.
- Villadsen, J. (1998). Simple C^* -algebras with perforation. *J. Funct. Anal.* 154(1):110–116.