ПРИЛОЗИ, Одделение за природно-математички и биотехнички науки, МАНУ, том **41**, бр. 1, стр. 49–55 (2020)
CONTRIBUTIONS, Section of Natural, Mathematical and Biotechnical Sciences, MASA, Vol. **38,** No. 1, pp. 49–55 (2020)

Received: March 22, 2020
Accepted: June 2, 2020

ISSN 1857–9027
e-ISSN 1857–9949
UDC: 512.536:511.12
DOI:10.20903/csnmbs.masa.2020.41.1.157

Review

ADDITIVE SEMIGROUPS OF INTEGERS. EMBEDDING DIMENSION OF NUMERICAL SEMIGROUPS

Violeta Angjelkoska, Dončo Dimovski

Faculty of Informatics, FON University, Skopje, Republic of North Macedonia
Macedonian Academy of Sciences and Arts, Skopje, Republic of North Macedonia

e-mail: violeta.angelkoska@fon.edu.mk, ddimovskd@gmail.com

We characterize the embedding dimension of numerical semigroups in the same manner as additive semigroups of integers are characterized in [1]. Moreover, we give a particular characterization of the Frobenius number of numerical semigroups with embedding dimension less than or equal to 3.

Key words: numerical semigroups; embedding dimension; Frobenius number

INTRODUCTION

This paper has been motivated by the results about the structure of additive semigroups of integers (Dimovski, [1]), geometric description of finitely generated subsemigroups of the additive semigroup $\mathbb{N}^n$ (Dimovski and Hadži - Kosta Josifovska, [2]) and the description of finitely generated additive subgroups of $\mathbb{Z}^n$ (Hadži - Kosta Josifovska and Dimovski, [3]).

The main results stated in these papers are the following:

Theorem 1.1. (Theorem 1.2. in [1]) Let G be a semigroup consisting of positive integers. Let n be the smallest integer in G, d the greatest common divisor of the elements of G and $n = kd$. Let us denote by A_i the set of all the elements in G whose remainder after division by n is id, i.e.

$$A_i = \{a | a \in G, a = nt + id, t \in \mathbb{N}\}.$$

Then:

(i) $G = A_0 \cup A_1 \cup \dots \cup A_{k-1}$, the union is disjoint.

(ii) There exist $1 = a_0, a_1, \dots, a_{k-1}$, such that

$$A_i = \{tn + id | t \geq a_i\} \text{ and}$$

$$a_i + a_j \geq \begin{cases} a_{i+j}, & i+j < k \\ a_{i+j-k} - 1, & i+j \geq k. \end{cases}$$

(iii) If $m_i = a_i n + id$, then $\{n = m_0, m_1, \dots, m_{k-1}\}$ is a set of generators for G.

(iv) Let

$$b = max\{ a_0, a_1, \dots, a_{k-1}\},$$

$s = max\{ i | a_i = b\}$ and $c = (b-1)k + s + 1$. Then

$$(c-1)d \notin G \text{ and } \{td | t \geq c\} = G_* \subseteq G.$$

(We say that G_* is the *regular part* of G.)

Theorem 1.2. (Theorem 2.1. in [1]) Let α be a congruence on G and $\alpha \neq \Delta_G$ (Δ_G is the equality on G). Then there exist $m, s_0, s_1, \dots, s_{k-1} \in \mathbb{N}$ such that:

(i) $a\alpha b \Rightarrow m | a - b$.

(ii) ($\forall t \in \mathbb{N}_0$) $[(s_i + t)n + id]^\alpha$ is an infinite class, and, for every $v \in A_i$, $v < s_i n + id \Rightarrow v^\alpha$ is a finite class for $0 \leq i \leq k-1$.

(iii) The integers s_i satisfy the following conditions:

$$s_i \geq a_i,$$

$$s_i + a_j \geq \begin{cases} s_{i+j}, & i+j < k \\ s_{i+j-k} - 1, & i+j \geq k. \end{cases}$$

Theorem 1.3. (Theorem 2.1. in [2]) An additive subsemigroup G of $\mathbb{N}^n$ for $n > 1$ is finitely generated if and only if G is a subset of $Cone(A)$ for some subset A of G.

Theorem 1.3. shows the major difference between the structure of additive subsemigroups of $\mathbb{Z}^n$ for $n > 1$ and additive subsemigroups of $\mathbb{Z}$, since any additive subsemigroup of $\mathbb{Z}$ is finitely generated. For better understanding of the additive subsemigroups of $\mathbb{Z}^n$ a good description of the additive subgroups of $\mathbb{Z}^n$ is given in [3].

Four years ago, we came across two papers about numerical semigroups (Semigroup Forum, see [4],[5]). We found out that they are in fact semigroups of nonnegative integers, whose greatest common divisor of their elements is 1.

Later, we found out that there are a lot of papers about numerical semigroups (see [6] - [13]), discussing the following notions: multiplicity, conductor, Frobenius number, embedding dimension, gaps, genus, etc. and also theorems analogous to Theorem 1.1, but not to Theorem 1.2.

With the notions as in Theorem 1.1, when $d = 1$, $G \cup \{0\}$ is a numerical semigroup, whose multiplicity is n, conductor is c, the gaps are all the numbers $tn + i$, for $t < a_i$, the genus is $\sum_{i=0}^{n-1} a_i$ and the Frobenius number is $c - 1$.

The notion of embedding dimension is not considered in [1]. The aim of this paper is to characterize the embedding dimension of numerical semigroups in the same manner as additive semigroups of integers are characterized in [1]. Moreover, using this characterization, we obtain an explicit form for the Frobenius number of numerical semigroups with embedding dimension less than or equal to 3.

Further on, instead of the term additive semigroups of nonnegative integers, we use the term numerical semigroups. Thus, a numerical semigroup G is a proper nonempty subset of $\mathbb{N}_0$, closed under addition, containing 0 and whose complement is finite, i.e. $\mathbb{N}_0 \backslash G$ is finite. We say that a set

$$S = \{n_1, n_2, \dots, n_t\} \subseteq \mathbb{N}$$

is a set of generators for G, denoted by $G = < S >$, if the elements of G are linear combinations of $n_1, n_2, \dots, n_t$ with nonnegative integer coefficients.

The condition (*iii*) in Theorem 1.1. implies that every numerical semigroup has a finite set of generators. Moreover, it has a unique minimal set of generators ([4]). The cardinality of the minimal set of generators for G is called *embedding dimension* of G, denoted by $ed(G)$. The smallest number in the minimal set of generators is called *multiplicity* of G, denoted by n. The largest number not belonging to a numerical semigroup G is called *Frobenius number* of G, denoted by $F(G)$. The set $\mathbb{N}_0 \backslash G$ is known as the set of gaps of G. Its cardinality is called *genus* of G, denoted by $g(G)$.

In this paper a numerical semigroup G will be denoted by $G = [n, A]$, where n is the multiplicity of G and

$$A = \{1 = a_0, a_1, \dots, a_{n-1}\},$$

where $a_0, a_1, \dots, a_{n-1}$ are as in Theorem 1.1.

SOME PRELIMINARY NOTIONS AND RESULTS

The addition of integers modulo n will be denoted by $\oplus$ and the additive group of integers modulo n will be denoted by $(\mathbb{Z}_n, \oplus)$. If $X \subseteq \mathbb{Z}_n$, the subgroup of $(\mathbb{Z}_n, \oplus)$ generated by X will be denoted by $< X >$. The subtraction of integers modulo n will be denoted by $\ominus$. The multiplication of integers modulo n will be denoted by $\odot$. For $i_1, \dots, i_k \in \mathbb{Z}_n$ and $k \in \mathbb{N}$, the integer part $\left[\frac{i_1 + \dots + i_k}{n}\right]$ will be denoted by $[n; i_1, \dots, i_k]$, i.e.

$$[n; i_1, \dots, i_k] = \left[\frac{i_1 + \dots + i_k}{n}\right].$$

Lemma 2.4. Let $n, k, t \in \mathbb{N}$, $i_u, j_v \in \mathbb{Z}_n$ for $1 \leq u \leq k$, $1 \leq v \leq t$, $j = i_1 \oplus \dots \oplus i_k$ and $s = j_1 \oplus \dots \oplus j_t$. Then:

(*i*) $[n; i_1, \dots, i_k] = \dfrac{i_1 + \dots + i_k - i_1 \oplus \dots \oplus i_k}{n}$;

(*ii*) $[n; i_1, \dots, i_k, j_1, \dots, j_t]$
$= [n; j, j_1, \dots, j_t] + [n; i_1, \dots, i_k]$;

(*iii*) $[n; i_1, \dots, i_k, j_1, \dots, j_t]$
$= [n; j, s] + [n; i_1, \dots, i_k] + [n; j_1, \dots, j_t]$;

(*iv*) $[n; i] = 0$.

Proof. (*i*) Since $j = i_1 \oplus \dots \oplus i_k$, it follows that

$$i_1 + \dots + i_k = tn + j \text{ for some } t \in \mathbb{N}.$$

Thus,

$$\left[\frac{i_1 + \dots + i_k}{n}\right] = t = \frac{i_1 + \dots + i_k - j}{n},$$

i.e.

$$[n; i_1, \dots, i_k] = \frac{i_1 + \dots + i_k - i_1 \oplus \dots \oplus i_k}{n}.$$

(*ii*) Using (*i*) we obtain

$$\begin{aligned} &[n; j, j_1, \dots, j_t] + [n; i_1, \dots, i_k] \\ &= \frac{j + j_1 + \dots + j_t - j \oplus s + i_1 + \dots + i_k - j}{n} \\ &= \frac{i_1 + \dots + i_k + j_1 + \dots + j_t - j \oplus s}{n} \\ &= [n; i_1, \dots, i_k, j_1, \dots, j_t]. \end{aligned}$$

(*iii*) Follows from (*ii*).

(*iv*) Follows from (*i*). ■

Applying Lemma 2.4, the condition (*ii*) in Theorem 1.1 can be written as

$$a_{i \oplus j} \leq a_i + a_j + [n; i, j].$$

Lemma 2.5. Let $G = [n; \{a_0 = 1, a_1, \dots, a_{n-1}\}]$ be a numerical semigroup. Then for arbitrary $i_1, \dots, i_k \in \mathbb{Z}_n, k \in \mathbb{N}$ we have that

$$a_{i_1 \oplus \dots \oplus i_k} \leq a_{i_1} + \dots + a_{i_k} + [n; i_1, \dots, i_k].$$

Proof. The proof is by induction on k. It is easily seen that the inequality holds for $k = 1$. Namely, $a_{i_1} =$

a_{i_1}. The condition (*ii*) in Theorem 1.1 implies that the inequality holds for $k = 2$.
Assume that

$$a_{i_1 \oplus \ldots \oplus i_k} \leq a_{i_1} + \ldots + a_{i_k} + [n; i_1, \ldots, i_k].$$

The condition (*ii*) in Theorem 1.1, the inductive hypothesis and Lemma 2.4 imply that

$$a_{i_1 \oplus \ldots \oplus i_k \oplus i_{k+1}} \leq a_{i_1 \oplus \ldots \oplus i_k} + a_{i_{k+1}} + [n; i_1 \oplus \ldots \oplus i_k, i_{k+1}] \leq a_{i_1} + \ldots + a_{i_k} + a_{i_{k+1}} + [n; i_1, \ldots, i_k] + [n; i_1 \oplus \ldots \oplus i_k, i_{k+1}] = a_{i_1} + \ldots + a_{i_k} + a_{i_{k+1}} + [n; i_1, \ldots, i_k, i_{k+1}]. \blacksquare$$

For a numerical semigroup

$$G = [n; \{a_0 = 1, a_1, \ldots, a_{n-1}\}]$$

we define the following sets:

$$R(G) = \{i \oplus j | i, j \in \mathbb{Z}_n, a_{i \oplus j} = a_i + a_j + [n; i, j]\} \text{ and } S(G) = \mathbb{Z}_n \setminus R(G).$$

Lemma 2.6. $0 \in S(G)$.

Proof. Since $a_0, a_1, \ldots, a_{n-1} \in \mathbb{N}$, it follows that

$$a_0 = 1 < a_i + a_j + [n; i, j] \text{ for all } i, j \in \mathbb{Z}_n. \blacksquare$$

EMBEDING DIMENSION OF NUMERICAL SEMIGROUPS

We will give a characterization of the embedding dimension of numerical semigroups in the same manner as a characterization of the additive semigroups of integers was given in [1].

Let $G = [n; \{a_0 = 1, a_1, \ldots, a_{n-1}\}]$ be a numerical semigroup, $B_0 = \{a_i n + i | i \in \mathbb{Z}_n\}$ and

$$\mathcal{M}_0 = \{a_i n + i | i \in R(G)\}.$$

From the definition of B_0 and $\mathcal{M}_0$ it follows that

$$|B_0 \setminus \mathcal{M}_0| = |\mathbb{Z}_n \setminus R(G)| = |S(G)|.$$

Theorem 3.1. The set $B_0 \setminus \mathcal{M}_0$ is the minimal set of generators for G. Thus,

$$ed(G) = |B_0 \setminus \mathcal{M}_0| = |S(G)|.$$

Proof. We will consider the following four steps.

Step 1. If $R(G) = \emptyset$ then $\mathcal{M}_0 = \emptyset$. We will show that B_0 is the minimal set of generators for G by contradiction.

Assume that, for some $i \in \mathbb{Z}_n \setminus \{0\}$,

$$a_i n + i = a_{i_1} n + i_1 + \cdots + a_{i_k} n + i_k,$$

where $k \geq 2$ and $a_{i_s} n + i_s \in B_0 \setminus \{a_i n + i\}$ for each $s \in \{1, \ldots, k\}$. Then

$$a_i n + i = (a_{i_1} + \ldots + a_{i_k}) n + i_1 + \ldots + i_k = (a_{i_1} + \ldots + a_{i_k}) n + [n; i_1, \ldots, i_k] n + i_1 \oplus \ldots \oplus i_k = (a_{i_1} + \ldots + a_{i_k} + [n; i_1, \ldots, i_k]) n + i_1 \oplus \ldots \oplus i_k.$$

This implies that $i = i_1 \oplus \ldots \oplus i_k$ and

$$a_i = a_{i_1 \oplus \ldots \oplus i_k} = a_{i_1} + \ldots + a_{i_k} + [n; i_1, \ldots, i_k].$$

Let $j = i_2 \oplus \ldots \oplus i_k$ and assume that

$$a_i = a_{i_1 \oplus j} < a_{i_1} + a_j + [n; i_1, j].$$

By Lemma 2.5 we have that

$$a_{i_1} + \ldots + a_{i_k} + [n; i_1, \ldots, i_k] = a_{i_1 \oplus \ldots \oplus i_k} \leq a_{i_1} + \ldots + a_{i_k} + [n; i_1, \ldots, i_k].$$

Next, the assumption and Lemma 2.5 imply that:

$$a_{i_1} + \ldots + a_{i_k} + [n; i_1, \ldots, i_k] < a_{i_1} + a_j + [n; i_1, j] \leq a_{i_1} + a_{i_2} \ldots + a_{i_k} + [n; i_2, \ldots, i_k] + [n; i_1, j].$$

This implies that

$$[n; i_1, \ldots, i_k] < [n; i_2, \ldots, i_k] + [n; i_1, j],$$

contrary to Lemma 2.4 (*ii*).

Hence, $a_i = a_{i_1} + a_j + [n; i_1, j]$. So $i \in R(G)$, contrary to $R(G) = \emptyset$. Therefore, B_0 is the minimal set of generators for G.

Step 2. Let $R(G) \neq \emptyset$ and x_1 be the largest element in B_0 such that $x_1 = a_{t_1} n + t_1$ and $t_1 \in R(G)$. This implies that $t_1 = i \oplus j$ for some $i, j \in \mathbb{Z}_n$ and

$$a_{i \oplus j} = a_i + a_j + [n; i, j].$$

Thus,

$$x_1 = (a_i + a_j + [n; i, j]) n + i \oplus j = a_i n + a_j n + [n; i, j] n + i \oplus j = a_i n + a_j n + i + j = u + v,$$

where $u = a_i n + i$ and $v = a_j n + j$. Since $u, v > 0$, it follows that $x_1 \neq u$ and $x_1 \neq v$. Therefore,

$$x_1 \in < B_0 \setminus \{x_1\} >, \text{ i.e. } < B_1 > = < B_0 > = G, \text{ where } B_1 = B_0 \setminus \{x_1\}.$$

If $R(G) \setminus \{t_1\} = \emptyset$, the same discussion as in Step 1, implies that B_1 is the minimal set of generators for G.

Step 3. We continue by induction to obtain the elements

$$t_1, \ldots, t_r \in R(G), x_1 > x_2 > \ldots > x_r \in B_0$$

and $B_r \subset B_{r-1} \subset \ldots \subset B_1 \subset B_0$, such that

$$x_s = a_{t_s} n + t_s \text{ and } B_s = B_{s-1} \setminus \{x_s\},$$

for every $s \in \{1, \ldots, r\}$.

If $R(G) \setminus \{t_1, \ldots, t_r\} = \emptyset$, the same discussion as in Step 1, implies that B_r is the minimal set of generators for G. If $R(G) \setminus \{t_1, \ldots, t_r\} \neq \emptyset$, let x_{r+1} be the largest element in B_r such that $x_{r+1} = a_t n + t$ for some $t \in R(G) \setminus \{t_1, \ldots, t_r\}$. This implies that $x_r > x_{r+1}$ and $a_t = a_{i \oplus j} = a_i + a_j + [n; i, j]$ for some $i, j \in \mathbb{Z}_n$.

Thus,

$$x_{r+1} = (a_i + a_j + [n; i, j]) n + i \oplus j = a_i n + a_j n + [n; i, j] n + i \oplus j = a_i n + a_j n + i + j = u + v,$$

where $u = a_i n + i$ and $v = a_j n + j$. From $u, v > 0$, we have that $x_{r+1} \neq u$ and $x_{r+1} \neq v$.

Since $x_1 > x_2 > \ldots > x_r > x_{r+1}$, it follows that $u, v \in B_0 \setminus \{x_1, \ldots, x_{r+1}\}$, i.e.

$$x_{r+1} \in < B_{r+1} > = < B_r \setminus \{x_{r+1}\} >.$$

Hence,

$$< B_{r+1} > = < B_r > = \ldots = < B_1 > = < B_0 > = G.$$

Step 4. This procedure has to stop, since $R(G)$ has a finite number of elements, i.e. there is some t_m such that $R(G) \setminus \{t_1, \ldots, t_m\} = \emptyset$. The same discussion as in Step 1 implies that B_m is the minimal set of generators for G. Since

$$|B_m| = |B_0 \backslash \{x_1, \ldots, x_m\}| = |B_0 \backslash \mathcal{M}_0| = |S(G)|,$$
we have
$$ed(G) = |B_0 \backslash \mathcal{M}_0| = |S(G)|. \blacksquare$$

Let n be a given positive integer. Let $T \subseteq \mathbb{Z}_n \backslash \{0\}$ be a generating set for $\mathbb{Z}_n$, i.e. $< T > = \mathbb{Z}_n$ and let $B(T) = \{b_s | s \in T\} \subseteq \mathbb{N}$ satisfies the following condition:

if $t \in T$ and $t = i_1 \oplus \ldots \oplus i_r$ for $i_1, \ldots, i_r \in T \backslash \{t\}$,
then $b_t < b_{i_1} + \ldots + b_{i_r} + [n; i_1, \ldots, i_r]$. (1)

We define a set $P = \{a_0, a_1, \ldots, a_{n-1}\}$ as follows:
(i) $a_0 = 1$;
(ii) If $i \in T$, then $a_i = b_i$;
(iii) If $i \notin T$, then
$$a_i = min\{ b_{i_1} + \ldots + b_{i_r} + [n; i_1, \ldots, i_r] | i = i_1 \oplus \ldots \oplus i_r, i_1, \ldots, i_r \in T\}.$$

By the definition of the set P it follows that for each $i \in \mathbb{Z}_n \backslash \{0\}$, there is $t \in \mathbb{N}$ and some $i_1, \ldots, i_t \in T$ such that
$$a_i = b_{i_1} + \ldots + b_{i_t} + [n; i_1, \ldots, i_t],$$
$$\text{where } i = i_1 \oplus \ldots \oplus i_t. \qquad (2)$$

Theorem 3.2. With the above notions, we have:
(i) $G = [n; P]$ is a numerical semigroup, denoted by $[n; T; B(T)]$.
(ii) $R([n; T; B(T)]) = \mathbb{Z}_n \backslash (T \cup \{0\})$.
(iii) $ed([n; T; B(T)]) = |T| + 1$.

Proof.
(i) By (2) it follows that
$$a_i = b_{i_1} + \ldots + b_{i_r} + [n; i_1, \ldots, i_r],$$
$$a_j = b_{j_1} + \ldots + b_{j_t} + [n; j_1, \ldots, j_t],$$
where $i = i_1 \oplus \ldots \oplus i_r$ and $j = j_1 \oplus \ldots \oplus j_t$ for some $r, t \in \mathbb{N}$.
If $i \oplus j \in T$ then
$$a_{i \oplus j} = b_{i \oplus j} < b_{i_1} + \ldots + b_{i_r} + b_{j_1} + \ldots + b_{j_t} + [n; i_1, \ldots, i_r, j_1, \ldots, j_t],$$
where $i \oplus j = i_1 \oplus \ldots \oplus i_r \oplus j_1 \oplus \ldots \oplus j_t$.
If $i \oplus j \notin T$ then
$$a_{i \oplus j} = min\{ b_{i_1} + \ldots + b_{i_k} + [n; i_1, \ldots, i_k] | i \oplus j = i_1 \oplus \ldots \oplus i_k, i_1, \ldots, i_k \in T\}$$
$$\leq b_{i_1} + \ldots + b_{i_r} + b_{j_1} + \ldots + b_{j_t} + [n; i_1, \ldots, i_r, j_1, \ldots, j_t].$$
In both cases, we have
$$\begin{aligned} a_{i \oplus j} &\leq b_{i_1} + \ldots + b_{i_r} + b_{j_1} + \ldots + b_{j_t} + [n; i_1, \ldots, i_r, j_1, \ldots, j_t] \\ &= a_i - [n; i_1, \ldots, i_r] + a_j - [n; j_1, \ldots, j_t] + [n; i_1, \ldots, i_r, j_1, \ldots, j_t] \\ &= a_i + a_j - [n; i_1, \ldots, i_r] + [n; i_1, \ldots, i_r, j] \\ &= a_i + a_j + [n; i, j], \end{aligned}$$
i.e.
$$a_{i \oplus j} \leq a_i + a_j + [n; i, j].$$
Thus, $a_0, a_1, \ldots, a_{n-1}$ satisfy the condition (ii) in Theorem 1.1 and $G = [n, P]$ is a numerical semigroup.

(ii) Let $t \in R(G)$. Then $t = i \oplus j$ and $a_t = a_i + a_j + [n; i, j]$, where
$$a_i = b_{i_1} + \ldots + b_{i_r} + [n; i_1, \ldots, i_r],$$
$$a_j = b_{j_1} + \ldots + b_{j_k} + [n; j_1, \ldots, j_k],$$
$$i = i_1 \oplus \ldots \oplus i_r \text{ and } j = j_1 \oplus \ldots \oplus j_k,$$
for $r, k \in \mathbb{N}$.
If $t \in T$ then
$$\begin{aligned} &b_{i_1} + \ldots + b_{i_r} + b_{j_1} + \ldots + b_{j_k} + [n; i_1, \ldots, i_r, j_1, \ldots, j_k] \\ &> a_{i \oplus j} = a_t = a_i + a_j + [n; i, j] \\ &= b_{i_1} + \ldots + b_{i_r} + [n; i_1, \ldots, i_r] + b_{j_1} + \ldots + b_{j_k} + [n; j_1, \ldots, j_k] + [n; i, j], \end{aligned}$$
which implies that
$$[n; i_1, \ldots, i_r] + [n; j_1, \ldots, j_k] + [n; i, j] < [n; i_1, \ldots, i_r, j_1, \ldots, j_k],$$
contrary to Lemma 2.4. So $t \notin T$. This shows that $R(G) \subseteq \mathbb{Z}_n \backslash T$.
For $t = 0$,
$$a_0 = 1 < a_i + a_j + [n; i, j] \text{ for all } i, j \in \mathbb{Z}_n, \text{ i.e. }$$
$t \in \mathbb{Z}_n \backslash (T \cup \{0\})$. Hence, $R(G) \subseteq \mathbb{Z}_n \backslash (T \cup \{0\})$.
Let $t \in \mathbb{Z}_n \backslash (T \cup \{0\})$. Since $t \notin T \cup \{0\}$, it follows that there are $i_1, \ldots, i_r \in T$ and $r \in \mathbb{N}$ such that
$$t = i_1 \oplus \ldots \oplus i_r$$
and
$$a_t = a_{i_1 \oplus \ldots \oplus i_r} = b_{i_1} + \ldots + b_{i_r} + [n; i_1, \ldots, i_r] = a_{i_1} + \ldots + a_{i_r} + [n; i_1, \ldots, i_r].$$
Let $j = i_2 \oplus \ldots \oplus i_r$. Then
$$a_t = a_{i_1} + a_{i_2} + \ldots + a_{i_r} + [n; i_1, j] + [n; i_2, \ldots, i_r] \geq a_{i_1} + a_j + [n; i_1, j] = a_{i_1 \oplus j} = a_t.$$
Hence $a_t = a_{i_1} + a_j + [n; i_1, j]$, which implies that $t \in R(G)$. This completes the proof, i.e.
$$R(G) = \mathbb{Z}_n \backslash (T \cup \{0\}).$$
(iii) Follows from (i) and (ii). $\blacksquare$

By all these results we obtain the following theorem:

Theorem 3.3. A numerical semigroup G has $ed(G) = d$ iff $G = [n; T; B(T)]$ for some: positive integer n; $T \subseteq \mathbb{Z}_n \backslash \{0\}$ such that $< T > = \mathbb{Z}_n$ and $|T| = d - 1$; and some $B(T) \subseteq \mathbb{N}$, that satisfies the condition (1).

FROBENIUS NUMBER OFNUMERICAL SEMIGROUPS

The Frobenius number $F(G)$ of a numerical semigroup G is the largest integer not belonging to G. In fact, $F(G)$ is the largest integer such that the linear equation $m_1 x_1 + \ldots + m_r x_r = F(G)$ does not have any non-negative integer solution, where
$$\{m_1, \ldots, m_r\}$$
is the minimal set of generators for G.

It is shown that if $G = < m_1, m_2 >$ and $GCD(m_1, m_2) = 1$, then $F(G) = m_1 m_2 - m_1 - m_2$ ([6]).

The question of finding a general formula for the Frobenius number, in terms of the minimal set of generators for G when $ed(G) \geq 3$, turned out to be much more difficult to answer.

F. Curtis has proved in [10] that Frobenius number cannot be given by "closed" formulas of a certain type when $ed(G) \geq 3$.

Several authors have developed algorithms that compute the Frobenius number of numerical semigroups with embedding dimension 3. The first is Johnson ([15]). Rødseth developed an algorithm using continued fractions ([14]). The algorithm by Davison ([16]) is the fastest known algorithm for computing the Frobenius number for $ed(G) = 3$, according to Beihoffer, Nijenhuis and Wagon ([17]).

Recently, an explicit general formula for computing $F(G)$ for $ed(G) = 3$, was given by Denham in [18] and Tripathi in [19].

When $ed(G) > 3$, the Frobenius number has been exactly determined only for few special cases ([14]).

A variety of algorithms for computing the Frobenius number for $ed(G) > 3$, as well as upper bounds and lower bounds, are quite well elaborated in [14].

By Theorem 1.1, the Frobenius number of $G = [n, A]$ is

$$F(G) = an + k - n,$$

where

$$a = max\{ a_0, \dots, a_{n-1}\} \text{ and } k = max\{ i | a_i = a\}.$$

This is the simplest general form for the Frobenius number.

In continuation, we give a particular characterization of the Frobenius number of numerical semigroups with embedding dimension less than or equal to 3, in terms of its minimal set of generators.

Let $G = [n; T; B(T)]$, $T = \{j_1, \dots, j_k\}$,

$$\mathcal{A} = \{a_s n + s | s \in \mathbb{Z}_n\} \text{ and}$$

$$\mathcal{M} = \{b_{j_r} n + j_r | r = 1, \dots, k\}, \text{ i.e.}$$

$$\mathcal{M} = \{m_1, \dots, m_k\}.$$

We define $\varphi: \mathbb{Z}^k \to \mathbb{Z}_n$ by

$$\varphi(z_1, \dots, z_k) = t \text{ iff } \textstyle\sum_{s=1}^{k} z_s m_s \equiv t \ (mod\, n).$$

It is easy to check that the map φ is a homomorphism and $H = ker\, \varphi$ is an additive subgroup of $\mathbb{Z}^k$ of rank k. Let $B^0 = H \cap (\mathbb{N}_0)^k$, $B = B^0 \backslash \{(0, \dots, 0)\}$, $D = B + (\mathbb{N}_0)^k$ and $C = (\mathbb{N}_0)^k \backslash D$. (We say that C is the carrier of G).

Theorem 4.1. For each $r \in \mathcal{A} \backslash \{0\}$, $r = p_1 m_1 + \dots + p_k m_k$ for some $(p_1, \dots, p_k) \in C$.

Proof. Assume contrary that for some $r \in \mathcal{A} \backslash \{0\}$, $r = p_1 m_1 + \dots + p_k m_k$ and $(p_1, \dots, p_k) \notin C$. Then $(p_1, \dots, p_k) \in B + (\mathbb{N}_0)^k$, i.e.

$$(p_1, \dots, p_k) = (r_1, \dots, r_k) + (q_1, \dots, q_k) = (r_1 + q_1, \dots, r_k + q_k),$$

where $(r_1, \dots, r_k) \in B$ and $(q_1, \dots, q_k) \in (\mathbb{N}_0)^k$. Since $(r_1, \dots, r_k) \in B$ it follows that

$$\varphi(r_1, \dots, r_k) = 0.$$

This implies that $\varphi(p_1, \dots, p_k) = \varphi(q_1, \dots, q_k)$, and the obvious inequality

$$p_1 m_1 + \dots + p_k m_k > q_1 m_1 + \dots + q_k m_k$$

contradicts the fact that $r \in \mathcal{A} \backslash \{0\}$. ■

If $ed(G) = 1$ then $T = \emptyset$ and $G = < n >$. So, $n = 1$ and the Frobenius number of G does not exist.

Let $ed(G) = 2$, i.e. $G = [n; \{i\}; \{b_i\}]$, where

$$GCD(n, i) = 1,\ x = b_i n + i,\ \mathcal{M} = \{x\} \text{ and}$$

$$\mathcal{A} = \{a_s n + s | s \in \mathbb{Z}_n\} = \{m_s | s \in \mathbb{Z}_n\}.$$

The definition of G implies that $m_{t \odot i} = tx$, so the Frobenius number of $G = [n; \{i\}; \{b_i\}]$ is

$$F(G) = (n-1)x - n = nx - x - n.$$

Let $ed(G) = 3$, i.e. $G = \left[n; \{i, j\}; \{b_i, b_j\}\right]$, where

$$GCD(n, i) = GCD(n, j) = 1, x = b_i n + i,$$

$$y = b_j n + j, \mathcal{M} = \{x, y\} \text{ and}$$

$$\mathcal{A} = \{a_s n + s | s \in \mathbb{Z}_n\} = \{m_s | s \in \mathbb{Z}_n\}.$$

The definition of G implies that

$$m_s = min\{ px + qy | p \odot i \oplus q \odot j = s\}.$$

If $p' \odot i = q' \odot j$ and $p'x > q'y$, then

$$p' \odot i \oplus q \odot j = q' \odot j \oplus q \odot j = (q' + q) \odot j$$

$$\text{and } p'x + qy > (q + q')y.$$

Similarly, for $p' \odot i = q' \odot j$ and $q'y > p'x$,

$$q' \odot j \oplus p \odot i = p' \odot i \oplus p \odot i = (p' + p) \odot i$$

$$\text{and } q'y + px > (p + p')x.$$

If $p \odot i = q \odot j$, then $\varphi(p, -q) = 0$, for the homomorphism $\varphi: \mathbb{Z}^2 \to \mathbb{Z}_n$, i.e. $(p, -q) \in H$. In order to find $min\{ px + qy\}$, the above discussion shows that we have to have a good control on the pairs $(p, -q) \in H$ for $p, q \in \mathbb{Z}_n$.

We say that a pair $(p, -q) \in H$, for $p, q \in \mathbb{Z}_n$, is a *minimal pair* if there is no $(p', -q') \in H$, for $p', q' \in \mathbb{Z}_n$, such that $p' < p$ and $q' < q$. We say that two minimal pairs $(p, -q)$, $(u, -v)$ are *consecutive* if $p > u$, $q < v$ and

$$0 < c < p, 0 < d < v \Rightarrow (c, -d) \notin H.$$

We will prove the following lemma.

Lemma 4.2. Let $(p, -q), (u, -v)$ be two minimal consecutive pairs. Then $pv - qu = n$ and

$$\{s \odot i \oplus r \odot j | (s, r) \in A_L \cup A_R\} = \mathbb{Z}_n,$$

where

$$A_L = \{(s, r) | 0 \leq s < p, 0 \leq r < v - q\},$$

$$A_R = \{(s, r) | 0 \leq s < p - u, 0 \leq r < v\}.$$

Proof. Let

$$K = \{s \odot i \oplus r \odot j | (s, r) \in A_L \cup A_R\}.$$

The proof is in three steps.

Step 1. The assumption $GCD(n,i) = GCD(n,j) = 1$ implies that for every $t \in \mathbb{Z}_n$, $t = \alpha \odot i \oplus \beta \odot j$ for some $(\alpha,\beta) \in \mathbb{N} \times \mathbb{N}$. If $(\alpha,\beta) \in A_L \cup A_R$, then $t \in K$. If $(\alpha,\beta) \notin A_L \cup A_R$, then we have to consider 4 cases: $\alpha < p$, $\beta < v$; $\alpha \geq p$, $\beta < v$; $\alpha < p$, $\beta \geq v$; and $\alpha \geq p$, $\beta \geq v$.

Case 1. $\alpha < p$, $\beta < v$ and $(\alpha,\beta) \notin A_L \cup A_R$.

Since $(\alpha,\beta) \notin A_L$, it follows that $v - q \leq \beta < v$, and since $(\alpha,\beta) \notin A_R$, it follows that $p - u \leq \alpha < p$.

Next, the assumptions $p \odot i = q \odot j$ and $u \odot i = v \odot j$ imply that

$$\begin{aligned}(\alpha \ominus (p \ominus u)) \odot i \oplus (\beta \ominus (v \ominus q)) \odot j \\ = \big(\alpha - (p-u)\big) \odot i \oplus \big(\beta - (v-q)\big) \odot j \\ = \alpha \odot i \ominus p \odot i \oplus u \odot i \oplus \beta \odot j \ominus v \odot j \oplus q \odot j \\ = \alpha \odot i \oplus \beta \odot j = t = \alpha' \odot i \oplus \beta' \odot j,\end{aligned}$$

where

$$\alpha' = \big(\alpha - (p-u)\big) < \alpha < p \text{ and}$$
$$\beta' = \big(\beta - (v-q)\big) < \beta < v.$$

If $(\alpha',\beta') \in A_L \cup A_R$, then $t \in K$. If $(\alpha',\beta') \notin A_L \cup A_R$, then we repeat the discussion above. After finitely many repetitions we will obtain that $t \in K$.

Case 2. $\alpha \geq p$, $\beta < v$.

If $v - q \leq \beta < v$, we apply the same argument as in Case 1, and obtain that

$$t = \alpha' \odot i \oplus \beta' \odot j,$$

where

$$\alpha' = \big(\alpha - (p-u)\big) < \alpha \text{ and}$$
$$\beta' = \big(\beta - (v-q)\big) < \beta < v.$$

Next, let $\beta < v - q < v$. Then $\beta + q < v \leq n$, and

$$\begin{aligned}(\alpha \ominus p) \odot i \oplus (\beta \oplus q) \odot j \\ = (\alpha - p) \odot i \oplus (\beta + q) \odot j \\ = \alpha \odot i \ominus p \odot i \oplus \beta \odot j \oplus q \odot j \\ = \alpha \odot i \oplus \beta \odot j = t = \alpha' \odot i \oplus \beta' \odot j,\end{aligned}$$

where

$$\alpha' = (\alpha - p) < \alpha \text{ and } \beta < \beta' = (\beta + q) < v.$$

In both cases, if $(\alpha',\beta') \in A_L \cup A_R$, then $t \in K$.

Let $(\alpha',\beta') \notin A_L \cup A_R$. If (α',β') is in Case 1, we obtain that $t \in K$. If (α',β') is not in Case 1, then it is in Case 2, and we repeat the same discussion as above. After finitely many repetitions of the above discussion we will obtain that $t \in K$.

Case 3. $\alpha < p$, $\beta \geq v$.

This case is symmetric to the Case 2.

Case 4. $\alpha \geq p$, $\beta \geq v$.

By the same discussion as in Case 1, we obtain that $t = \alpha' \odot i \oplus \beta' \odot j$, where

$$\alpha' = \big(\alpha - (p-u)\big) < \alpha \text{ and}$$
$$\beta' = \big(\beta - (v-q)\big) < \beta.$$

If $(\alpha',\beta') \in A_L \cup A_R$, then $t \in K$. If $(\alpha',\beta') \notin A_L \cup A_R$, we apply again one of the previous cases, and after a finite number of such applications, we obtain that $t \in K$.

The above discussion implies that $\mathbb{Z}_n \subseteq K$.

Step 2. Let $(\alpha,\beta) \in A_R$ and $(\alpha,\beta) \neq (0,0)$. Then $0 < \alpha + u < p$ and $0 < v - \beta < v$. This, together with the assumption that $(p,-q),(u,-v)$ are minimal consecutive pairs, implies that

$$(\alpha + u) \odot i \oplus (-(v-\beta)) \odot j \neq 0, \text{ i.e.}$$
$$(\alpha + u) \odot i \oplus (\beta - v) \odot j \neq 0.$$

Since $u \odot i \oplus (-v) \odot j = 0$, we obtain that

$$\alpha \odot i \oplus \beta \odot j \neq 0.$$

Similarly, if $(\alpha,\beta) \in A_L$ and $(\alpha,\beta) \neq (0,0)$, then

$$\alpha \odot i \oplus \beta \odot j \neq 0.$$

We have shown that for $(\alpha,\beta) \in A_L \cup A_R$,

$$\alpha \odot i \oplus \beta \odot j = 0 \Rightarrow (\alpha,\beta) = (0,0).$$

Step 3. Let $(\alpha_1,\beta_1),(\alpha_2,\beta_2) \in K$ such that

$$\alpha_1 \odot i \oplus \beta_1 \odot j = \alpha_2 \odot i \oplus \beta_2 \odot j, \text{ i.e.}$$
$$(\alpha_1 \ominus \alpha_2) \odot i \oplus (\beta_1 \ominus \beta_2) \odot j = 0.$$

The conclusion of Step 2 implies that

$$\alpha_1 \ominus \alpha_2 = 0 \text{ and } \beta_1 \ominus \beta_2 = 0,$$

and since $\alpha_1,\alpha_2,\beta_1,\beta_2 < n$ it follows that

$$(\alpha_1,\beta_1) = (\alpha_2,\beta_2).$$

Thus, $K \subseteq \mathbb{Z}_n$. This, together with Step 1, implies that $K = \mathbb{Z}_n$.

A simple calculation implies that

$$n = |K| = |A_L \cup A_R| = pv - qu \,. \blacksquare$$

Next, for $G = [n; \{i,j\}; \{b_i,b_j\}]$, $x = b_i n + i$ and $y = b_j n + j$, let:

- p be the smallest positive integer such that $px > (p \odot i \odot j^{-1})y$, and
- v be the smallest positive integer such that $vy > (v \odot j \odot i^{-1})x$.

A simple calculation implies that the pairs

$$(p, -p \odot i \odot j^{-1}) \text{ and } (v \odot j \odot i^{-1}, -v)$$

satisfy the condition of Lemma 4.2. Thus,

$$\mathcal{A} = \{sx + ry \,|\, (s,r) \in A_L \cup A_R\} \text{ and}$$
$$F(G) = (p-1)x + (v-1)y$$
$$- min\{(v \odot j \odot i^{-1})x, (p \odot i \odot j^{-1})y\} - n.$$

For a real number x, let $[x]$ be the integer part of x, i.e. let $[x]$ be the biggest integer smaller or equal than x, and let

$$\lceil x \rceil = \begin{cases} [x] + 1, & x \notin \mathbb{Z} \\ [x], & x \in \mathbb{Z}. \end{cases}$$

To find all the minimal pairs we start with the minimal pairs $(n,0)$ and $(j \odot i^{-1}, -1)$. The next minimal pair is $\left(\left\lceil \frac{n}{j \odot i^{-1}} \right\rceil (j \odot i^{-1}) - n, -\left\lceil \frac{n}{j \odot i^{-1}} \right\rceil\right)$. If $(p,-q)$ and $(u,-v)$ are two consecutive minimal pairs such that $u \neq 0$, then the next minimal pair is

$$\left(\left\lceil \frac{p}{u} \right\rceil u - p, -\left(\left\lceil \frac{p}{u} \right\rceil v - q\right)\right).$$

With the above discussion we proved the following theorem.

Theorem 4.3. Let $G = \langle n, x, y \rangle$ be a numerical semigroup with $ed(G) = 3$. Then:
(i) There are unique $p, q, u, v \in \mathbb{N}$ obtained by the procedure given above, such that:

$$px \equiv qy (mod\ n),\ vy \equiv ux (mod\ n),$$
$$px > qy \text{ and } vy > ux;$$

(ii) The Frobenius number $F(G)$ of G is

$$px + vy - \frac{ux + qy - |ux - qy|}{2} - n - x - y. \blacksquare$$

REFERENCES

[1] Д. Димовски, Адитивни полугрупи на цели броеви, *МАНУ, Скопје, Прилози*, **IX**, **2**, (1977), стр. 21–25.

[2] Д. Димовски, М. Хаџи-Коста Јосифовска, Конечно генерирани потполугрупи од адитивната полугрупа $\mathbb{N}^{\mathrm{n}}$, *Math. Maced*., Vol.**1** (2003), стр. 77–88.

[3] М. Хаџи-Коста Јосифовска, Д. Димовски, Опис на конечно генерирани адитивни подгрупи од $\mathbb{Z}^{\mathrm{n}}$, *Зборник на трудови од III конгрес на математичарите на Македонија*, Струга, (2005), стр. 261–274.

[4] V. Barucci, F. Khouja, On the class semigroup of a numerical semigroup, *Semigroup Forum*, **92** (2016), pp. 377–392.

[5] G. Failla, C. Peterson, R. Utano, Algorithms and basic asymptotics for generalized numerical semigroups in $\mathbb{N}^d$, *Semigroup Forum*, **92** (2016), pp. 460–473.

[6] J. C. Rosales, P. A. García-Sánchez, *Numerical Semigroups*, Developments in mathematics, Springer, New York, 2009.

[7] J. C. Rosales, On numerical semigroups, *Semigroup Forum*, **52** (1996), pp. 307–318.

[8] J. C. Rosales, P. A. García-Sánchez, J. I. García-García, M. B. Branco, Systems of inequalities and numerical semigroups, *Journal of the London Mathematical Society*, **65** (2002), pp. 611–623.

[9] R. Fröberg, G. Gottlieb, R. Häggkvist, On numerical semigroups, *Semigroup Forum*, **35** (1987), pp. 63–83.

[10] F. Curtis, On formulas for the Frobenius number of a numerical semigroup, *Math. Scand*., **67** (1990), pp. 190–192.

[11] A. M. Robles-Pérez, J. C. Rosales, The Frobenius problem for numerical semigroups with embedding dimension equal to three, *Math. Comput*., **81** (2012), pp. 1609–1617.

[12] J. C. Rosales, Numerical semigroups with Apéry sets of unique expression, *J. Algebra*, **226** (2000), pp. 479–487.

[13] V. Barucci, D. E. Dobbs, M. Fontana, Maximality properties in numerical semigroups and applications to one-dimensional analytically irreducible local domains, *Mem. Amer. Math. Soc*., **598** (1997).

[14] J. L. Ramìrez Alfonsìn, *The Diophantine Frobenius Problem*, Oxford University Press, Oxford, 2005.

[15] S. M. Johnson, A linear Diophantine problem. *Canadian Journal of Mathematics*, **12** (1960), pp. 390–398.

[16] J. L. Davison, On the linear Diophantine problem of Frobenius, *Journal of Number Theory*, **48** (1994), pp. 353–363.

[17] D. Beihoffer, J. Hendry, A. Nijenhuis, S. Wagon, Faster algorithms for Frobenius numbers, *Electronic Journal of Combinatorics*, **12** (2005).

[18] G. Denham, Short generating functions for some semigroup algebras, *Electronic Journal of Combinatorics*, **10** (2003).

[19] A. Tripathi, Formulae for the Frobenius number in three variables, *Journal of Number Theory*, **170** (2017), pp. 368–389.

АДИТИВНИ ПОЛУГРУПИ ОД ЦЕЛИ БРОЕВИ. ДИМЕНЗИЈА НА НУМЕРИЧКИ ПОЛУГРУПИ

Виолета Анѓелкоска, Дончо Димовски

Факултет за информатика, Универзитет ФОН, Скопје, Република Северна Македонија
Македонска академија на науките и уметностите, Скопје , Република Северна Македонија

Во овој труд дадена е карактеризација на димензијата на нумеричките полугрупи од аспект на структурата на адитивните полугрупи од цели броеви дадена во [1]. Дадена е експлицитна формула за Фробениусовиот број $F(G)$ кога димензијата на нумеричката полугрупа G е помала или еднаква на 3.

Клучни зборови: нумерички полугрупи; димензија; Фробениусов број