International Journal of Algebra, Vol. 15, 2021, no. 4, 181 - 190
HIKARI Ltd, www.m-hikari.com
https://doi.org/10.12988/ija.2021.91564

An Approach in Computing the Frobenius Number of Numerical Semigroups with Embedding Dimension Equal to 3

Violeta Angjelkoska

Faculty of Information and Communication Technology
FON University, Skopje, Republic of North Macedonia

Dončo Dimovski

Macedonian Academy of Sciences and Arts
Skopje, Republic of North Macedonia

Irena Stojmenovska

Faculty of Computer Science and Information Technology
University American College, Skopje, Republic of North Macedonia

Abstract

We present a proof, based on the Euclidean algorithm, of a theorem for numerical semigroups with embedding dimension equal to 3, and thus we provide a characterization of the corresponding Frobenius number.

Keywords: Numerical semigroups, Frobenius number.

1 Introduction and preliminaries

Additive semigroups of nonnegative integers whose greatest common divisor of numbers is 1, are also called numerical semigroups. Numerical semigroups are interesting not only for their application in algebraic geometry, number theory, differential equations, cryptography, but also for the large number of open related questions.

Let $\mathbb{N}_0$ be the set of nonnegative integers and $\mathbb{N}$ be the set of positive integers. A **numerical semigroup** is a proper nonempty subset G of $\mathbb{N}_0$ that is closed under addition, contains the number 0 and $\mathbb{N}_0 \backslash G$ is finite. A set $S = \{a_1, \ldots, a_m\} \subseteq G$ is called a set of generators for G, denoted by $G = < S >$ or $G = < a_1, \ldots, a_m >$, if $G = \{\alpha_1 n_1 + \cdots + \alpha_m n_m | \alpha_1, \ldots, \alpha_m \in \mathbb{N}_0\}$. The set S is a **minimal set of generators** for G, if no proper subset of S is a set of generators for G. Every numerical semigroup G is finitely generated and it has a unique minimal set of generators.

The study of numerical semigroups is closely related to a determination and consequently application of the invariants within. Let G be a numerical semigroup. 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 for G is called the **multiplicity** of G, denoted by n. The largest number not belonging to a numerical semigroup G is called **Frobenius number**, denoted by $F(G)$. The set $\mathbb{N}_0 \backslash G$ is known as the set of **gaps**. Its cardinality is called **genus** of G and is denoted by $g(G)$. The **Apery set** of G with respect to an element $a \in G$ is the set $Ap(G, a) = \{x \in G | x - a \notin G\}$.

Finding $F(G)$ and $g(G)$ of a numerical semigroup G is equivalent to solving the Frobenius problem i.e., finding the largest positive integer that cannot be represented as a nonnegative integer linear combination of given positive coprime integers, and determining the number of such positive integers.

We came across several paper about Frobenius number of numerical semigroups with embedding dimension equal to 3 ([1]-[9]). In [2], there have been given a particular characterization of the Frobenius number of numerical semigroups with embedding dimension less or equal to 3.

In this paper, we present a proof of a theorem for numerical semigroups with embedding dimension equal to 3, similar to Theorem 4.3 in [2]. As a consequence, we provide an approach for computing the corresponding Frobenius number. 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 $\ominus$. 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. The multiplication of integers modulo n will be denoted by $\odot$. In continuation, we will use notations from [2]. For $i_1, \ldots, i_k \in \mathbb{Z}_n$ and $k \in \mathbb{N}$ the integer part $\left[\frac{i_1 + \ldots + i_k}{n}\right]$ will be denoted by $[n; i_1, \ldots, i_k]$. A numerical semigroup G will be denoted as $G = [n; T; B(T)]$, where n is multiplicity of G, $T \subseteq \mathbb{Z}_n \backslash \{0\}$ such that $< T > = \mathbb{Z}_n$ and $|T| = ed(G) - 1$, and $B(T) = \{b_s | s \in T\} \subseteq \mathbb{N}$ satisfies the following condition:

if $t \in T$ and $t = i_1 \oplus \ldots \oplus i_r$, за $i_1, \ldots, i_r \in T \backslash \{t\}$ and $r \in \mathbb{N}$, then

$$b_t < b_{i_1} + \ldots + b_{i_r} + [n; i_1, \ldots, i_r].$$

Theorem 1.1 (Theorem 4.3. in [2]). Let $G = \langle n, x, y \rangle$ be a numerical semigroup with $ed(G) = 3$. Then:

(i) There are unique $p, q, u, v \in \mathbb{N}$ 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

$$F(G) = px + vy - \frac{ux + qy - |ux - qy|}{2} - n - x - y. \blacksquare$$

We note that the procedure of finding $p, q, u, v \in \mathbb{N}$ from Theorem 1.1. is based on detecting corresponding minimal pairs of numbers. For deeper reading, see [2].

2 An approach in computing the Frobenius number of numerical semigroups with embedding dimension equal to 3

Bellow we present a result similar to the one obtained in Theorem 1.1, but in this case, the procedure allowing to compute the corresponding Frobenius number is based on the Euclidean algorithm.

Theorem 2.1. Let $G = [n; \{i, j\}; \{b_i, b_j\}]$ be a numerical semigroup such that $x = b_i n + i, y = b_j n + j,\ GCD(x, n) = GCD(y, n) = 1$ and $n < x < y$. Then

(i) There exist $p, q, r, s \in \mathbb{N}$ such that

$$0 < p \le q, 0 < r \le s,$$
$$qr + ps - pr = n, q \odot i = (s - r) \odot j, (q - p) \odot i = s \odot j,$$
$$qx > (s - r)y, (q - p)x < sy \text{ and}$$
$$Ap(G, n) = \{\alpha x + \beta y | 0 \le \alpha < q, 0 \le \beta < r\} \cup \{\alpha x + \beta y | 0 \le \alpha < p, 0 \le \beta < s\};$$

(ii) For the Frobenius number $F(G)$ we have

$$F(G) = qx + sy - \frac{(q - p)x + (s - r)y - |(q - p)x - (s - r)y|}{2} - n - x - y.$$

Proof. (i) We will consider the following four steps.

Step 1. Let $n_0 = n$ and $j_0 = j \odot i^{-1}$, where i^{-1} is the inverse of i modulo n. Since $n_0 > j_0$, by Euclidian algorithm we obtain te following equalities:

$$\begin{aligned} n_0 &= k_0 j_0 + n_1 \\ j_0 &= t_0 n_1 + j_1 \\ &\vdots \\ n_m &= k_m j_m + n_{m+1} \\ j_m &= t_m n_{m+1} + j_{m+1} \\ &\vdots \end{aligned} \tag{2.1}$$

where

$$n_0 > j_0 > n_1 > j_1 > \ldots > n_m > j_m > \ldots.$$

Since $n_0, j_0, n_1, j_1, \ldots \in \mathbb{N}$, the previous procedure ends after finite number of steps. Let d be a positive integer such that $j_d \neq 0$ and $j_{d+1} = 0$. The equalities (2.1), for $0 \le m \le d + 1$, can be written as

$$n_m = \alpha_m n_0 - \beta_m j_0, \text{ and}$$
$$j_m = \gamma_m j_0 - \delta_m n_0.$$

Hence, $\alpha_0 = 1, \beta_0 = 0, \gamma_0 = 1, \delta_0 = 0$, $\alpha_1 = 1, \beta_1 = k_0, \gamma_1 = 1 + t_0 k_0$ and $\delta_1 = t_0$. From $n_m = k_m j_m + n_{m+1}$, for $0 \le m \le d$, we have that

$$n_{m+1} = n_m - k_m j_m = \alpha_m n_0 - \beta_m j_0 - k_m(\gamma_m j_0 - \delta_m n_0) \text{ i.e.,}$$
$$n_{m+1} = (\alpha_m + k_m \delta_m) n_0 - (\beta_m + k_m \gamma_m) j_0.$$

Let

$$\alpha_{m+1} = \alpha_m + k_m \delta_m \text{ and } \beta_{m+1} = \beta_m + k_m \gamma_m.$$

Since $j_m = t_m n_{m+1} + j_{m+1}$, for $0 \le m \le d$, we obtain that

$$j_{m+1} = j_m - t_m n_{m+1} = \gamma_m j_0 - \delta_m n_0 - t_m(\alpha_{m+1} n_0 - \beta_{m+1} j_0) \text{ i.e.,}$$
$$j_{m+1} = (\gamma_m + t_m \beta_{m+1}) j_0 - (\delta_m + t_m \alpha_{m+1}) n_0.$$

Let

$$\gamma_{m+1} = \gamma_m + t_m \beta_{m+1} \text{ and } \delta_{m+1} = \delta_m + t_m \alpha_{m+1}.$$

Hence, for $0 \le m \le d$, we have that

$$n_{m+1} = \alpha_{m+1} n_0 - \beta_{m+1} j_0$$
$$n_{m+1} + \beta_{m+1} j_0 = \alpha_{m+1} n_0,$$

so

$$(n_{m+1} + \beta_{m+1} j_0)x \equiv (\alpha_{m+1} n_0)x (mod\, n) \text{ i.e.,}$$
$$n_{m+1} x + \beta_{m+1} j_0 x \equiv 0 (mod\, n).$$

From $j_0 x \equiv y (mod\, n)$, we obtain that

$$n_{m+1} x + \beta_{m+1} y \equiv 0 (mod\, n) \text{ i.e.,}$$
$$n_{m+1} x \equiv -\beta_{m+1} y (mod\, n).$$

Since $j_m = \gamma_m j_0 - \delta_m n_0$, for $0 \le m \le d$, we have that

$$j_m x = \gamma_m j_0 x - \delta_m n_0 x \equiv \gamma_m y (mod\, n) \text{ i.e.,}$$
$$(j_m - a n_{m+1})x \equiv (\gamma_m + a\beta_{m+1}) y (mod\, n),$$

Since

$$j_m = t_m n_{m+1} + j_{m+1} \text{ and } n_{m+1} \le j_m - a n_{m+1} < j_m,$$

we obtain that $0 \le a \le t_m - 1$. We will prove that for $0 \le a \le t_m - 1$ and $0 \le m \le d$ the following equality holds

$$(j_m - a n_{m+1})\beta_{m+1} + n_{m+1}(\gamma_m + (a+1)\beta_{m+1}) - n_{m+1}\beta_{m+1} = n.$$

Namely,

$$\begin{aligned}
&(j_m - a n_{m+1})\beta_{m+1} + n_{m+1}(\gamma_m + (a+1)\beta_{m+1}) - n_{m+1}\beta_{m+1} \\
&= j_m \beta_{m+1} - a n_{m+1}\beta_{m+1} + n_{m+1}\gamma_m + n_{m+1}(a+1)\beta_{m+1} - n_{m+1}\beta_{m+1} \\
&= j_m \beta_{m+1} - a n_{m+1}\beta_{m+1} + n_{m+1}\gamma_m + a n_{m+1}\beta_{m+1} + n_{m+1}\beta_{m+1} - n_{m+1}\beta_{m+1} \\
&= j_m \beta_{m+1} + n_{m+1}\gamma_m \\
&= (\gamma_m j_0 - \delta_m n_0)\beta_{m+1} + (\alpha_{m+1} n_0 - \beta_{m+1} j_0)\gamma_m \\
&= \gamma_m j_0 \beta_{m+1} - \delta_m n_0 \beta_{m+1} + \alpha_{m+1} n_0 \gamma_m - \beta_{m+1} j_0 \gamma_m \\
&= \alpha_{m+1} n_0 \gamma_m - \delta_m n_0 \beta_{m+1} = (\alpha_{m+1}\gamma_m - \delta_m \beta_{m+1}) n_0.
\end{aligned} \tag{2.2}$$

Furthermore,

$$\begin{aligned}
&(\alpha_{m+1}\gamma_m - \delta_m \beta_{m+1}) \\
&= (\alpha_m + k_m \delta_m)\gamma_m - \delta_m(\beta_m + k_m \gamma_m) \\
&= \alpha_m \gamma_m + k_m \delta_m \gamma_m - \delta_m \beta_m - \delta_m k_m \gamma_m \\
&= \alpha_m \gamma_m - \beta_m \delta_m \\
&= \alpha_m(\gamma_{m-1} + \beta_m t_m) - \beta_m(\delta_{m-1} + \alpha_m t_m) = \alpha_m \gamma_{m-1} - \beta_m \delta_{m-1} \\
&\vdots \\
&= \alpha_2 \gamma_1 - \beta_2 \delta_1
\end{aligned}$$

$$= (\alpha_1 + k_1\delta_1)\gamma_1 - \delta_1(\beta_1 + k_1\gamma_1)$$
$$= \alpha_1\gamma_1 + k_1\delta_1\gamma_1 - \delta_1\beta_1 - \delta_1 k_1\gamma_1 = \alpha_1\gamma_1 - \delta_1\beta_1$$
$$= 1 + t_0k_0 - t_0k_0 = 1.$$

Replacing this in (2.2), we obtain that

$$(j_m - an_{m+1})\beta_{m+1} + n_{m+1}(\gamma_m + (a+1)\beta_{m+1}) - n_{m+1}\beta_{m+1} = n. \quad (2.3)$$

Let

$$p_{m+1} = n_{m+1}, r_{m+1} = \beta_{m+1},$$
$$q_{m+1}^a = j_m - an_{m+1} = j_m - ap_{m+1} \text{ and}$$
$$s_{m+1}^{a+1} = \gamma_m + (a+1)\beta_{m+1} = \gamma_m + (a+1)r_{m+1}.$$

With these substitutions the equality (2.3) can be written as

$$q_{m+1}^a r_{m+1} + p_{m+1}s_{m+1}^{a+1} - p_{m+1}r_{m+1} = n, \quad (2.4)$$

for $0 \le m \le d$ and $0 \le a \le t_m - 1$, where $0 < p_{m+1} \le q_{m+1}^a$ and $0 < r_{m+1} \le s_{m+1}^{a+1}$. Moreover, the equation (2.4) can be written as

$$n = q_{m+1}^a s_{m+1}^{a+1} - (q_{m+1}^a - p_{m+1})(s_{m+1}^{a+1} - r_{m+1}). \quad (2.5)$$

Since $q_{m+1}^a x \equiv (s_{m+1}^{a+1} - r_{m+1})y(mod\, n)$, we obtain that

$$q_{m+1}^a \odot i = (s_{m+1}^{a+1} - r_{m+1})\odot j \quad (2.6)$$

and

$$q_{m+1}^a x + r_{m+1}y \equiv s_{m+1}^{a+1}y(mod\, n)$$
$$q_{m+1}^a x - p_{m+1}x \equiv s_{m+1}^{a+1}y(mod\, n)$$
$$(q_{m+1}^a - p_{m+1})x \equiv s_{m+1}^{a+1}y(mod\, n) \text{ i.e.,}$$
$$(q_{m+1}^a - p_{m+1})\odot i = s_{m+1}^{a+1}\odot j. \quad (2.7)$$

Since p_{m+1}, r_{m+1}, q_{m+1}^a, s_{m+1}^{a+1} are positive integers such that $0 < p_{m+1}$, r_{m+1}, q_{m+1}^a, $s_{m+1}^{a+1} < n$, for $0 \le m \le d$ and $0 \le a \le t_m - 1$, the case when $q_{m+1}^a = j_m - ap_{m+1} = 1$ will not be considered. Namely, for $p_{m+1} \le j_m - ap_{m+1} < j_m$ and $j_m - ap_{m+1} = 1$, there are the following two possibilities:

- $p_{d+1} = 0$, which implies that $j_d = 1$, $r_{d+1} = 0$ and from $(j_d - an_{d+1})x \equiv (\gamma_d + ar_{d+1})y(mod\, n)$, the only possible case is $x \equiv \gamma_d y(mod\, n)$. Hence, $t_d = 1$.
- $p_{d+1} = 1$, which implies that $j_d \neq 1$. Replacing this in (2.3) we obtain that $s_{d+1}^{t_d} = \gamma_d + (a+1)r_{m+1} = n$.

The procedure above determinates all the positive integers that satisfy the conditions (2.4), (2.6) and (2.7).

Step 2. We will consider sequences $\{u_b\}$ and $\{v_b\}$ with length $t_0 + \ldots + t_d + 2$ such that

$$u_1 = n, u_2 = q_1^0, \ldots, u_{t_0+1} = q_1^{t_0-1}, u_{t_0+2} = q_2^0, \ldots, u_{t_0+t_1+1} = q_2^{t_1-1}, \ldots,$$
$$u_{t_0+\ldots+t_{d-1}+2} = q_{d+1}^0, \ldots, u_{t_0+\ldots+t_d+1} = q_{d+1}^{t_d-1} \text{ and } u_{t_0+\ldots+t_d+2} = 0,$$

and

$$v_1 = 0, v_2 = s_0^1, v_3 = s_1^1, \ldots, v_{t_0+2} = s_1^{t_0}, v_{t_0+3} = s_2^1, \ldots, v_{t_0+t_1+2} = s_2^{t_1}, \ldots,$$
$$v_{t_0+\ldots+t_d+1} = s_{d+1}^{t_d-1} \text{ and } v_{t_0+\ldots+t_d+2} = s_{d+1}^{t_d},$$

where $q_1^0 = j_0$, $s_0^1 = q_{d+1}^{t_d-1} = 1$, $s_{d+1}^{t_d-1} = j_0^{-1}$ and $s_{d+1}^{t_d} = n$.

Since

$$n > q_1^0 > \ldots > q_1^{t_0-1} > q_2^0 > \ldots > q_2^{t_1-1} > \ldots > q_{d+1}^0 > \ldots > q_{d+1}^{t_d-1} > 0,$$

And

$$0 < s_0^1 < s_1^1 <\ldots< s_1^{t_0} < s_2^1 <\ldots< s_2^{t_1} <\ldots< s_{d+1}^1 <\ldots< s_{d+1}^{t_d-1} < s_{d+1}^{t_d} = n,$$

the sequence $\{u_b\}$ monotonically decreases and the sequence $\{v_b\}$ monotonically increases. Considering the construction of the sequences $\{u_b\}$ and $\{v_b\}$, it can be easily shown that

$$\begin{vmatrix} u_b & -v_b \\ -u_{b+1} & v_{b+1} \end{vmatrix} = u_b v_{b+1} - u_{b+1} v_b = n, \text{ for } 1 \le b \le t_0 + \ldots + t_d + 1, \text{ and}$$

$$u_b \odot i = v_b \odot j, \text{ for } 1 \le b \le t_0 + \ldots + t_d + 2.$$

Step 3. Next, we will show that there exists $b \in \mathbb{N}$, such that $2 \le b \le t_0 + \ldots + t_d$, $u_b x > v_b y$ and $u_{b+1} x < v_{b+1} y$. Since $i = (j^{-1} \odot i) \odot j$ we have that $b_i < (j^{-1} \odot i) b_j + [n, \underbrace{j, \ldots,}_{j^{-1}\odot i} j]$, which implies that $x = b_i n + i < (j^{-1} \odot i) y$.

Similarly, $y = b_j n + j < (i^{-1} \odot j) x$. Hence, there are $u, v \in \mathbb{Z}_n$ such that $ux > (u \odot j^{-1} \odot i) y$ and $vy > (v \odot i^{-1} \odot j) x$. Moreover, it is clear that $u, v \notin \{0, 1\}$ (by definition). So, let q and s are the smallest elements belonging to $\mathbb{Z}_n \backslash \{0,1\}$ such that $qx > (q \odot j^{-1} \odot i) y$ and $sy > (s \odot i^{-1} \odot j) x$. Then, for q_1 and s_1 such that $0 \le q_1 < q$ and $0 \le s_1 < q \odot j^{-1} \odot i$, we have that

$$q_1 \odot i \neq s_1 \odot j,$$

and for q_2 and s_2 such that $0 \le q_2 < s$ and $0 \le s_2 < s \odot i^{-1} \odot j$, we have that

$$q_2 \odot i \neq s_2 \odot j.$$

If $q \le s \odot j \odot i^{-1}$ then $sy > (s \odot j \odot i^{-1}) x \ge qx > (q \odot i \odot j^{-1}) y$, which implies that $s > q \odot i \odot j^{-1}$, and

$$\begin{aligned} (s - q \odot i \odot j^{-1}) y &= sy - (q \odot i \odot j^{-1}) y \\ &> (s \odot j \odot i^{-1}) x - (q \odot i \odot j^{-1}) y > (s \odot j \odot i^{-1}) x - qx \\ &= (s \odot j \odot i^{-1} - q) x = ((s - q \odot i \odot j^{-1}) \odot (j \odot i^{-1})) x. \end{aligned}$$

Hence, $s - q \odot i \odot j^{-1} < s$. This is in contradiction with the assumption that s is the smallest element in $\mathbb{Z}_n \backslash \{0,1\}$ such that $sy > (s \odot i^{-1} \odot j) x$. Therefore, $q > s \odot j \odot i^{-1}$.

If $s \le q \odot i \odot j^{-1}$ and if we consider the case $q > s \odot j \odot i^{-1}$, we have that

$$\begin{aligned} (q \odot i \odot j^{-1} - s) y &= (q \odot i \odot j^{-1}) y - sy \\ &< qx - (s \odot j \odot i^{-1}) x = (q - s \odot j \odot i^{-1}) x = ((q \odot i \odot j^{-1} - s) \odot (i^{-1} \odot j)) x. \end{aligned}$$

Hence, $q - s \odot i \odot j^{-1} < q$. This is in contradiction with the assumption that q is the smallest element in $\mathbb{Z}_n \backslash \{0, 1\}$ such that $qx > (q \odot j^{-1} \odot i) y$. Therefore, $s > q \odot i \odot j^{-1}$.

Step 4. We will firstly prove that $n = qs - (q \odot i \odot j^{-1})(s \odot j \odot i^{-1})$. Let

$$\begin{aligned} D = &\{(\gamma, \delta) | 0 \le \gamma < q, 0 \le \delta < s - q \odot i \odot j^{-1}\} \\ &\cup \{(\gamma, \delta) | 0 \le \gamma < q - s \odot j \odot i^{-1}, 0 \le \delta < s\} \text{ and} \end{aligned}$$

$$K = \{\gamma \odot i \oplus \delta \odot j) | (\gamma, \delta) \in D\}.$$

The fact that $GCD(n, i) = GCD(n, j) = 1$ 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 $(\alpha, \beta) \in D$ then $t \in K$. If $(\alpha, \beta) \notin D$, we need to consider the following 4 cases:

- $\alpha < q$, $\beta < s$ and $(\alpha, \beta) \notin D$;
- $\alpha \ge q$ and $\beta < s$;
- $\alpha < q$ and $\beta \ge s$;
- $\alpha \ge q$ and $\beta \ge s$.

Case 1. Let $\alpha < q$, $\beta < s$ and $(\alpha, \beta) \notin D$.

Since $(\alpha, \beta) \notin D$ it follows that

$$q - s \odot i^{-1} \odot j \leq \alpha < q \text{ and } s - q \odot i \odot j^{-1} \leq \beta < s.$$

So

$$(\alpha \ominus (q \ominus s \odot j \odot i^{-1})) \odot i \oplus (\beta \ominus (s \ominus q \odot i \odot j^{-1})) \odot j$$
$$= (\alpha - (q - s \odot j \odot i^{-1})) \odot i \oplus (\beta - (s - q \odot i \odot j^{-1})) \odot j$$
$$= \alpha \odot i \ominus q \odot i \oplus s \odot j \odot i^{-1} \odot i \oplus \beta \odot j \ominus s \odot j \oplus q \odot i \odot j^{-1} \odot j$$
$$= \alpha \odot i \ominus q \odot i \oplus s \odot j \oplus \beta \odot j \ominus s \odot j \oplus q \odot i$$
$$= \alpha \odot i \oplus \beta \odot j = t = \alpha' \odot i \oplus \beta' \odot j,$$

where $\alpha' = (\alpha - (q - s \odot j \odot i^{-1})) < \alpha < q$ and $\beta' = (\beta - (s - q \odot i \odot j^{-1})) < \beta < s$.

If $(\alpha', \beta') \in D$ then $t \in K$. If $(\alpha', \beta') \notin D$, then we repeat the discussion above and after a finite number of steps, we will obtain that $t \in K$.

Case 2. Let $\alpha \geq q$ and $\beta < s$.

If $s - q \odot i \odot j^{-1} \leq \beta < s$, as in Case 1, we have that

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

where $\alpha' = (\alpha - (q - s \odot j \odot i^{-1})) < \alpha < q$ and $\beta' = (\beta - (s - q \odot i \odot j^{-1}) < \beta < s$.

If $\beta < s - q \odot i \odot j^{-1} < s$, then $\beta + q \odot i \odot j^{-1} < s$ and

$$(\alpha \ominus q) \odot i \oplus (\beta \oplus q \odot i \odot j^{-1}) \odot j$$
$$= (\alpha - q) \odot i \oplus (\beta + q \odot i \odot j^{-1}) \odot j$$
$$= \alpha \odot i \ominus q \odot i \oplus \beta \odot j \oplus q \odot i = \alpha \odot i \oplus \beta \odot j = t = \alpha' \odot i \oplus \beta' \odot j,$$

where $\alpha' = \alpha - q < \alpha$ and $\beta < \beta' = \beta + q \odot i \odot j^{-1} < s$.

In both cases, $(\alpha', \beta') \in D$ implies that $t \in K$. Let $(\alpha', \beta') \notin D$. If (α', β') is as in Case 1, we obtain that $t \in K$. If (α', β') is not as in Case 1, then it is as in Case 2, and we repeat the discussion above. Consequently, after a finite number of steps we will obtain that $t \in K$.

Case 3. Let $\alpha < q$ and $\beta \geq s$.

This case is symmetric to Case 2.

Case 4. Let $\alpha \geq q$ and $\beta \geq s$.

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

$$\alpha' = (\alpha - (q - s \odot j \odot i^{-1})) < \alpha < q \text{ and } \beta' = (\beta - (s - q \odot i \odot j^{-1})) < \beta < s.$$

If $(\alpha', \beta') \in D$ then $t \in K$. If $(\alpha', \beta') \notin D$, we apply again one of the previous cases, and after a finite number of steps, we get that $t \in K$. All the above implies that $\mathbb{Z}_n \subseteq K$.

Next, we will prove that $t = 0$ is in K only for $(0,0) \in D$. It is easily seen that

$$(q - s \odot j \odot i^{-1}, s - q \odot i \odot j^{-1}) \notin D \text{ and}$$
$$(q - s \odot j \odot i^{-1}) \odot i \oplus (s - q \odot i \odot j^{-1}) \odot j = 0.$$

Assume the contrary i.e., let exist some α' and β' such that $0 < \alpha' < q - s \odot j \odot i^{-1}$ and $0 < \beta' < s$, satisfying $\alpha' \odot i \oplus \beta' \odot j = 0$. Then, $\alpha' + s \odot j \odot i^{-1} < q$, $s - \beta' < s$ and

$$(\alpha' + s \odot j \odot i^{-1}) \odot i = (s - \beta') \odot j \text{ i.e.,}$$
$$(\alpha' + s \odot j \odot i^{-1}) x \equiv (s - \beta') y (mod\, n).$$

If $(\alpha' + s\odot j\odot i^{-1})x > (s-\beta')y$, then being $x<y$ and $\alpha'\odot i\oplus\beta'\odot j = 0$, we obtain that

$$(\alpha' + s\odot j\odot i^{-1})x > (s-\beta')y = (s+\alpha'\odot i\odot j^{-1})y$$
$$= \big((\alpha' + s\odot j\odot i^{-1})\odot i\odot j^{-1}\big)y,$$

which contradicts to the assumption for s. Similarly, we conclude that the inequality $(\alpha' + s\odot j\odot i^{-1})x < (s-\beta')y$ does not hold. Hence, $\alpha' \geq q - s\odot j\odot i^{-1}$ or $\beta' \geq s$. Next, let $q - s\odot j\odot i^{-1} \leq \alpha' < q$ and $0 < \beta' < s - q\odot i\odot j^{-1}$. We assume that there are α' and β' such that $q - s\odot j\odot i^{-1} \leq \alpha' < q$, $0 < \beta' < s - q\odot i\odot j^{-1}$ and $\alpha'\odot i\oplus\beta'\odot j = 0$. Then $q-\alpha' < q$, $\beta' + q\odot i\odot j^{-1} < s$ and

$$(q-\alpha')\odot i = (\beta' + q\odot i\odot j^{-1})\odot j \text{ i.e.,}$$
$$(q-\alpha')x \equiv (\beta' + q\odot i\odot j^{-1})y (mod\, n).$$

If $(q-\alpha')x > (\beta' + q\odot i\odot j^{-1})y$, then from $x<y$ and $\alpha'\odot i\oplus\beta'\odot j = 0$ we obtain that

$$(q-\alpha')x > (\beta' + q\odot i\odot j^{-1})y = (q\odot i\odot j^{-1} - \alpha'\odot i\odot j^{-1})y$$
$$= ((q-\alpha')'\odot i\odot j^{-1})y,$$

which contradicts to the assumption for q. Again, we conclude similarly that the inequality $(q-\alpha')x < (\beta' + q\odot i\odot j^{-1})y$ does not hold.

Hence, $t=0$ is in K only for $(0,0) \in D$. Next, let $(\alpha_1,\beta_1),(\alpha_2,\beta_2) \in D$ and

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

Since $t=0$ is in K only for $(0,0) \in D$, we have that $\alpha_1 \ominus \alpha_2 = 0$ and $\beta_1 \ominus \beta_2 = 0$. This, together with $0 < \alpha_1,\alpha_2,\beta_1,\beta_2 < n$ implies that $(\alpha_1,\beta_1) = (\alpha_2,\beta_2)$. From the above it follows that the elements of the set K are incongruent modulo n. Thus $K \subseteq \mathbb{Z}_n$. This, together with $\mathbb{Z}_n \subseteq K$ implies that $K = \mathbb{Z}_n$ i.e.,

$$|K| = n \text{ and } n = qs - (q\odot i\odot j^{-1})(s\odot j\odot i^{-1}).$$

From the previous discussion, we conclude that numbers $q, s, q\odot i\odot j^{-1}$ and $s\odot j\odot i^{-1}$ satisfy equalities (2.4), (2.5), (2.6) and (2.7). Moreover, $q > s\odot j\odot i^{-1}$ and $s > q\odot i\odot j^{-1}$.

Hence, there is a unique $b \in \mathbb{N}$, satisfying $2 \leq b \leq t_0 + \ldots + t_d$, and u_b, u_{b+1}, v_{b+1} and v_b, elements of the corresponding sequences $\{u_b\}$ and $\{v_b\}$ from Step 2, such that

$$u_b = q, u_{b+1} = s\odot j\odot i^{-1}, v_{b+1} = s \text{ and } v_b = q\odot i\odot j^{-1}.$$

Furthermore, there exist nonnegative integers m and a such that

$$0 \leq m \leq d, 0 \leq a \leq t_m - 1,$$
$$q = u_b = q_{m+1}^{a}, s = v_{b+1} = s_{m+1}^{a+1}, s_{m+1}^{a+1} - r_{m+1} = q\odot i\odot j^{-1} \text{ and}$$
$$q_{m+1}^{a} - p_{m+1} = s\odot j\odot i^{-1}.$$

Let $r = r_{m+1}$ and $p = p_{m+1}$. Then

$$r = r_{m+1} = v_{b+1} - v_b, p = p_{m+1} = u_b - u_{b+1},$$
$$0 < p \leq q, 0 < r \leq s,$$
$$qr + ps - pr = n, q\odot i = (s-r)\odot j, (q-p)\odot i = s\odot j,$$
$$qx > (s-r)y \text{ and } (q-p)x < sy.$$

Summing all up, the results obtained in the steps we have considered, we conclude that

$$Ap(G,n) = \{\alpha x + \beta y | 0 \leq \alpha < q, 0 \leq \beta < r\} \cup \{\alpha x + \beta y | 0 \leq \alpha < p, 0 \leq \beta < s\}.$$

(ii) From (i) we have that

$$F(G) = (q-1)x + (s-1)y - min\{(q-p)x, (s-r)y\} - n \text{ i.e,}$$

$$F(G) = qx + sy - \frac{(q-p)x + (s-r)y - |(q-p)x - (s-r)y|}{2} - n - x - y. \blacksquare$$

Consequently, and according to the construction in the proof of Theorem 2.1, we get the following:

For a given numerical semigroup $G = \langle n, x, y \rangle$ such that $ed(G) = 3, n < x < y$, $GCD(x, n) = GCD(y, n) = 1, x \equiv i(mod\, n)$ and $y \equiv j(mod\, n)$, there exists a unique $b \in \mathbb{N}$ satisfying $2 \le b \le t_0 + \ldots + t_d + 1$, and also u_b, u_{b+1}, v_b and v_{b+1} (elements of sequences $\{u_b\}$ and $\{v_b\}$), such that $u_b x > v_b y$ and $u_{b+1} x < v_{b+1} y$. Hence, the numerical semigroup $G = \langle n, x, y \rangle$ is determined by the matrix $\begin{bmatrix} u_b & -v_b \\ -u_{b+1} & v_{b+1} \end{bmatrix}$.

Since $u_b x > v_b y$ and $u_{b+1} x < v_{b+1} y$ i.e., $\frac{y}{x} < \frac{u_b}{v_b}$ and $\frac{y}{x} > \frac{u_{b+1}}{v_{b+1}}$ we have that

$$\frac{u_{b+1}}{v_{b+1}} < \frac{y}{x} < \frac{u_b}{v_b}.$$

Combining the condition $\frac{u_{b+1}}{v_{b+1}} < \frac{u_b}{v_{b+1}} < \frac{u_b}{v_b}$ with Theorem 2.1, for the corresponding Frobenius number $F(G)$ we obtain that

$$F(G) = \begin{cases} (u_b - u_{b+1})x + v_{b+1}y - n - x - y, & \frac{u_b}{v_{b+1}} \le \frac{y}{x} < \frac{u_b}{v_b} \\ u_b x + (v_{b+1} - v_b)y - n - x - y, & \frac{u_{b+1}}{v_{b+1}} < \frac{y}{x} < \frac{u_b}{v_{b+1}}. \end{cases}$$

References

[1] J. L. R. Alfonsín, *The Diophantine Frobenius Problem*, Oxford University Press, Oxford, 2005. https://doi.org/10.1093/acprof:oso/9780198568209.001.0001

[2] V. Angjelkoska, D. Dimovski, Additive semigroups of integers. Embedding dimension of numerical semigroups, *Contributions*, *Masa*, **41** (2020), 49–55.

[3] J. L. Davison, On the linear Diophantine problem of Frobenius, *Journal of Number Theory*, **48** (1994), 353–363. https://doi.org/10.1006/jnth.1994.1071

[4] H. Greenberg, Solution to a linear diophantine equation for nonnegative integers, *Journal of Algorithms,* **9** (1988), 343-353. https://doi.org/10.1016/0196-6774(88)90025-9

[5] S. M. Johnson, A linear Diophantine Problem, *Canadian Journal of Mathematics*, **12 (**1960), 390–398. https://doi.org/10.4153/cjm-1960-033-6

[6] A. Mahdavi, F. Rahmati, On numerical semigroups with embedding dimension three, *Transactions on Combinatorics*, **6** (2017), 1-6.

[7] A. M. Robles-Perez, J. C. Rosales, The Frobenius problem for numerical semigroups with embedding dimension equal to three, *Mathematics of coputaton*, **81** (2012), 1609-1617. https://doi.org/10.1090/s0025-5718-2011-02561-5

[8] J. C. Rosales, M. B. Branco, The Frobenius problem for numerical semigroups, *Journal of Number theory*, **131** (2011), 2310-2319. https://doi.org/10.1016/j.jnt.2011.05.011

[9] J. C. Rosales, P. A. García-Sánchez, *Numerical Semigroups*, Developments in Mathematics, Springer, New York, 2009. https://doi.org/10.1007/978-1-4419-0160-6

Received: July 7, 2021; Published: July 23, 2021