THE FROBENIUS PROBLEM IN DIMENSION THREE

AURELIANO M. ROBLES-PÉREZ AND JOSÉ CARLOS ROSALES

Abstract. Let S be a numerical semigroup with embedding dimension three. If its minimal generators are pairwise relatively prime numbers, then we give semi-explicit formulas for the Frobenius number and the genus of S in such way that, if the multiplicity of S is fixed, then they become explicit.

1. Introduction

Let $\mathbb{N}$ be the set of nonnegative integers. A *numerical semigroup* is a subset S of $\mathbb{N}$ that is closed under addition, $0 \in S$ and $\mathbb{N} \setminus S$ is finite. The elements of $\mathbb{N} \setminus S$ are the *gaps* of S, and the cardinality of such a set is called the *genus* of S, denoted by $\mathrm{g}(S)$. The *Frobenius number* of S is the largest integer that does not belong to S and it is denoted by $\mathrm{F}(S)$.

If $A \subseteq \mathbb{N}$ is a nonempty set, then $\langle A \rangle$ is the submonoid of $(\mathbb{N}, +)$ generated by A, that is, $\langle A \rangle = \{\lambda_1 a_1 + \ldots + \lambda_n a_n \mid n \in \mathbb{N} \setminus \{0\},\ a_1, \ldots, a_n \in A,\ \lambda_1, \ldots, \lambda_n \in \mathbb{N}\}$. In [8] it is proved that $\langle A \rangle$ is a numerical semigroup if and only if $\gcd\{A\} = 1$, where gcd means *greatest common divisor*.

It is well known (see [8]) that every numerical semigroup S admits a *unique minimal system of generators* $X = \{n_1 < n_2 < \ldots < n_e\}$, that is, $X \subseteq S$ is a finite set such that $S = \langle X \rangle$ and, in addition, no proper subset of X generates S. The integers e and n_1 are known as the *embedding dimension* ($\mathrm{e}(S)$) and the *multiplicity* ($\mathrm{m}(S)$) of S, respectively.

The Frobenius problem (see [3]) consists of finding formulas for the Frobenius number and the genus of a numerical semigroup in terms of its minimal system of generators. The problem was solved by Sylvester and Curran Sharp (see [9]) when the embedding dimension is two. In fact, if $S = \langle n_1, n_2 \rangle$, then $\mathrm{F}(S) = n_1 n_2 - n_1 - n_2$ and $\mathrm{g}(S) = \frac{(n_1-1)(n_2-1)}{2}$.

At present, this problem is open for embedding dimensions greater than or equal to three. To be precise, in [1] Curtis showed that it is impossible to find a polynomial formula (that is, a finite set of polynomials) that computes the Frobenius number if the embedding dimension is equal to three. On the other hand, several authors (see [6, 3]) have developed algorithms that compute the Frobenius number for each numerical semigroup with dimension three. Actually, in [4] Ramírez-Alfonsín and Rødseth obtain an efficient algorithm that computes certain parameters, and then give a semi-explicit formula for the Frobenius number. Our aim is to highlight the possibility of obtaining an explicit formula if the multiplicity is fixed.

If m is a positive integer, we denote by $\mathfrak{L}(m)$ the set of numerical semigroups with multiplicity m and embedding dimension three. Using the concept of *set of chained solutions* of certain system of equations, we will solve explicitly the Frobenius problem for $\mathfrak{L}(m)$.

Both of the authors are supported by FQM-343 (Junta de Andalucía), MTM2010-15595 (MICINN, Spain), and FEDER funds. The second author is also partially supported by Junta de Andalucía/Feder grant number FQM-5849.

2. Background

Let $\{n_1, n_2, n_3\}$ be the minimal system of generators of a numerical semigroup S. If $d = \gcd\{n_1, n_2\}$, it is well known (see [2, 6]) that $\mathrm{F}(S) = d\,\mathrm{F}\left(\langle \frac{n_1}{d}, \frac{n_2}{d}, n_3\rangle\right) + (d-1)n_3$ and $\mathrm{g}(S) = d\,\mathrm{g}\left(\langle \frac{n_1}{d}, \frac{n_2}{d}, n_3\rangle\right) + \frac{(d-1)(n_3-1)}{2}$.

Remark 2.1. Let S be a numerical semigroup minimally generated by $\{n_1, n_2, n_3\}$. In [8, Chapter 9] it is proved that S is a symmetric numerical semigroup if and only if there exists a rearrangement of its generators such that $\mathrm{e}\left(\langle \frac{n_1}{d}, \frac{n_2}{d}, n_3\rangle\right) = 2$ with $d = \gcd\{n_1, n_2\}$. Thus, we have that $\mathrm{F}(S) = \frac{1}{d}n_1n_2 - n_1 - n_2 + (d-1)n_3$ $\left(\text{and } \mathrm{g}(S) = \frac{\mathrm{F}(S)+1}{2}\right)$ in such a case.

Therefore, we can focus our attention on numerical semigroups whose three minimal generators m_1, m_2, m_3 are pairwise relatively prime numbers (that is, non-symmetric numerical semigroups). Moreover, and without loss of generality, we will suppose that $m_1 < m_2 < m_3$.

We will say that $(a_1, \ldots, a_n)$ is an *integer n-tuple* if $a_1, \ldots, a_n \in \mathbb{Z}$ (where $\mathbb{Z}$ is the set of integers). We will say that the n-tuple $(a_1, \ldots, a_n)$ is *strongly positive* if $a_1, \ldots, a_n \in \mathbb{N} \setminus \{0\}$.

The next result will be fundamental for our purpose.

Lemma 2.2. [7, Theorem 8] *Let m_1, m_2, m_3 be pairwise relatively prime positive integers. Then the system of equations*

$$\left\{\begin{array}{l} m_1 = x_{12}x_{13} + x_{12}x_{23} + x_{13}x_{32} \\ m_2 = x_{13}x_{21} + x_{21}x_{23} + x_{23}x_{31} \\ m_3 = x_{12}x_{31} + x_{21}x_{32} + x_{31}x_{32} \end{array}\right. \tag{1}$$

has a strongly positive integer solution if and only if $\mathrm{e}(\langle m_1, m_2, m_3\rangle) = 3$. *Moreover, if such a solution exists, then it is unique.*

Let $S = \langle m_1, m_2, m_3\rangle$. If $(x_{12}, x_{13}, x_{23}, x_{32}, x_{21}, x_{31}) = (r_{12}, r_{13}, r_{23}, r_{32}, r_{21}, r_{31})$ is the solution of system (1), we denote by $\mathrm{Six}(S) = (r_{12}, r_{13}, r_{23}, r_{32}, r_{21}, r_{31})$. The importance of knowing $\mathrm{Six}(S)$ is shown in the following result.

Lemma 2.3. [7, Propositions 15 and 17] *Under the above conditions, we have that*

(1) $\mathrm{F}(\langle m_1, m_2, m_3\rangle) = \frac{1}{2}((c_1-2)m_1 + (c_2-2)m_2 + (c_3-2)m_3 + |r_{23}m_3 - r_{32}m_2|)$,
(2) $\mathrm{g}(\langle m_1, m_2, m_3\rangle) = \frac{1}{2}((c_1-1)m_1 + (c_2-1)m_2 + (c_3-1)m_3 - c_1c_2c_3 + 1)$,

where $c_1 = r_{21} + r_{31}$, $c_2 = r_{12} + r_{32}$, and $c_3 = r_{13} + r_{23}$.

3. Sets of chained solutions

Let us observe that, if m_1, m_2, m_3 are pairwise relatively prime positive integers such that $\mathrm{e}(\langle m_1, m_2, m_3\rangle) = 3$, then there exists $k \in \{2, \ldots, m_1 - 1\}$ such that $\gcd\{k, m_1\} = 1$ and $m_3 \equiv km_2 \pmod{m_1}$. From now on we assume these conditions.

Proposition 3.1. *Let $(x_{12}, x_{13}, x_{23}, x_{32}) = (a_{12}, a_{13}, a_{23}, a_{32})$ be a strongly positive integer solution of $m_1 = x_{12}x_{13} + x_{12}x_{23} + x_{13}x_{32}$. Then there exist a_{21}, a_{31} positive integers such that $(a_{12}, a_{13}, a_{23}, a_{32}, a_{21}, a_{31})$ is a strongly positive integer solution of (1) if and only if the following conditions are fulfilled:*

1) $a_{12} + a_{32} - ka_{23} \equiv 0 \pmod{m_1}$;
2) $ka_{13} + ka_{23} - a_{32} \equiv 0 \pmod{m_1}$;

3) $\frac{a_{23}}{a_{12}+a_{32}} < \frac{m_2}{m_3} < \frac{a_{13}+a_{23}}{a_{32}}$.

As a consequence of Proposition 3.1, we have that the unique strongly positive integer solution of (1) is an extension of a strongly positive integer solution of the system

$$\left\{\begin{array}{rcll} x_{12}x_{13}+x_{12}x_{23}+x_{13}x_{32} & = & m_1 & \\ x_{12}+x_{32}-kx_{23} & \equiv & 0 & \pmod{m_1} \\ kx_{13}+kx_{23}-x_{32} & \equiv & 0 & \pmod{m_1}. \end{array}\right. \tag{2}$$

If (a,b,c,d) is a strongly positive integer 4-tuple, then we denote by $\mathrm{I}(a,b,c,d)$ the open interval $\left]\frac{c}{a+d}, \frac{b+c}{d}\right[$.

Lemma 3.2. *Let $X = \{s_1, \ldots, s_n\}$ be a set of strongly positive integer solutions of (2) such that*

1) *the initial end of $\mathrm{I}(s_1)$ is $\frac{1}{k}$;*
2) *for each $i \in \{1, \ldots, n-1\}$, the final end of $\mathrm{I}(s_i)$ is equal to the initial end of $\mathrm{I}(s_{i+1})$;*
3) *the final end of $\mathrm{I}(s_n)$ is greater than or equal to one.*

Then there exists a unique $i \in \{1, \ldots, n\}$ such that $\frac{m_2}{m_3} \in \mathrm{I}(s_i)$.

A set X as in Lemma 3.2 will be called a *set of chained solutions* of (2).

Theorem 3.3. *Let $X = \{s_1, \ldots, s_n\}$ be a set of chained solutions of (2). If $\frac{m_2}{m_3} \in \mathrm{I}(s_i)$ and $s_i = (a_{12}, a_{13}, a_{23}, a_{32})$, then*

$$\mathrm{Six}(\langle m_1, m_2, m_3\rangle) = \left(a_{12}, a_{13}, a_{23}, a_{32}, \frac{(a_{12}+a_{32})m_2 - a_{23}m_3}{m_1}, \frac{(a_{13}+a_{23})m_3 - a_{32}m_2}{m_1}\right).$$

As a consequence of Theorem 3.3, if we have a set of chained solutions of (2), then we have a formula for $\mathrm{Six}(S)$. Therefore, we need a procedure to compute such a set. As usual, if x is a real number, then we set $\lfloor x \rfloor = \max\{z \in \mathbb{Z} \mid z \le x\}$. Moreover, if a, b are integers such that $b \neq 0$, then $a \bmod b = a - \left\lfloor \frac{a}{b} \right\rfloor b$.

Lemma 3.4. *Under the stated conditions,*

(1) $(x_{12}, x_{13}, x_{23}, x_{32}) = \left(m_1 \bmod k, \left\lfloor \frac{m_1}{k} \right\rfloor, 1, k - m_1 \bmod k\right)$ *is a strongly positive integer solution of (2).*
(2) *if $(x_{12}, x_{13}, x_{23}, x_{32}) = (a_{12}, a_{13}, a_{23}, a_{32})$ is a strongly positive integer solution of (2) and $a_{32} > a_{12}$, then $(x_{12}, x_{13}, x_{23}, x_{32}) = (a_{12}, a_{13}, a_{13}+a_{23}, a_{32}-a_{12})$ is another strongly positive integer solution of (2). Moreover, the final end of $\mathrm{I}(a_{12}, a_{13}, a_{23}, a_{32})$ and the initial end of $\mathrm{I}(a_{12}, a_{13}, a_{13}+a_{23}, a_{32}-a_{12})$ are equal.*
(3) *if $(x_{12}, x_{13}, x_{23}, x_{32}) = (a_{12}, a_{13}, a_{23}, a_{32})$ is a strongly positive integer solution of (2), $a_{12} \ge a_{32}$, and the final end of $\mathrm{I}(a_{12}, a_{13}, a_{23}, a_{32})$ is less than one, then $(x_{12}, x_{13}, x_{23}, x_{32}) = (a_{12}-(t-1)a_{32}, ta_{13}+(t-1)a_{23}, a_{13}+a_{23}, ta_{32}-a_{12})$ is another strongly positive integer solution of (2) for $t = \left\lfloor \frac{a_{12}}{a_{32}} \right\rfloor + 1$. Moreover, the initial end of $\mathrm{I}(a_{12}-(t-1)a_{32}, ta_{13}+(t-1)a_{23}, a_{13}+a_{23}, ta_{32}-a_{12})$ is equal to the final end of $\mathrm{I}(a_{12}, a_{13}, a_{23}, a_{32})$.*

By beginning with the solution given in Lemma 3.4-(1), if we apply the constructions of Lemma 3.4-(2,3) in a suitable order, then we get that there the exists a set of chained solutions of (2).

Remark 3.5. See [5] for more details about the proofs of the results of this section.

4. An example

In order to clarify our results, let us see an example.

Example 4.1. Let us have $S \in \mathfrak{L}(5)$ and let $m_1 = 5 < m_2 < m_3$ be the minimal generators of S. Then $m_3 \equiv km_2 \pmod 5$ for some $k \in \{2,3,4\}$. Consequently, we have that,

- if $m_3 \equiv 2m_2 \pmod 5$, then $X = \{(1,2,1,1)\}$ is a set of chained solutions of (2). Therefore, $\mathrm{Six}(\langle 5, m_2, m_3\rangle) = \left(1,2,1,1,\frac{2m_2-m_3}{5},\frac{3m_3-m_2}{5}\right)$, $\mathrm{F}(S) = 2m_3 - 5$, and $\mathrm{g}(S) = \frac{2m_2+4m_3}{5} - 2$.
- if $m_3 \equiv 3m_2 \pmod 5$, then $X = \{(2,1,1,1)\}$ is a set of chained solutions of (2). Therefore, $\mathrm{Six}(\langle 5, m_2, m_3\rangle) = \left(2,1,1,1,\frac{3m_2-m_3}{5},\frac{2m_3-m_2}{5}\right)$, $\mathrm{F}(S) = m_2 + m_3 - 5$, and $\mathrm{g}(S) = \frac{4m_2+2m_3}{5} - 2$.
- if $m_3 \equiv 4m_2 \pmod 5$, then $X = \{(1,1,1,3),(1,1,2,2)\}$ is a set of chained solutions of (2). Therefore,
  - if $\frac{m_2}{m_3} < \frac{2}{3}$, then $\mathrm{Six}(\langle 5, m_2, m_3\rangle) = \left(1,1,1,3,\frac{4m_2-m_3}{5},\frac{2m_3-3m_2}{5}\right)$, $\mathrm{F}(S) = \frac{1}{2}\left(3m_2 + m_3 + |3m_2 - m_3|\right) - 5$, and $\mathrm{g}(S) = \frac{6m_2+m_3}{5} - 2$.
  - if $\frac{m_2}{m_3} > \frac{2}{3}$, then $\mathrm{Six}(\langle 5, m_2, m_3\rangle) = \left(1,1,2,2,\frac{3m_2-2m_3}{5},\frac{3m_3-2m_2}{5}\right)$, $\mathrm{F}(S) = 2m_3 - 5$, and $\mathrm{g}(S) = \frac{3m_2+3m_3}{5} - 2$.

Remark 4.2. Let us observe that we only have used Lemma 3.4-(1,2) in the previous example. For using Lemma 3.4-(3) it is necessary a multiplicity greater than or equal to eleven. Thus, if we take $m_1 = 101$ and $k = 72$, then $X = \{(29,1,1,43),(29,1,2,14),(1,7,3,13),(1,7,10,12)\}$ is a set of chained solutions of (2).

References

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

[2] S. M. Johnson, *A linear Diophantine problem*, Canad. J. Math. **12** (1960), 390–398.

[3] J. L. Ramírez Alfonsín, *The Diophantine Frobenius problem*, Oxford Univ. Press, 2005.

[4] J. L. Ramírez Alfonsín and Ø. J. Rødseth, *Numerical semigroups: Apéry sets and Hilbert series*, Semigroup Forum **79** (2009), 323–340.

[5] A. M. Robles-Pérez and J. C. Rosales, *The Frobenius problem for numerical semigroups with embbeding dimension equal to three*, to appear in Math. Comput. doi:10.1090/S0025-5718-2011-02561-5.

[6] Ö. J. Rödseth, *On a linear Diophantine problem of Frobenius*, J. Reine Angew. Math. **301** (1978), 171–178.

[7] J. C. Rosales and P. A. García-Sánchez, *Numerical semigroups with embbeding dimension three*, Arch. Math. (Basel) **83** (2004), 488–496.

[8] J. C. Rosales and P. A. García-Sánchez, *Numerical semigroups*, Developments in Mathematics, vol. **20**, Springer, New York, 2009.

[9] J. J. Sylvester, *Problem 7382, The Educational Times, and Journal of the College of Preceptors, New Series*, **36(266)** (1883), 177. Solution by W. J. Curran Sharp, ibid., **36(271)** (1883), 315.

A.M. Robles-Pérez, Department of Applied Mathematics, University of Granada
E-mail address: `arobles@ugr.es`

J.C. Rosales, Department of Algebra, University of Granada
E-mail address: `jrosales@ugr.es`