www.combinatorics.ir

Transactions on Combinatorics
ISSN (print): 2251-8657, ISSN (on-line): 2251-8665
Vol. 6 No. 2 (2017), pp. 1-6.

www.ui.ac.ir

ON NUMERICAL SEMIGROUPS WITH EMBEDDING DIMENSION THREE

ALI MAHDAVI AND FARHAD RAHMATI*

Communicated by Dariush Kiani

Abstract. Let $f \neq 1, 3$ be a positive integer. We prove that there exists a numerical semigroup S with embedding dimension three such that f is the Frobenius number of S. We also show that the same fact holds for affine semigroups in higher dimensional monoids.

1. **Introduction and basic notations**

This note is motivated by results of [8], that every positive integer is the Frobenius number of a numerical semigroup with at most three generators. The main result in this note is that every positive integer $f \neq 1, 3$, is the Frobenius number of a numerical semigroup with embedding dimension three (see Theorem 2.4). The set of nonnegative integers will be denoted by $\mathbb{N}$. A numerical semigroup S is a submonoid of $\mathbb{N}$ such that $\mathbb{N} \backslash S$ is finite. Applications of numerical semigroups are found in the study of the parameters of Algebraic Geometry codes and cryptography (see [4],[6]). For a nonempty subset A of $\mathbb{N}$, we will denote by $\langle A \rangle$ the submonoid of $\mathbb{N}$ generated by A. It is well known that $\langle A \rangle$ is a numerical semigroup if and only if $\gcd(A) = 1$ ([9, Lemma 2.1]). Let S be a numerical semigroup generated by $A = \{a_1, a_2, \ldots, a_n\}$. If no proper subset of A generates S, the set A is called a minimal system of generators of S. Every numerical semigroup has a unique minimal system of generators which is a finite set ([9, Theorem 2.7]). The cardinality of the minimal system of generators of S is called the embedding dimension of S and will be denoted by $e(S)$. For $a \in S \backslash \{0\}$ we define the Apéry set of a in S as the set

$$\mathrm{Ap}(S, a) = \{ s \in S \,|\, s - a \notin S \} .$$

MSC(2010): 20M05, 20M14, 11D07.

Keywords: Frobenius number, Frobenius vector, Numerical semigroup, simplicial affine semigroup.

Received: 11 July 2016, Accepted: 25 September 2016.

*Corresponding author.

This set has precisely a elements, which can be denoted by $\omega_0, \omega_1, \ldots, \omega_{a-1}$, where ω_i is the smallest element of S in respective congruences class mod a, for all $i \in \{0, \ldots, a-1\}$ (see [9, Lemma 2.4]).

The Frobenius number of a numerical semigroup S, generated by $a_1, \ldots, a_n$ is the largest integer $f^*(S)$ such that the linear equation $a_1x_1 + \cdots + a_nx_n = f^*(S)$ does not have any non-negative integer solutions. Note that $f^*(S)$ is the largest integer not belonging to S. It is not hard to show that $f^*(S) + a$ is the greatest element, $\max(\mathrm{Ap}(S, a))$, in $\mathrm{Ap}(S, a)$. The Frobenius number of a semigroup has been investigated by several authors ([3],[5],[7]). For $n = 2$, Sylvester proved in [12] that $f^*(\langle a_1, a_2\rangle) = a_1a_2 - a_1 - a_2$. But if $n \geq 3$, no closed formula is known ([3]). From Sylvester's formula, for a two-generators numerical semigroup S, $f^*(S)$ is always an odd integer and for every odd integer f, $f^*(\langle 2, f + 2\rangle) = f$.

The Frobenius problem is generelized to higher dimensional cases (see [1], [2], [13], [14]). In the last section we show that every vector $f \in \mathbb{N}^r \backslash E_r \cup 3E_r$ is the minimal Frobenius vector of an affine semigroup S minimally generated by $r + 1$ elements.

2. One dimensional case

To prove our main result we start by proving the following proposition.

Proposition 2.1. *Let f be a positive integer. If $12 | f$, then there exists a numerical semigroup S with $e(S) = 3$ such that $f^*(S) = f$.*

Proof. Let r and m be integers such that $f = 3^r m$ with $(3, m) = 1$. Set $a_1 = 3^{r+1}, a_2 = \frac{m}{2} + 3, a_3 = 3^r\frac{m}{4} + \frac{m}{2} + 3$ and $S = \mathbb{N}a_1 + \mathbb{N}a_2 + \mathbb{N}a_3$. Since $(3, m) = 1$, we have $\gcd(a_1, a_2, a_3) = 1$. We first show that $e(S) = 3$. Let $a_3 = n_1a_1 + n_2a_2$, for some $n_1, n_2 \in \mathbb{N}$. As $(3, m) = 1$, we have $n_2 \neq 0$. So

$$3^r\frac{m}{4} = n_1 3^{r+1} + (n_2 - 1)(\frac{m}{2} + 3) \Rightarrow (\frac{m}{4} - 3n_1)3^r = (n_2 - 1)(\frac{m}{2} + 3)$$

and thus $3^r | (n_2 - 1)$. Hence $3^r \leq n_2 - 1$, which implies $\frac{m}{2} + 3 \leq \frac{m}{4} - 3n_1$, contradicting that $m, n_1 \in \mathbb{N}$. So $e(S) = 3$. One can easily check that

(1) $3a_3 = \frac{m}{4}a_1 + 3a_2$;
(2) $(\frac{a_1}{3} + 2)a_2 = a_1 + 2a_3$;
(3) $(\frac{a_1}{3} - 1)a_2 + a_3 = (\frac{m}{4} + 1)a_1$.

Every element in $\mathrm{Ap}(S, a_1)$ is a linear combination of a_2 and a_3. Let

$$B = \big\{0, a_2, 2a_2, \ldots, (\tfrac{a_1}{3} + 1)a_2, a_3, 2a_3, a_2 + a_3, 2a_2 + a_3, \ldots, (\tfrac{a_1}{3} - 2)a_2 + a_3, a_2 + 2a_3, 2a_2 + 2a_3, \ldots, (\tfrac{a_1}{3} - 2)a_2 + 2a_3\big\}.$$

Using the relations (1), (2) and (3), we have $\mathrm{Ap}(S, a_1) \subseteq B$ and since

$$|B| = 1 + (\frac{a_1}{3} + 1) + 2 + (\frac{a_1}{3} - 2) + (\frac{a_1}{3} - 2) = a_1 = |\mathrm{Ap}(S, a_1)|,$$

the equality holds. Since $12 | f$, we have $r \geq 1$ and $m \geq 4$. So

$$(\frac{a_1}{3} - 2)a_2 + 2a_3 - (\frac{a_1}{3} + 1)a_2 = 2a_3 - 3a_2 = 3^r\frac{m}{2} + m + 6 - 3\frac{m}{2} - 9 > 0.$$

This implies that $\max(\mathrm{Ap}(S,a_1)) = (\frac{a_1}{3}-2)a_2+2a_3$. Hence

$$\begin{aligned} f^*(S) &= \max(\mathrm{Ap}(S,a_1)) - a_1 \\ &= (\frac{a_1}{3}-2)a_2+2a_3-a_1 \\ &= (\frac{a_1}{3}-2)a_2+2a_3+a_1-2a_1 \\ &= (\frac{a_1}{3}-2)a_2+(\frac{a_1}{3}+2)a_2-2a_1 \\ &= 3^r m. \end{aligned}$$

□

By Lemma 1.1 and Proposition 1.2 in [8], we have the following proposition.

Proposition 2.2. *Let f be a positive integer.*
(1) If $3\nmid f$, then $f^*(\langle 3,a,b\rangle)=f$, where $\{a,b\}=\{x\in\{f+1,f+2,f+3\}\,|3\not| x\}$;
(2) If f is even and $4\nmid f$, then $f^*(\langle 4,\frac{f}{2}+2,\frac{f}{2}+4\rangle)=f$;
(3) If $(4,f)=1$, $3|f$ and $f>12$, then $f^*(\langle 4,\frac{f}{3}+4,f+4\rangle)=f$.

The following remark tells us that, when $e(S)=3$, $f^*(S)\neq 1,3$.

Remark 2.3. *Let S be a numerical semigroup generated by $A=\{a_1,a_2,a_3\}$ and let $e(S)=3$.*
(1) If $f^*(S)=1$, then $2\in A$ and thus $e(S)=2$, a contradiction;
(2) Let $f^*(S)=3$. Since $e(S)=3$, so $1,2\notin A$. Thus $A=\{4,5,6\}$ and $f^*(S)=7$, a contradiction.

Our main result is the following theorem.

Theorem 2.4. *Let $f\neq 1,3$ be a positive integer. Then there exists a numerical semigroup S with $e(S)=3$ such that $f^*(S)=f$.*

Proof. Every positive integer can be written as $12n+i$ for $i\in\{0,1,2,\dots,11\}$ by the division algorithm. To prove the theorem, we consider five cases.
case 1: If $3\nmid f$, the claim follows by Proposition 2.2.
case 2: If $f=12n, n>0$, the claim follows by Proposition 2.1.
case 3: If $f=12n+3, n>0$, we set $S=\langle 4,4n+5,12n+7\rangle$. From Proposition 2.2, $f^*(S)=12n+3$. We show that $e(S)=3$. Since $12n+7$ has a remainder of 3 modulo 4, $4n+5$ has a remainder of 1 modulo 4 and $2(4n+5)$ has a remainder of 2 modulo 4, we conclude that $12n+7\notin\langle 4,4n+5\rangle$. So $e(S)=3$.
case 4: If $f=12n+6, n\geq 0$, we set $S=\langle 4,6n+5,6n+7\rangle$. Clearly $6n+7\notin\langle 4,6n+5\rangle$. So $e(S)=3$. Moreover from Proposition 2.2, $f^*(S)=12n+6$.
case 5: $f=12n+9, n\geq 0$. There are two cases to consider.
(1) $f=9$. It is easy to see that the Frobenius number of $S=\langle 5,6,8\rangle$ is $f=9$.
(2) If $f=12n+9, n\geq 1$, we set $S=\langle 4,4n+7,12n+13\rangle$. From Proposition 2.2, $f^*(S)=12n+9$. We show that $e(S)=3$. Since $12n+13$ has a remainder of 1 modulo 4, $4n+7$ has a remainder of 3

modulo 4 and $2(4n+7)$ has a remainder of 2 modulo 4, we conclude that $12n+13 \notin \langle 4, 4n+7\rangle$. So $e(S) = 3$. □

Remark 2.5. *From Theorem 2.4, the minimal generators of the numerical semigroup S, associated to the given Frobenius number f, are constructed explicitly.*

3. Higher dimensional case

Let $A = \{\mathbf{v}_1, \dots, \mathbf{v}_r, \mathbf{v}_{r+1}, \dots, \mathbf{v}_n\}$ be a subset of $\mathbb{N}^r$ for some positive integer $r \geq 2$ and let

$$S = \mathbb{N}A = \left\{ \sum_{i=1}^{n} n_i \mathbf{v}_i \,|n_i \in \mathbb{N} \right\}$$

be the affine semigroup generated by A. The group spanned by S, denoted by G, is defined as $G = \{\mathbf{u} - \mathbf{v} \mid \mathbf{u}, \mathbf{v} \in S\}$. We can define the following relation on G: for any $\mathbf{u}, \mathbf{v} \in G$, $\mathbf{v} \preceq \mathbf{u} \Leftrightarrow \mathbf{u} - \mathbf{v} \in S$. The cone spanned by S and interior of the cone spanned by S, are denoted by:

$$C = \left\{ \sum_{i=1}^{n} q_i \mathbf{v}_i \,|q_i \in \mathbb{Q}_{\geq 0} \right\} \text{ and } C^\circ = \left\{ \sum_{i=1}^{n} q_i \mathbf{v}_i \,|q_i \in \mathbb{Q}_{> 0} \right\}$$

respectively. The vector $f^* \in G \backslash S$ is called a *Frobenius vector* for S, if for all $\mathbf{x} \in C^\circ \cap G$, we have $f^* + \mathbf{x} \in S$ (see Fig 1). Moreover, the Frobenius vector f^* is called minimal, if there is no Frobenius vector f such that $f^* \in f + C$.

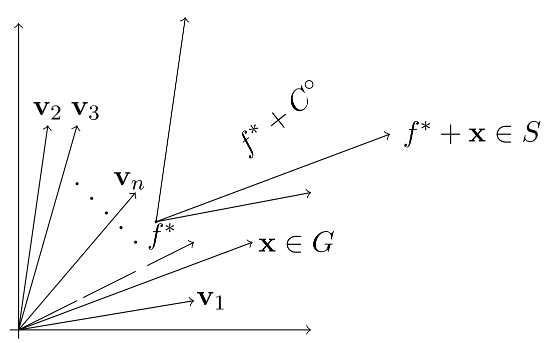

Fig.1

Definition 3.1. *The semigroup S is called* simplicial *if there exist $\mathbf{v}_{i_1}, \mathbf{v}_{i_2}, \dots, \mathbf{v}_{i_r} \in A$ such that $\mathbf{v}_{i_1}, \mathbf{v}_{i_2}, \dots, \mathbf{v}_{i_r}$ are linearly independent over $\mathbb{Q}$ and $C = \mathbb{Q}_{\geq 0}\mathbf{v}_{i_1} + \cdots + \mathbb{Q}_{\geq 0}\mathbf{v}_{i_r}$.*

If r is less than three, every affine semigroup is simplicial. Assume without loss of generality that $\{i_1, \dots, i_r\} = \{1, \dots, r\}$. For simplicial affine semigroups, the set $T = \cap_{i=1}^{r}(\mathrm{Ap}(\mathrm{S}, \mathbf{v}_{\mathrm{i}}))$ is always finite (see [10, Section 1]). By a free semigroup we mean the following (for more details, please see [11]).

Definition 3.2. *The semigroup S is called free, if the cardinality of T is $c_{r+1}c_{r+2}\cdots c_n$, where*

$$c_i = \min\{k \in \mathbb{N}_{>0} \mid k\mathbf{v}_i \in \langle \mathbf{v}_1, \dots, \mathbf{v}_{i-1}\rangle\}, i = r+1, \dots, n.$$

In [2], the author proves the following proposition.

Proposition 3.3. *With the above notation, assume that S is free and $\eta = \max_{\preceq} T$. Then S has a unique minimal Frobenius vector of the form $f^*(S) = \eta - \sum_{i=1}^{r} \mathbf{v}_i$.*

Let $E_r = \{\mathbf{e}_1, \dots, \mathbf{e}_r\}$ be the standard basis of $\mathbb{N}^r$ and $3E_r = \{3\mathbf{e}_1, \dots, 3\mathbf{e}_r\}$. The following is our main result.

Theorem 3.4. *Let f be a nonzero vector in $\mathbb{N}^r, r \geq 2$, and $f \notin E_r \cup 3E_r$. Then there exists an affine semigroup $S \subset \mathbb{N}^r$ generated by at most $r+1$ elements, such that f is the unique minimal Frobenius vector of S.*

Proof. Let $f = (\alpha_1, \alpha_2, \dots, \alpha_r)$ and f has at least two nonzero components. For every $i = 1, \dots, r$, if $\alpha_i \neq 0$, we set $\mathbf{v}_i = (0, \dots, 0, 3\alpha_i, 0, \dots, 0)$. Let $\alpha_{i_1}, \alpha_{i_2}, \dots$ and α_{i_t} be nonzero components of f. By assumption $t > 1$. We set $S = \langle \mathbf{v}_{i_1}, \dots, \mathbf{v}_{i_t}, 2f \rangle$. Since $2f = \frac{2}{3}\mathbf{v}_{i_1} + \cdots + \frac{2}{3}\mathbf{v}_{i_t}$, without loss of generality we can assume that S is a simplicial affine semigroup in $\mathbb{N}^t$. It is not hard to see that $\min\{k \in \mathbb{N} \mid k(2f) \in \mathbb{N}\mathbf{v}_{i_1} + \cdots + \mathbb{N}\mathbf{v}_{i_t}\}$ is equal to 3 and $T = \{0, 2f, 4f\}$. So S is free and $\eta = 4f$. By using Proposition 3.3, we conclude that $f^*(S) = \eta - (\mathbf{v}_{i_1} + \cdots + \mathbf{v}_{i_t}) = f$.

Now let f has only one nonzero component. Let $\alpha_k \neq 0, k \in \{1, \dots, r\}$. By using Theorem 2.4, there exists a numerical semigroup $S_k = \langle a_1, a_2, a_3 \rangle$ with $e(S_k) = 3$, such that $f^*(S_k) = \alpha_k$. Let S be the affine semigroup generated by $\{\mathbf{v}_1 = a_1\mathbf{e}_k, \mathbf{v}_2 = a_2\mathbf{e}_k, \mathbf{v}_3 = a_3\mathbf{e}_k\}$. It is not hard to see that f is the minimal Frobenius vector of S. □

Corollary 3.5. *Let f be a nonzero vector in $\mathbb{N}^2$, and $f \notin E_2 \cup 3E_2$. Then there exists an affine semigroup $S \subset \mathbb{N}^2$ minimally generated by three elements, such that f is the unique minimal Frobenius vector of S.*

Proof. There are two cases. (i) f has two nonzero components, and (ii) f has one nonzero components. In both cases there exists an affine semigroup minimally generated by three elements, such that $f^*(S) = f$. □

Example 3.6. *Let $f = (12, 23)$. We set $\mathbf{v}_1 = (36, 0), \mathbf{v}_2 = (0, 69)$, $\mathbf{v}_3 = (24, 46)$ and $S = \mathbb{N}\mathbf{v}_1 + +\mathbb{N}\mathbf{v}_2 + \mathbb{N}\mathbf{v}_3$. So $f^*(S) = 2\mathbf{v}_3 - \mathbf{v}_1 - \mathbf{v}_2 = (12, 23)$ (see* Fig 2).

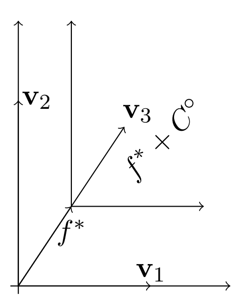

Fig.2

Acknowledgement

The authors would like to thank the anonymous reviewers for their helpful and constructive comments that greatly contributed to improving the final version of the paper.

References

[1] A. Assi, P. A. García-Sánchez and I. Ojeda, Frobenius vectors, Hilbert series and Gluings of Affine Semigroups, *J. Commut. Algebra*, **7** (2015) 317–335.

[2] A. Assi, The Frobenius vector of a free affine semigroup, *J. Algebra Appl.*, **11** (2012) 1–10.

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

[4] G. L. Feng and T. R. N. Rao, A simple approach for construction of algebraic-geometric codes from affine plane curves, *IEEE Trans. Inform. Theory*, **40** (1994) 1003–1012.

[5] R. Fröberg, The Frobenius number of some semigroups, *Comm. Algebra*, **22** (1994) 6021–6024.

[6] C. Kirfel and G. R. Pellikaan, The minimum distance of codes in an array coming from telescopic semigroups, (special issue), *IEEE Trans. Inform. Theory*, **41** (1995) 1720–1732.

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

[8] J. C. Rosales, P. A. García-Sánchez and J. I. Garcia-Garcia, Every positive integer is the Frobenius number of a numerical semigroup with three generators, *Math. Scand.*, **94** (2004) 5–12.

[9] J. C. Rosales and P. A. García-Sánchez, Numerical Semigroups, Developments in mathematics, **20**, Springer, New York, 2009.

[10] J. C. Rosales and P. A. García-Sánchez, On Cohen-Macaulay and gorenstein simplicial affine semigroups, *Proc. Edinburgh Math. Soc. (2)*, **41** (1998) 517–537.

[11] J. C. Rosales and P. A. García-Sánchez, On free affine semigroups, *Semigroup Forum*, **58** (1999) 367–385.

[12] J. J. Sylvester, *Mathematical questions with their solutions*, Educational Times, **41** (1884) 171–178.

[13] B. Vizvári, *Generation of uniformly distributed random vectors of good quality*, Rutgers University, Rutgers Center for Operations Research, 1994 1–11.

[14] B. Vizvári, *On a generalization of the Frobenius problem*, Technical Report MN/30 Computer and Automation Inst., Hungarian Academy of Sciences, 1987.

Ali Mahdavi

Department of Pure Mathematics, Faculty of Mathematics and Computer Science, Amirkabir University of Technology Tehran, Iran

Email: a_mahdavi@aut.ac.ir

Farhad Rahmati

Department of Pure Mathematics, Faculty of Mathematics and Computer Science, Amirkabir University of Technology Tehran, Iran

Email: frahmati@aut.ac.ir