An algorithm to compute the primitive elements of an embedding dimension three numerical semigroup

F. Aguiló-Gost [1,4]

Departament de Matemàtica Aplicada IV
Univ Politècnica de Catalunya
Barcelona, España

P. A. García-Sánchez, [2,5]

Departamento de Álgebra
Universidad de Granada
Granada, España

D. Llena [3,6]

Departamento de Matemáticas
Universidad de Almería
Almería, España

Abstract

We give an algorithm to compute the set of primitive elements for an embedding dimension three numerical semigroups. We show how we use this procedure in the study of the construction of L-shapes and the tame degree of the semigroup.

Keywords: Numerical semigroup, L-shapes, primitive elements, tame degree.

1 Introduction

Let S be a numerical semigroup, that is, a submonoid of $(\mathbb{N}, +)$ with finite complement in $\mathbb{N}$ (here $\mathbb{N}$ denotes the set of nonnegative integers). It is well known that S is finitely generated as monoid: exists $A \subset S$ finite such that $S = \langle A \rangle = \{\sum_{a \in A} \lambda_a a \mid \lambda_a \in \mathbb{N}\}$. Moreover, there is a unique minimal (with respect to set inclusion) A satisfying this condition, which is known as minimal generating system. Suppose that $A = \{a_1, \dots, a_n\}$. Then the monoid morphism

$$\varphi : \mathbb{N}^n \to S, \ (x_1, \dots, x_n) \mapsto \sum_{i=1}^{n} x_i a_i$$

is surjective, and so S is isomorphic as monoid to $\mathbb{N}^n / \ker \varphi$, where

$$\ker \varphi = \{(x, y) \in \mathbb{N}^n \times \mathbb{N}^n \mid \varphi(x) = \varphi(y)\}.$$

The congruence $\ker \varphi$ is a monoid too, and it is minimally generated by the set of minimal (with respect to the order given by the Cartesian product) nonzero elements of $\ker \varphi \setminus \{(0, 0)\}$, which we denote by $\mathcal{I}(\ker \varphi)$, (see [10, Chapter 8]). Let e_i be the ith row of the $n \times n$ identity matrix. Then (e_i, e_i) is always one of these minimal elements.

Define

$$\mathrm{Prim}(S) = \{\varphi(a) \mid (a, b) \in \mathcal{I}(\ker \varphi) \text{ for some } b \neq a\},$$

which we call *primitive elements of S*.

In [4] an algorithm to compute $\mathcal{I}(\ker \varphi)$ is given, and so $\mathrm{Prim}(S)$. In this work, we particularize this method to the very particular case when S is a numerical semigroup with embedding dimension three ($n = 3$). Prior to this, we present two examples where an improvement of this procedure is welcomed.

1.1 L-forms

Let S be a numerical semigroup minimally generated by $\{a_1, \dots, a_n\}$. Given $k, m \in \mathbb{N}$, $m \neq 0$, we denote by $[k]_m$ the congruence class of k modulo m. The *Apéry set* of m in S is $\mathrm{Ap}(S, m) = \{s \in S \mid s - m \notin S\}$. It is well known that if $m \in S \setminus \{0\}$, then $\mathrm{Ap}(S, m) = \{w_0, \dots, w_{m-1}\}$ with $w_i = \min([i]_m \cap S)$.

[4] Email: matfag@ma4.upc.edu
[5] Email: pedro@ugr.es
[6] Email: dllena@ual.es

Let $[\![i_1, \ldots, i_{n-1}]\!]$ be the unitary $(n-1)$-cube $[i_1, i_1+1] \times \cdots \times [i_{n-1}, i_{n-1}+1]$ in $\mathbb{R}^{n-1}$. We label each cube with his weight $i_1 a_1 + \ldots + i_n a_n$. And we say that an equivalence class $[m]_{a_n}$ is *represented* by the corresponding related cubes $[\![x_1, \ldots, x_{n-1}]\!]$ with $a_1 x_1 + \cdots + a_{n-1} x_{n-1} \equiv m \pmod{a_n}$.

Let us define the *discrete cone* of unitary cubes

$$\Delta(i_1, \ldots, i_{n-1}) = \{[\![j_1, \ldots, j_{n-1}]\!] : 0 \leq j_1 \leq i_1, \ldots, 0 \leq j_{n-1} \leq i_{n-1}\}$$

for $(i_1, \ldots, i_{n-1}) \in \mathbb{N}^{n-1}$, and the set of unitary cubes labeled with $[m]_{a_n}$

$$Q_m = \{[\![i_1, \ldots, i_{n-1}]\!] : [i_1 a_1 + \ldots + i_{n-1} a_{n-1}]_{a_n} = [m]_{a_n}, (i_1, \ldots, i_{n-1}) \in \mathbb{N}^{n-1}\}.$$

The minimum weight of unitary cubes representing $[m]_{a_n}$ will be denoted by

$$M_m = \min\{i_1 a_1 + \ldots + i_{n-1} a_{n-1} : [\![i_1, \ldots, i_{n-1}]\!] \in Q_m\}.$$

Definition 1.1 [Minimum Distance Diagram] A *Minimum Distance Diagram*, $\mathcal{H}$, related to the numerical semigroup $S = \langle a_1, \ldots, a_n \rangle$ is a set of a_n unitary cubes in $\mathbb{N}^{n-1}$ with the following three properties

(a) If $X = [\![x_1, \ldots, x_{n-1}]\!], Y = [\![y_1, \ldots, y_{n-1}]\!] \in \mathcal{H}$ represent the same equivalence class, then $X = Y$.

(b) If $[\![x_1, \ldots, x_{n-1}]\!] \in \mathcal{H}$, then $x_1 a_1 + \ldots + x_{n-1} a_{n-1} = M_{x_1 a_1 + \ldots + x_{n-1} a_{n-1}}$.

(c) If $[\![x_1, \ldots, x_{n-1}]\!] \in \mathcal{H}$, then $\Delta(x_1, \ldots, x_{n-1}) \subseteq \mathcal{H}$.

Minimum distance diagrams were used first in the computation of distances in weighted and non-weighted Cayley digraphs ([8,9]). These diagrams tesellate the $\mathbb{R}^{n-1}$ space (so they are also named *tiles*). When $n = 3$ they are well known as *L-shaped tiles* and many works appeared in the bibliography ([1,6]) on Cayley digraphs and numerical semigroups. Less is known of generic tiles when $n \geq 4$, with the exception of some particular cases ([7,9]).

An important property of minimum distance diagrams is that the Apéry set $\mathrm{Ap}(S, a_n) = \{\mathrm{w}(x_1, \ldots, x_{n-1}) : [\![x_1, \ldots, x_{n-1}]\!] \in \mathcal{H}\}$ where $\mathcal{H}$ is any minimum distance diagram related to the semigroup S. When $n = 3$, several applications have been given using this fact, for instance efficient algorithms for the computation of the *Frobenius number* and the *genus* of numerical semigroups.

Fig. 1. Minimum distance diagram related to $\langle 4, 9, 11 \rangle$

Example 1.2 Consider $S = \langle 4, 9, 11 \rangle$, then Figure 1 shows a minimum distance diagram related to S. The labels of the cubes are their weights.

Now let $S = \langle 5, 7, 11, 13 \rangle$. Then Figure 2 shows a minimum distance diagram $\mathcal{H}$ related to S, labeled with weights also. The labels of the cubes also form the Apéry set $\mathrm{Ap}(S, 13)$.
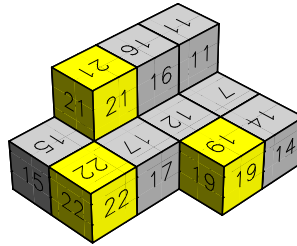

Fig. 2. Minimum distance diagram related to $\langle 5, 7, 11, 13 \rangle$

Given $s \in S$, define $\mathsf{Z}(s) = \varphi^{-1}(s)$ as the *set of factorizations* of s in S (actually in terms of $\{a_1, \ldots, a_n\}$). We study the number of different L-forms of S in terms of the factorizations of some elements in the Apéry set of a_n. For $n = 3$ there are at most two L-forms, but this is not the case for $n > 3$. For instance, for $\langle 5, 7, 11, 13 \rangle$, we have

```
gap> LFormsOfNumericalSemigroup(NumericalSemigroup([5,7,11,13]));
[[[0,0,0],[1,0,0],[0,1,0],[2,0,0],[0,0,1],[1,1,0],[0,2,0],[3,0,0],[1,0,1],[2,1,0],[1,2,0],[0,3,0],[0,0,2]],
 [[0,0,0],[1,0,0],[0,1,0],[2,0,0],[0,0,1],[1,1,0],[0,2,0],[3,0,0],[1,0,1],[2,1,0],[1,2,0],[0,3,0],[3,1,0]],
 [[0,0,0],[1,0,0],[0,1,0],[2,0,0],[0,0,1],[1,1,0],[0,2,0],[3,0,0],[1,0,1],[2,1,0],[1,2,0],[2,0,1],[0,0,2]],
 [[0,0,0],[1,0,0],[0,1,0],[2,0,0],[0,0,1],[1,1,0],[0,2,0],[3,0,0],[1,0,1],[2,1,0],[1,2,0],[2,0,1],[3,1,0]]]
```

The implementation has been performed using the `numericalsgps` ([5]) GAP package.

In the above representation, each L-form is given by a list containing a factorization for each of the elements in $\mathrm{Ap}(S, 13)$ with respect to the semigroup $\langle 5, 7, 11 \rangle$. Thus, in order to compute all possible L-forms, we first compute $\mathrm{Ap}(S, 13)$, which has 13 elements, and then we compute for each of these elements its set of factorizations in $\langle 5, 7, 11 \rangle$; finally we have to find a factorization for each element and arrange the chosen factorizations coherently with the definition of L-form. In this example we see that the eleven first elements are always the same, while those at the end change: $[0, 3, 0]$ can be replaced with $[2, 0, 1]$, whilst $[0, 0, 2]$ with $[3, 1, 0]$. This is due to the fact that $21 = 3 \cdot 7 = 2 \cdot 2 + 1 \cdot 11$ and $22 = 3 \cdot 5 + 1 \cdot 7 = 2 \cdot 11$. Notice that these two elements, 21 and 22, are primitive elements that belong to the Apéry set. The L-shape in Figure 2, corresponds to the last element in the list.

The first problem we encounter is when we try to obtain the Apéry set when

a_4 is "big". We have some evidences that the L-shapes are determined by the set $\mathrm{Prim}(\langle a_1, a_2, a_3 \rangle) \cap \mathrm{Ap}(S, a_4)$ (and for this we do not need to determine the Apéry set, since we only have to filter those primitive elements s with the condition $s - a_4 \notin S$). With this approach our execution times passed from hours to a bunch of seconds.

1.2 The tame degree

Let $x = (x_1, \ldots, x_n) \in \mathsf{Z}(s)$ be a factorization of $s \in S = \langle a_1, \ldots, a_n \rangle$. We define its length as $|x| = \sum_{i=1}^n x_i$. If $y = (y_1, \ldots, y_n)$ is another factorization, we denote by $x \wedge y = (\min\{x_1, y_1\}, \ldots, \min\{x_n, y_n\})$. The distance between x and y is defined as

$$\mathrm{d}(x, y) = \max\{|x - (x \wedge y)|, |y - (x \wedge y)|\},$$

that is, the maximum of the lengths of the factorizations once we remove the common part of x and y.

An N-chain, with $N \in \mathbb{N}$, of factorizations joining x with y is a sequence $x_1, \ldots, x_k \in \mathsf{Z}(s)$ such that: $x_1 = x$, $x_k = y$, and for all i, $\mathrm{d}(x_i, x_{i+1}) \leq N$.

The *catenary degree* of s, $\mathsf{c}(s)$, is the minimum of the $N \in \mathbb{N}$, such that for any two factorizations of S there exists an N-chain joining them. The catenary degree of S is the supremum of the catenary degrees of all the elements of S, and we denote it by $\mathsf{c}(S)$. This supremum is indeed a maximum, that is, it is reached in a particular element of S.

The *tame degree* of s is the minimum $N \in \mathbb{N}$ such that whenever $s - a_i \in S$ for some $i \in \{1, \ldots, n\}$, for any $x \in \mathsf{Z}(s)$, there exists $y = (y_1, \ldots, y_n) \in \mathsf{Z}(s)$ such that $\mathrm{d}(x, y) \leq N$. The tame degree of s is denoted by $\mathsf{t}(s)$, and the tame degree of S, as occurs with the catenary degree, it is defined as the supremum (once more a maximum in our setting) of the tame degrees of the elements of S, and we denote it by $\mathsf{t}(S)$.

In [1], formulas for $\mathsf{c}(S)$, for the case $n = 3$ (embedding dimension three) are presented in terms of the parameters of any of the L-shapes associated to S. For arbitrary embedding dimension we know ([3]) that the catenary degree of S is attained in the elements that are used to construct a minimal presentation of S (which is a minimal generating set of $\ker \varphi$ as a congruence). In contrast to this, the tame degree is attained in the primitive elements of S, which as we have seen above are those that appear related to the minimal generating set of $\ker \varphi$ as a monoid.

A minimal presentation of S is *generic* if in all its elements every minimal generator of S appears. In this case, $\mathsf{c}(S) = \mathsf{t}(S)$ (see [2]). For $n = 3$, S has a generic presentation if and only if it is not symmetric (where symmetric

means that $x \in \mathbb{Z} \setminus S$ implies $\mathrm{F}(S) - x \in S$, with $\mathrm{F}(S)$ the Frobenius number of S; see for instance [11, Chapter 9]). In general, $\mathsf{c}(S) \leq \mathsf{t}(S)$, and thanks to the study of the primitive elements in embedding dimension three, we have been able, with C. Viola, to characterize those embedding dimension three numerical semigroups for which the inequality is strict ([12]).

2 Computing primitive elements for embedding dimension three numerical semigroups

As we have seen above, primitive elements are of great help for the computation of L-shapes and the tame degree. In this section we sketch how we have particularized the general procedure explained in [4] to the particular case of embedding dimension three. So assume in what follows that S is minimally generated by $\{n_1, n_2, n_3\}$. Associated to the kernel congruence of φ (defined in the introduction), we define the subgroup of $\mathbb{Z}^3$

$$M = \{(x_1 - y_1, x_2 - y_2, x_3 - y_3) \colon ((x_1, x_2, x_3), (y_1, y_2, y_3)) \in \ker \varphi\}$$

(see [10] for more details on this subgroup).

The method proposed in [4], starting from a basis of M, constructs all possible combinations by changing the sign of its elements, and then "saturates" these sets Let us precise the concept of saturation a bit more.

Definition 2.1 Let $(x_1, \ldots x_n)$ and $(y_1, \ldots y_n)$ be in $\mathbb{Z}^n$. We write $(x_1, \ldots x_n) \sqsubseteq (y_1, \ldots y_n)$ if $x_i y_i \geq 0$ and $|x_i| \leq |y_i|$ for all $i \in \{1, \ldots, n\}$.

A set A of $\mathbb{Z}^n$ is *saturated* if for any $a_i, a_j \in A$ there exists $a_h \in A$ such that $a_h \sqsubseteq a_i + a_j$.

We study the saturation process of $B_s = \{(0, n_3/g, -n_2/g), (g, -y_2, y_3)\}$, which is a base of M, where $g = \gcd(n_2, n_3)$.

Definition 2.2 Let $x = (x_1, x_2, x_3) \in \mathbb{Z}^3$. The signature of x, $\mathrm{sg}(x)$, is the tern formed by the signs of x_1, x_2 and x_3. Zero is assumed to have both positive and negative sign.

Remark 2.3 If the signatures of a and b coincide, then the sum is comparable with both elements, that is, $\mathrm{sg}(a) = \mathrm{sg}(b)$ implies $a \sqsubseteq a + b$ and $b \sqsubseteq a + b$. Hence, in order to "saturate" we must consider taking elements with different signature.

Remark 2.4 In order to check if an element is incomparable with the rest, we simply have to compare it with those having its same signature.

Thus, two elements are incomparable with respect to $\sqsubseteq$ if either they have different signatures, or they have the same signature and some of their coordinates increase while other decrease (in absolute value).

We start with B_s, whose elements are

$$x_0 = (0, n_3/g, -n_2/g) = (0, +, -), \qquad x_1 = (g, -y_2, y_3) = (g, -, +).$$

Since they have different signature, by Remark 2.3 their addition is a possible new candidate for the saturation. We obtain

$$a_1 = x_0 + x_1 = (g, n_3/g - y_2, y_3 - n_2/g) = (g, +, -).$$

This new element has the same signature as x_0 but the first coordinate is larger, while the other two are smaller in absolute value. Hence by Remark 2.4, we obtain a new incomparable element that we add to the saturation of B_s.

We denote by A_i the ith step in the saturation of A. We write $A = B_s$, and thus $A_1 = \{x_0, x_1, a_1\}$.

Lemma 2.5 *In the saturation process, while there is no element with signature* $(+, -, -)$ *, only a new element will be added. If* $a_i = a_{i-1} + a_j$, *then* $a_{i+1} = a_i + a_j$ *if* $sg(a_i) = sg(a_{i-1})$; *or* $a_{i+1} = a_i + a_{i-1}$ *if* $sg(a_i) = sg(a_{i-1})$.

When the first element with signature $(+, -, -)$ appears, two new elements are added in the next saturation step.

Lemma 2.6 *If* a_i *is the first element with signature* $(+, -, -)$, *then* $b_1 = a_i + a_j$ *y* $c_1 = a_i + a_{i-1}$ *are incomparable with the preceding a's.*

Then, after the ith step, we will start adding elements b_2 and c_2 raising from b_1 and c_1, respectively, where $b_2 = b_1 + a_j$, or $b_2 = b_1 + a_i$; while $c_2 = c_1 + a_{i-1}$, or $c_2 = c_1 + a_i$.

The following lemma asserts that $b_x + c_y$ is comparable, and thus we do not add it in any saturation.

Lemma 2.7 *Let* b_x *be an incomparable element obtained from* b_1 *(that is, adding to b_1 either a_j or some previous b_i), and let c_y be another incomparable element obtained from c_1 (that is, adding a_{i-1} or some previous c_j). Then* $a_i \sqsubseteq b_x + c_y$.

Theorem 2.8 *The primitive elements of* $S = \langle n_1, n_2, n_3 \rangle$ *can be computed as follows. Start with* $B_s = \{(0, n_3/g, -n_2/g), (g, -y_2, y_3)\}$ *and applying twice the division algorithm first with n_3/g and y_2, and then with n_2/g and y_3, we obtain two list of elements in which the second coordinate will decreasing until*

we reach $(n_3/g_2, 0, -n_1/g_2)$ where $g_2 = gcd(n_1, n_3)$, and in the second list the third coordinate will be decreasing until we obtain $(n_2/g_3, -n_1/g_3, 0)$ where $g_3 = gcd(n_1, n_2)$. Both list will have the same elements until a_i is attained, and then we will get the series of b's and c's.

According to the procedure presented in [4], we must saturate B_s and $B_{-s} = \{(0, n_3/g, -n_2/g), (-g, y_2, -y_3)\}$, but this last set is already saturated.

Example 2.9 Take $S = \langle 17, 31, 41 \rangle$.

$$x_0 = (0, 41, -31), x_1 = (1, -27, 20),$$

$$a_1 = (1, 14, -11), a_2 = (2, -13, 9), a_3 = (3, 1, -2) = 82, a_4 = (5, -12, 7)$$

$$a_5 = (8, -11, 5), a_6 = (11, -10, 3), a_7 = (14, -9, 1), a_8 = (17, -8, -1),$$

$$c_1 = (31, -17, 0),$$

$$b_1 = (20, -7, -3), b_2 = (23, -6, -5), b_3 = (26, -5, -7), b_4 = (29, -4, -9)$$

$$b_5 = (32, -3, -11), b_6 = (35, -2, -13), b_7 = (38, -1, -15), b_8 = (41, 0, -17).$$

One of the advantages of this procedure is that from the output one can easily compute a minimal presentation for S.

References

[1] Aguiló-Gost, F., and P.A. García-Sánchez, *Factoring in embedding dimension three numerical semigroups*, Electronic. Journ. of Comb., 17, R138: 21 pp. 2010.

[2] Blanco, V., P.A. García-Sánchez, and A. Geroldinger, *Semigroup-theoretical characterizations of arithmetical invariants with applications to numerical monoids and Krull monoids*, Illinois J. Math. 55:1385–1414, 2011.

[3] Chapman, S. T., P.A. García-Sánchez, D. Llena, V. Ponomarenko, and J. C. Rosales, *The catenary and tame degree in finitely generated commutative cancellative monoids*, Manuscripta Math. 120:253–264, 2006.

[4] Chapman, S.T., P.A. García-Sánchez, D. Llena, J.C. Rosales. *Presentations of finitely cancellative commutative monoids and nonnegative solutions of systems of linear equations*, Discrete Applied Mathematics, 154:1947–1959, 2006.

[5] Delgado, M., P. A. García-Sánchez and J. Morais, "NumericalSgps", *A GAP package for numerical semigroups*. Available via http://www.gap-system.org/.

[6] Fiol, M.A., J.L.A. Yebra, I. Alegre and M.Valero. *A discrete optimization problem in local networks and data alignment*, IEEE Trans. of Comp., C-36:702–713, 1987.

[7] Killingbergtrø, H.G., *Betjening av figur i Frobenius' problem*, Normat 2: 75–82, 2000.

[8] Rødseth, Ø.J., *Weighted multi-connected loop networks*, Discrete Mathematics 148:161–173, 1996.

[9] Sabariego, P. and F. Santos. *Triple-loop networks with arbitrarily many minimum distance diagrams*, Discrete Mathematics 309(6):1672–1684, 2009.

[10] Rosales, J. C., and P. A. García-Sánchez. "Finitely Generated Commutative Monoids," Nova Science Publishers, New York, 1999.

[11] Rosales, J. C., and P. A. García-Sánchez. "Numerical Semigroups," Developments in Mathematics 20. Springer, New York, 2009.

[12] C. Viola, "Catenary and tame degre for embedding dimension three numerical semigroups", Master Thesis, Università di Catania, in preparation.