arXiv:1907.01217v1 [math.CO] 2 Jul 2019

Characterization of gaps and elements of a numerical semigroup using Groebner bases

Guadalupe Márquez–Campos and José M. Tornero

ABSTRACT. This article is partly a survey and partly a research paper. It tackles the use of Groebner bases for addressing problems of numerical semigroups, which is a topic that has been around for some years, but it does it in a systematic way which enables us to prove some results and a hopefully interesting characterization of the elements of a semigroup in terms of Groebner bases.

1. Numerical semigroups

This paper deals with a very special family of semigroups. Recall that a semigroup is a pair $(X, \star)$, where X is a set and $\star$ is an associative internal operation. Actually we will be considering monoids, that is, semigroups with unit element, but there are no substantial differences for our concerns. We will be particularly interested in the so–called numerical semigroups. Useful references for the basic concepts are [**11, 4**].

DEFINITION 1.1. A numerical semigroup is a semigroup $S \subset \mathbb{Z}_{\geq 0}$.

EXAMPLE 1.2. The first natural example of a numerical semigroup is the semigroup generated by a set $\{a_1, ..., a_k\} \subset \mathbb{Z}_{\geq 0}$, which is the set of linear combinations of these integers with non–negative integral coefficients:

$$\langle a_1, ..., a_k \rangle = \{\lambda_1 a_1 + ... + \lambda_k a_k \mid \lambda_i \in \mathbb{Z}_{\geq 0}\} .$$

It turns out that this example is in fact the general case for a numerical semigroup.

PROPOSITION 1.3. Let $0 \leq a_1 \leq ... \leq a_k$ be integers such that $\gcd(a_1, ..., a_k) = 1$. Let us write $S = \langle a_1, ..., a_k \rangle$. Then there exists $N \in \mathbb{Z}$ such that $x \in S$, for all $x \geq N$.

PROOF. Let us write, from Bezout's Identity

$$m_1 a_1 + ... + m_k a_k = 1,$$

for some $m_i \in \mathbb{Z}$ and let

$$P = \sum_{m_i \geq 0} m_i a_i > 0, \quad Q = \sum_{m_j \leq 0} m_j a_j \leq 0.$$

We take an integer $t \geq (a_1 - 1)(-Q)$ and write it as $t = -Q(a_1 - 1) + k$, for a certain $k \geq 0$. We divide k by a_1,

$$k = qa_1 + r, \text{ con } 0 \leq r < a_1$$

and then

$$
\begin{aligned}
t &= -Q(a_1 - 1) + qa_1 + r \\
&= -Q(a_1 - 1) + qa_1 + rP - rQ \\
&= q \cdot a_1 + rP + (-Q)(a_1 - 1 - r)
\end{aligned}
$$

This finishes the proof, as $a_1, P, -Q \in S$ and all their coefficients lie in $\mathbb{Z}_{\geq 0}$, therefore $t \in S$. □

REMARK 1.4. If we had $\gcd(a_1, ..., a_k) = d > 1$ the situation would be pretty analogous, taking into account that we should work in the ring $\mathbb{Z}d$ instead of $\mathbb{Z}$. This is why, in the sequel, when we talk about numerical semigroups we will assume that $\{a_1, ..., a_k\}$ generate $\mathbb{Z}$ as an additive group.

COROLLARY 1.5. *Every numerical semigroup $S \neq \{0\}$ can be written in the form $S = \langle a_1, ..., a_k \rangle$.*

PROOF. Clearly if we take $a_1, ..., a_k \in S$ then it must hold $\langle a_1, ..., a_k \rangle \subset S$, so there is an $N \in \mathbb{Z}_{\geq 0}$ as in the proposition for $\langle a_1, ..., a_k \rangle$. Then it is clear that S is generated by

$$\{a_1, ..., a_k\} \cup \{x \in S \mid x < N\}.$$

□

As $S = \langle a_1, ..., a_k \rangle$ is nothing but the set of non–negative integers that can be written as a linear combination (with non–negative coefficients) of $\{a_1, ..., a_k\}$, the elements of S are often called *representable integers* (w.r.t. $\{a_1, ..., a_k\}$). In the same fashion the elements of the (finite) set $\mathbb{Z}_{\geq 0} \setminus S$ are called *non–representable integers*.

DEFINITION 1.6. Some important invariants associated to a numerical semigroup S are:
- The set of gaps, which is the finite set $\mathbb{Z}_{\geq 0} \setminus S$, noted $G(S)$.
- The genus of S, noted $g(S)$, which is the cardinal of $G(S)$.
- The Frobenius number of S which is the maximum of $G(S)$, noted $f(S)$.
- The set of sporadic elements, noted $N(S)$, which are elements of S smaller than $f(S)$, that is $N(S) = S \cap [0, f(S)]$.
- The cardinal of $N(S)$, noted $n(S)$ (this invariant has not a properly established name in the literature).
- The multiplicity of S, noted $m(S)$, which is the smallest non–zero element in S (obviously a generator in any case).
- The dimension of S, noted $d(S)$, which is the smallest possible cardinal of a set of generators.
- The conductor, noted $c(S)$, which is $f(S) + 1 \in S$.

REMARK 1.7. The Frobenius number and its actual computation is a major problem in numerical semigroups. For semigroups of dimension 2, $S = \langle a_1, a_2 \rangle$ it was solved by Sylvester [13], who proved

$$f(S) = a_1 a_2 - a_1 - a_2, \quad g(S) = \frac{c(S)}{2}.$$

This problem, also known as *the money–changing problem* or *the nugget problem* has not an easy solution for $d(S) \geq 3$. Some closed formulas are known for certain cases, but Ramírez–Alfonsín proved that the general problem is NP–hard under Turing reductions [10].

2. A characterization of elements and gaps in terms of Groebner bases

REMARK 2.1. The relationship between numerical semigroups and computational algebra tools can be traced back to the pioneering work of Herzog [5] and there is a great number of papers which build bridges between both subjects. This section is intended as a survey of a small subset of this rich relationship, containing the results we will be using afterwards in an organized and structured way.

Most results and related to Groebner bases can be found, for instance, in [1], along with some results from this section, whose proofs we have included for the convenience of the reader.

Let b be a fixed natural number, $\{a_1, a_2, a_3, ..., a_k\}$ a set of coprime non–negative integers, and $\{\sigma_1, \sigma_2, \sigma_3, ..., \sigma_k\}$ a set of variables taking values in $\mathbb{Z}_{\geq 0}$. We consider the equation:

$$\sigma_1 a_1 + \sigma_2 a_2 + \sigma_3 a_3 + ... + \sigma_k a_k = b.$$

We introduce a new variable x and rewrite the previous equation as:

$$(x^{a_1})^{\sigma_1} (x^{a_2})^{\sigma_2} (x^{a_3})^{\sigma_3} ... (x^{a_k})^{\sigma_k} = x^b.$$

Next we introduce new variables y_j, for $j = 1, ..., k$, and we set $x^{a_i} = y_i$, obtaining:

$$y_1^{\sigma_1} y_2^{\sigma_2} y_3^{\sigma_3} ... y_k^{\sigma_k} = x^b$$

where $\sigma_1, \sigma_2, \sigma_3, ..., \sigma_k$ are still unknown.

Consider the polynomial ideal

$$I = \langle y_1 - x^{a_1}, y_2 - x^{a_2}, y_3 - x^{a_3}, ..., y_k - x^{a_k} \rangle \subset \mathbb{Q}[x, y_1, ..., y_k],$$

and let $\mathcal{B} = \{g_1, g_2, g_3, ..., g_r\}$ a minimal Groebner basis of I (not necessarily a reduced one), with respect to the usual lexicographic ordering $x > y_1 > y_2 > ... > y_k$.

Let us note $q_i = exp(g_i)$, the exponents of the polynomials g_i; and

$$K_{q_i} = q_i + \mathbb{Z}_{\geq 0}^{k+1} \subset \mathbb{Z}_{\geq 0}^{k+1}.$$

The main target is now to prove that there are one–to–one correspondences between

$$G(S) \quad \longleftrightarrow \quad \left[\bigcap_i \overline{K_{q_i}} \right] \setminus \{x = 0\} \subset \mathbb{Z}_{\geq 0}^{k+1}$$

$$S \quad \longleftrightarrow \quad \left[\bigcap_i \overline{K_{q_i}} \right] \cap \{x = 0\} \subset \mathbb{Z}_{\geq 0}^{k+1}$$

in a very explicit way.

In order to do that we will use two closely related maps:

$$\phi : \mathbb{Q}[y_1, y_2, ..., y_k] \longrightarrow \mathbb{Q}[x]$$
$$y_j \longmapsto x^{a_j}$$

and its extension

$$\widetilde{\phi} : \mathbb{Q}[x, y_1, y_2, ..., y_k] \longrightarrow \mathbb{Q}[x]$$
$$y_j \longmapsto x^{a_j}$$
$$x \longmapsto x$$

LEMMA 2.2. $\ker\left(\widetilde{\phi}\right) = I$.

PROOF. $I \subset \ker\left(\widetilde{\phi}\right)$ is clear. If we take $f(x, y_1, ..., y_k) \in \ker\left(\widetilde{\phi}\right)$ we can perform Euclidean division w.r.t. $y_k, ..., y_1$ to get an expression

$$f = q_k(x, y_1, ..., y_k)(y_k - x^{a_k}) + ... + q_1(x, y_1)(y_1 - x^{a_1}) + r(x)$$

and $r(x)$ must lie in $\ker\left(\widetilde{\phi}\right)$, therefore $r(x) = 0$.   □

LEMMA 2.3. $\mathcal{B}$ is a binomial basis. Therefore the normal form of a monomial x^N, which we will write $N_{\mathcal{B}}\left(x^N\right)$, is always a monomial.

PROOF. It is well–known that the Groebner basis of a binomial ideal is again binomial [**3**]. Now assume we have a monomial M_1 and we want to reduce it w.r.t. a binomial $M_2 - M_3$, M_2 being the leading term.

If we cannot perform reduction, there is nothing to do. Otherwise $M_2 | M_1$ and then the remainder of the division is

$$M_1 - \frac{M_1}{M_2}(M_2 - M_3) = \frac{M_1 M_3}{M_2},$$

that is, a monomial.   □

LEMMA 2.4. Let I be an ideal in a polynomial ring $R = k[x_1, ..., x_n]$, $\mathcal{B}$ a Groebner basis of I, and $g, f \in R$. Then $f \equiv g \mod I$ if and only if $N_{\mathcal{B}}(f) = N_{\mathcal{B}}(g)$.

PROOF. It is a straightforward consequence of the fact that the mapping

$$f \longmapsto N_{\mathcal{B}}(f)$$

is k–linear.   □

THEOREM 2.5. Let $I = \langle y_1 - x^{a_1}, y_2 - x^{a_2}, y_3 - x^{a_3}, ..., y_k - x^{a_k}\rangle \subset \mathbb{Q}[x, y_1, ..., y_k]$ and let $\mathcal{B}$ be the reduced Groebner basis of I w.r.t. the lexicographic order $x < y_1 < ... < y_k$.

Then $f \in \mathbb{Q}[x]$ lies in $Im(\phi)$ if and only if there exists $h \in \mathbb{Q}[y_1, ..., y_k]$ such that $N_{\mathcal{B}}(f) = h$. Should this be the case

$$f = \phi(h) = h\left(x^{a_1}, ..., x^{a_k}\right).$$

PROOF. Assume $f = \phi(g) = g\left(x^{a_1}, ..., x^{a_k}\right)$. Then

$$f(x) - g(y_1, ..., y_k) \in \ker\left(\widetilde{\phi}\right) = I$$

and therefore

$$N_{\mathcal{B}}(f) = N_{\mathcal{B}}(g) = h(x, y_1, ..., y_k).$$

Now, as $\mathcal{B}$ does not depend on x, the elements of $\mathcal{B}$ used in the computation of $N_{\mathcal{B}}(g)$ must have their leading terms in $k[y_1, ..., y_k]$. But, as we are using the lex ordering, in fact they must lie completely in $k[y_1, ..., y_k]$. Therefore $h \in \mathbb{Q}[y_1, ..., y_k]$.

Assume now $N_{\mathcal{B}}(f) = h \in \mathbb{Q}[y_1, ..., y_k]$. Then $f - h \in I$ and therefore

$$f(x) - h(y_1, ..., y_k) = \sum_{i=1}^{k} g_i(x, y_1, ..., y_k)(y_i - x^{a_i}),$$

and doing $y_i = x^{a_i}$ we get $f = \phi(h) = h\left(x^{a_1}, ..., x^{a_k}\right)$. $\qquad\square$

COROLLARY 2.6. *If $x^N \in Im(\phi)$ then it is the image of a monomial $y_1^{\sigma_1}...y_k^{\sigma_k} \in \mathbb{Q}[y_1, ..., y_k]$.*

PROOF. From the theorem $x^N \in Im(\phi)$ if and only if $N_{\mathcal{B}}\left(x^N\right) = h$, with $x^N = \phi(h)$. As we saw previously, h must be a monomial. $\qquad\square$

REMARK 2.7. Although we have chosen the lex ordering, one may note that in fact all we need for our argument is the fact that the ordering is an elimination one for the variable x.

This idea will be most useful in the sequel, as it will allow us to change the ordering in order to meet our needs, and different orders will be used to tackle different problems.

THEOREM 2.8. *Let $S = \langle a_1, ..., a_k \rangle$, I and $\mathcal{B}$ as above, and let $N \in \mathbb{Z}_{\geq 0}$. Then*

$$N \in S \iff x^N \in Im(\phi).$$

Furthermore:
- *If $N \in S$, then $N_{\mathcal{B}}\left(x^N\right) = y_1^{\sigma_1}...y_k^{\sigma_k}$ and $N = \sigma_1 a_1 + ... + \sigma_k a_k$.*
- *If $N \notin S$, then $N_{\mathcal{B}}\left(x^N\right) = x^{\sigma_0} y_1^{\sigma_1}...y_k^{\sigma_k}$, with $\sigma_0 \neq 0$ and $N = \sigma_0 + \sigma_1 a_1 + ... + \sigma_k a_k$.*

PROOF. Let $N \in S$. Then there are $\sigma_1, ..., \sigma_k \in \mathbb{Z}_{\geq 0}$ with

$$N = \sigma_1 a_1 + ... + \sigma_k a_k,$$

and then

$$\begin{aligned} x^N &= x^{a_1\sigma_1 + a_2\sigma_2 + ... + a_k\sigma_k} &&= \left(x^{a_1}\right)^{\sigma_1}\left(x^{a_2}\right)^{\sigma_2}...\left(x^{a_k}\right)^{\sigma_k} \\ &= \phi(y_1^{\sigma_1})...\phi(y_k^{\sigma_k}) &&= \phi(y_1^{\sigma_1}...y_k^{\sigma_k}), \end{aligned}$$

that is, $x^N \in Im(\phi)$.

On the other hand, if $x^N \in Im(\phi)$, we know from the previous result

$$x^N = \phi(h) = \phi\left(y_1^{\sigma_1}...y_k^{\sigma_k}\right) = \left(x_1^{a_1}\right)^{\sigma_1} ... \left(x_k^{a_k}\right)^{\sigma_k},$$

and $N = \sigma_1 a_1 + ... + \sigma_k a_k$. We already know as well that, in this case, $h = N_{\mathcal{B}}\left(x^N\right)$.

Now, if $N \notin S$, we still know $N_{\mathcal{B}}\left(x^N\right)$ is a monomial, say

$$N_{\mathcal{B}}\left(x^N\right) = x^{\sigma_0} y_1^{\sigma_1}...y_k^{\sigma_k}.$$

As $N \notin S$, $N_{\mathcal{B}}\left(x^N\right) \notin \mathbb{Q}[y_1, ..., y_k]$, hence $\sigma_0 \neq 0$. As $N_{\mathcal{B}}(f) - f \in I$ for all polynomials f,

$$\exists h_i \in \mathbb{Q}[x, y_1, ..., y_k] \mid x^N - x_0^\sigma y_1^{\sigma_1}...y_k^{\sigma_k} = \sum_{i=1}^k h_i(y_i - x^{a_i}).$$

We do then $y_i = x^{a_i}$ and

$$x^N - x^{\sigma_0} x^{a_1 \sigma_1}...x^{a_k \sigma_k} = 0$$

hence $N = \sigma_0 + \sigma_1 a_1 + ... + \sigma_k a_k$.   □

We are now ready to prove the one–to–one correspondences mentioned above.

THEOREM 2.9. *Let* $S = \langle a_1, ..., a_k \rangle \subset \mathbb{Z}_{\geq 0}$ *be a numerical semigroup. Consider*

$$I = \langle y_1 - x^{a_1}, y_2 - x^{a_2}, y_3 - x^{a_3}, ..., y_k - x^{a_k} \rangle \subset \mathbb{Q}[x, y_1, ..., y_k]$$

and let $\mathcal{B} = \{g_1, ..., g_r\}$ *be the reduced Groebner basis of* I *w.r.t. an elimination ordering for* x, *with* $q_i = exp(g_i)$.

- *The mapping*

$$\mathcal{F} : G(S) \longrightarrow \left[\bigcap_i \overline{K_{q_i}}\right] \setminus \{x = 0\} \subset \mathbb{Z}_{\geq 0}^{k+1}$$
$$N \longmapsto exp\left(N_{\mathcal{B}}\left(x^N\right)\right)$$

  is one–to–one.
- *The mapping*

$$\mathcal{G} : S \longrightarrow \left[\bigcap_i \overline{K_{q_i}}\right] \bigcap \{x = 0\} \subset \mathbb{Z}_{\geq 0}^{k+1}$$
$$M \longmapsto exp\left(N_{\mathcal{B}}\left(x^M\right)\right)$$

  is one–to–one.

PROOF. Most of the results are more or less proved by now.

I. $\mathcal{F}$ is surjective.

Let $(\sigma_0, \sigma_1, ..., \sigma_k) \in Im(\mathcal{F})$. Then there is some $N \in G(S)$ with

$$exp\left(N_{\mathcal{B}}\left(x^N\right)\right) = (\sigma_0, \sigma_1, ..., \sigma_k).$$

Being a normal form, it must hold

$$(\sigma_0, \sigma_1, ..., \sigma_k) \in \bigcap_i \overline{K_{q_i}},$$

and we previously saw $\sigma_0 \neq 0$.

On the other hand, take

$$(\sigma_0, \sigma_1, ..., \sigma_k) \in \left[\bigcap_i \overline{K_{q_i}}\right] \bigcap \{x = 0\} = \left[\overline{\bigcup_i K_{q_i}}\right] \bigcap \{x = 0\},$$

so $(\sigma_0, \sigma_1, ..., \sigma_k)$ does not lie in any K_{q_i} and therefore

$$x^{\sigma_0} x^{a_1 \sigma_1}...x^{a_k \sigma_k} = N_{\mathcal{B}}\left(x^{\sigma_0} x^{a_1 \sigma_1}...x^{a_k \sigma_k}\right).$$

Consider now $N = \sigma_0 + \sigma_1 a_1 + ... + \sigma_k a_k$. Then

$$\widetilde{\phi}\left(x^N\right) = \widetilde{\phi}\left(x^{\sigma_0} y_1^{\sigma_1}...y_k^{\sigma_k}\right) \Longrightarrow x^N \equiv x^{\sigma_0} y_1^{\sigma_1}...y_k^{\sigma_k} \mod I.$$

From a previous proposition

$$N_{\mathcal{B}}\left(x^N\right) = N_{\mathcal{B}}\left(x^{\sigma_0} y_1^{\sigma_1}...y_k^{\sigma_k}\right),$$

and the fact that such N is not in S comes from the unicity of the normal form and the characterization of elements in S in the previous theorem.

II. $\mathcal{G}$ is surjective.

The proof goes parallel with the previous, with some necessary adjustments. Let us first consider $(\sigma_0, \sigma_1, ..., \sigma_k) \in Im(\mathcal{G})$. Then there is some $N \in S$ with

$$exp(N_{\mathcal{B}}(x^N)) = (\sigma_0, \sigma_1, ..., \sigma_k).$$

Being a normal form, it must hold

$$(\sigma_0, \sigma_1, ..., \sigma_k) \in \bigcap_i \overline{K_{q_i}},$$

and we have to see $\sigma_0 = 0$. But we get this from the previous theorem.

Let us see now

$$Im(\mathcal{G}) \supset \left[\bigcap_i \overline{K}_{q_i}\right] \bigcap \{x = 0\}, \ \forall i = 1, .., r.$$

That is, for every $(0, \sigma_1, ..., \sigma_k) \in \bigcap_i \overline{K_{q_i}}$, we will find $M \in S$ with

$$exp\left(N_{\mathcal{B}}\left(x^M\right)\right) = (0, \sigma_1, ..., \sigma_k).$$

But

$$(0, \sigma_1, ..., \sigma_k) \in \bigcap \overline{K_{q_i}} \implies y_1^{\sigma_1}...y_k^{\sigma_k} = N_{\mathcal{B}}\left(y_1^{\sigma_1}...y_k^{\sigma_k}\right).$$

We define $M = \sigma_1 a_1 + \sigma_2 a_2 + \sigma_3 a_3 + ... + \sigma_k a_k$ and from $\widetilde{\phi}$ we can see

$$\widetilde{\phi}\left(x^M\right) = \widetilde{\phi}\left(y_1^{\sigma_1}...y_k^{\sigma_k}\right) \implies x^M \equiv y_1^{\sigma_1}...y_k^{\sigma_k} \mod I.$$

This already implies $N_{\mathcal{B}}\left(x^M\right) = N_{\mathcal{B}}\left(y_1^{\sigma_1}...y_k^{\sigma_k}\right).$

III. $\mathcal{F}$ and $\mathcal{G}$ are injective.

Should we have two non–negative integers N_1, N_2 with

$$exp\left(N_{\mathcal{B}}\left(x^{N_1}\right)\right) = exp\left(N_{\mathcal{B}}\left(x^{N_2}\right)\right)$$

this implies $x^{N_1} \equiv x^{N_2} \mod I$. Then there are polynomials $h_1, ..., h_r$ with

$$x^{N_1} = x^{N_2} + \sum_{i=1}^{k} h_i(y_i - x^{a_i}),$$

and doing $y_i = x^{a_i}$ we get $x^{N_1} = x^{N_2}$ and $N_1 = N_2$. $\qquad \square$

EXAMPLE 2.10. Let us see a simple example, for a semigroup of dimension 2, $S\langle 5, 7\rangle$. Following Sylvester,

$$f(S) = 5 \cdot 7 - 5 - 7 = 23,$$

and its set of gaps is

$$G(S) = \{1, \ 2, \ 3, \ 4, \ 6, \ 8, \ 9, \ 11, \ 13, \ 16, \ 18, \ 23\}.$$

We consider then the ideal

$$I = \langle y_1 - x^5, \ y_2 - x^7 \rangle \subset \mathbb{Q}[x, y_1, y_2],$$

and we compute the (minimal) Groebner basis of I, using an elimination ordering for x. We have chosen the lex ordering $x > y_1 > y_2$. The resulting Groebner basis is
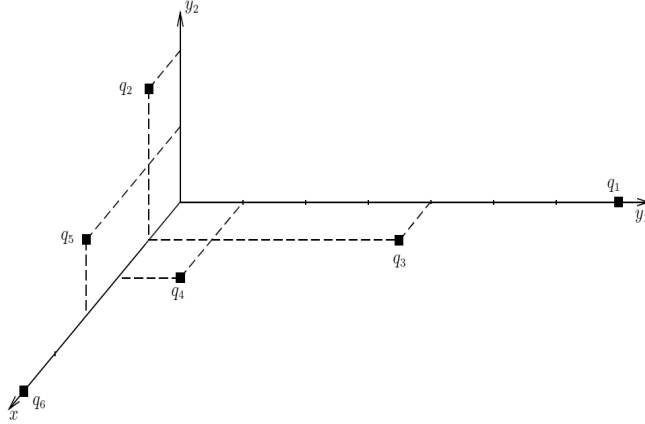
$$\mathcal{B} = \left\{ -y_2^5 + y_1^7, \ -y_1^3 + y_2^2 x, \ -y_2^3 + y_1^4 x, \ y_1 x^2 - y_2, \ y_2 x^3 - y_1^2, \ -y_1 + x^5 \right\}.$$

We can constuct now the sets

$$K_{q_i} = q_i + \mathbb{Z}_{\geq 0}^3 \subset \mathbb{Z}_{\geq 0}^3,$$

with the exponents of the elements in $\mathcal{B}$ (square points in the picture below):

$$
\begin{array}{lclclcl}
q_1 & = & (0,7,0), & q_2 & = & (1,0,2), & q_3 & = & (1,4,0), \\
q_4 & = & (2,1,0), & q_5 & = & (3,0,1), & q_6 & = & (5,0,0).
\end{array}
$$
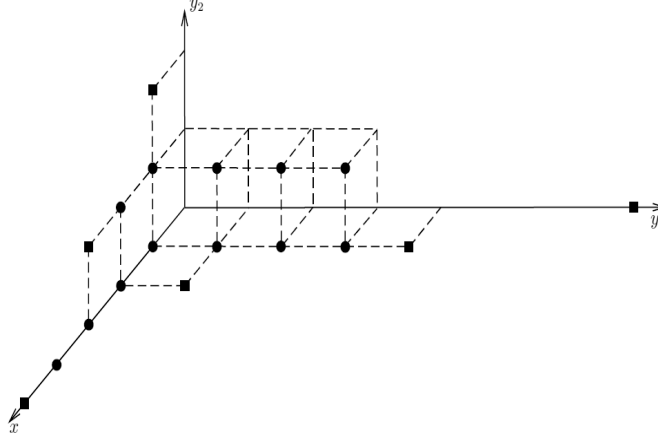

Now we check all elements from $G(S)$ and their one–to–one correspondence with

$$\left[\bigcap_i \overline{K_{q_i}} \right] \setminus \{x = 0\} \bigcap \mathbb{Z}_{\geq 0}^3$$

In order to do this, we compute the normal form of all monomials x^M with $M \in G(S)$, obtaining:

$$
\begin{array}{lclclclclcl}
N_{\mathcal{B}}(x^1) & = & x & \quad N_{\mathcal{B}}(x^2) & = & x^2 & \quad N_{\mathcal{B}}(x^3) & = & x^3 \\
N_{\mathcal{B}}(x^4) & = & x^4 & \quad N_{\mathcal{B}}(x^6) & = & xy_1 & \quad N_{\mathcal{B}}(x^8) & = & xy_2 \\
N_{\mathcal{B}}(x^9) & = & x^2 y_2 & \quad N_{\mathcal{B}}(x^{11}) & = & xy_1^2 & \quad N_{\mathcal{B}}(x^{13}) & = & xy_1 y_2 \\
N_{\mathcal{B}}(x^{16}) & = & xy_1^3 & \quad N_{\mathcal{B}}(x^{18}) & = & xy_1^2 y_2 & \quad N_{\mathcal{B}}(x^{23}) & = & xy_1^3 y_2
\end{array}
$$

These points can be seen in the lattice $\mathbb{Z}^3$, as expected (round points in the picture).

EXAMPLE 2.11. Let us consider now an example of dimension 3. Let $S = \langle 7, 9, 11 \rangle$. The Frobenius number of this numerical semigroup is:

$$f(S) = 26,$$

and its set of gaps:

$$G(S) = \{1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 8,\ 10,\ 12,\ 13,\ 15,\ 17,\ 19,\ 24,\ 26\}.$$

We can take the binomial ideal:

$$I = \langle y_1 - x^7, y_2 - x^9, y_3 - x^{11} \rangle \subset \mathbb{Q}[x, y_1, y_2, y_3]$$

and find the Groebner basis $\mathcal{B}$, using an elimination ordering w.r.t. x. For this example, we have taken the usual lexicographic ordering $x > y_1 > y_2 > y_3$. With this particular choice we get:

$$\begin{aligned}
\mathcal{B} \quad = \quad & \{y_2^{11} - y_3^9, -y_2^2 + y_3 y_1, y_2^9 y_1 - y_3^8, y_2^7 y_1^2 - y_3^7, y_2^5 y_1^3 - y_3^6, y_2^3 y_1^4 - y_3^5, \\
& y_1^5 y_2 - y_3^4, -y_2 y_3^3 + y_1^6, -y_2 y_1^2 + y_3^2 x, -y_1^3 + y_3 y_2 x, y_2^3 x - y_1^4, \\
& y_2^2 y_1^2 x - y_3^3, -y_3^2 + y_1^3 x, y_2 x^2 - y_3, y_1 x^2 - y_2, y_3 x^3 - y_1^2, -y_1 + x^7\}
\end{aligned}$$

We have to consider then, $q_i = exp(lt(g_i))$ where g_i is the i–th polynomial in $\mathcal{B}$, and take the corresponding set

$$K_{q_i} = q_i + \mathbb{Z}_{\geq 0}^{k+1} \subset \mathbb{Z}_{\geq 0}^{k+1},$$

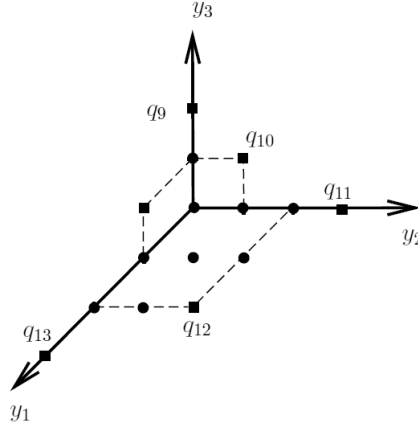in order to establish our bijections $\mathcal{F}$ and $\mathcal{G}$. In this case,

$$\begin{array}{llllll}
q_1 & = & (0, 0, 11, 0), & q_2 & = & (0, 1, 0, 1), \\
q_4 & = & (0, 2, 7, 0), & q_5 & = & (0, 3, 5, 0), \\
q_7 & = & (0, 5, 1, 0), & q_8 & = & (0, 6, 0, 0), \\
q_{10} & = & (1, 0, 1, 1), & q_{11} & = & (1, 0, 3, 0), \\
q_{13} & = & (1, 3, 0, 0), & q_{14} & = & (2, 0, 1, 0), \\
q_{16} & = & (3, 0, 0, 1), & q_{17} & = & (7, 0, 0, 0)
\end{array}$$

$$\begin{array}{lll}
q_3 & = & (0, 1, 9, 0), \\
q_6 & = & (0, 4, 3, 0), \\
q_9 & = & (1, 0, 0, 2), \\
q_{12} & = & (1, 2, 2, 0), \\
q_{15} & = & (2, 1, 0, 0),
\end{array}$$

Let us have a closer look to $\mathcal{F}$, so we are only interested in points of $\overline{\cup K_{q_i}}$ outside $x = 0$. In order to represent the points, we will consider the subcases $x = \lambda$, with $\lambda \in \mathbb{Z}_{\geq 0}$. We have then:

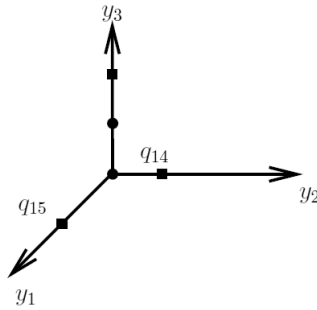- $x = 1$. In this hyperplane we find several corners q_i, precisely

$$q_9 = (0,0,2), \ q_{10} = (0,1,1), \ q_{11} = (0,3,0), \ q_{12} = (2,2,0), \ q_{13} = (3,0,0)$$

These points determine the elements of $\mathbb{Z}_{\geq 0}^4 \setminus \cup K_{q_i}$, along with $(1,1,0,1) \in K_{q_2}$. As in the previous pictures, we will draw square points for points in $\cup K_{q_i}$, and round points for points outside $\cup K_{q_i}$, thus associated with a unique element of $G(S)$ by means of $\mathcal{F}$:
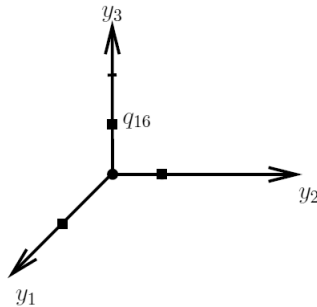

- At $x = 2$ these are the points which determine the set:

$$q_{14} = (0,1,0), \ q_{15} = (1,0,0), \ (0,0,2) \in K_{q_9}$$

- At $x = 3$, we have these points in $\cup K_{q_i}$

$$q_{16} = (0,0,1), \ (1,0,0) \in K_{q_{15}}, \ (0,1,0) \in K_{q_{14}}$$

- At $x = 4$, $x = 5$ and $x = 6$, the only relevant point is the origin, as $y_i < 1$ for $i = 1, 2, 3$
- Last, in $x = 7$ we have $(7, 0, 0, 0) = q_{17}$, so this is, so to speak, the *ceiling* for variable x.

If we compute the normal form of monomials x^{n_i}, where n_i is the i–th gap, we get:

$$
\begin{array}{lcllcllcl}
N_{\mathcal{B}}(x^1) & = & x & N_{\mathcal{B}}(x^2) & = & x^2 & N_{\mathcal{B}}(x^3) & = & x^3 \\
N_{\mathcal{B}}(x^4) & = & x^4 & N_{\mathcal{B}}(x^5) & = & x^5 & N_{\mathcal{B}}(x^6) & = & x^6 \\
N_{\mathcal{B}}(x^8) & = & xy_1 & N_{\mathcal{B}}(x^{10}) & = & xy_2 & N_{\mathcal{B}}(x^{12}) & = & xy_3 \\
N_{\mathcal{B}}(x^{13}) & = & x^2 y_3 & N_G(x^{15}) & = & xy_1^2 & N_{\mathcal{B}}(x^{17}) & = & xy_1 y_2 \\
N_{\mathcal{B}}(x^{19}) & = & xy_2^2 & N_{\mathcal{B}}(x^{24}) & = & xy_1^2 y_2 & N_{\mathcal{B}}(x^{26}) & = & xy_1 y_2^2
\end{array}
$$

REMARK 2.12. Therefore, for a given $N \geq 0$ we have a representation

$$
exp\left(N_{\mathcal{B}}(x^N)\right) = (\sigma_0, ..., \sigma_k) \implies N = \sigma_0 + \sum_{i=1}^{k} a_i \sigma_i,
$$

which is unique, provided

$$
(\sigma_0, ..., \sigma_k) \in \left[\bigcap_i \overline{K_{q_i}} \right],
$$

and which determines easily whether $N \in S$ or not, simply by looking at σ_0.

Let us consider $N \in S$. A very interesting function related to S (actually to the set $\{a_1, ..., a_k\}$) is the so–called denumerant, which is defined by

$$
\begin{aligned}
d : S & \longrightarrow \mathbb{Z} \\
N & \longmapsto d(N) = \sharp\left\{ (y_1, ..., y_k) \in \mathbb{Z}_{\geq 0}^k \mid N = \sum_{i=1}^{k} y_i a_i \right\}
\end{aligned}
$$

That is, $d(N)$ is nothing but the number of different representations of N as a non–negative integral linear combination of $\{a_1, ..., a_k\}$. The notion of denumerant was rst introduced by Sylvester [**14**].

On the other hand, if we take $N \in S$, aside from the representation mentioned above, we might have lots of others, only all of them in $\cup K_{q_i}$. Just in case someone is tempted, where is no relationship between $d(N)$ and

$$
\sharp\left\{ q_i \mid x^N \in K_{q_i} \right\},
$$

as an easy example may show.

Take as before $S = \langle 5, 7 \rangle$, and consider $N = 100$. The number of non–negative representations $100 = 5y_1 + 7y_2$ can be computed quickly, as all integral representations are given by

$$
y_1 = 7n + 6, \quad y_2 = -5n + 10, \quad n \in \mathbb{Z}.
$$

Hence only $n = 0, 1, 2$ are suitable, and therefore $d(100) = 3$. Analogously for $N = 327$ we get

$$
y_1 = 7n + 1, \quad y_2 = -5n + 46, \quad n \in \mathbb{Z}.
$$

hence we get $d(N) = 10$. However, both elements lie in the same quadrant K_{q_6}, and only in this one.

3. A first application: a bound "á la Wilf"

One of the most celebrated open problems in numerical semigroups is the so–called Wilf's Conjecture [**16**], which states a very simple relationship among three important invariants:

Wilf's Conjeture.– Let S be a numerical semigroup. Then

$$c(S) \leq e(S)n(S).$$

That is to say, the conjecture fixes a lower bound for the proportion of sporadic elements among those non–negative integers smaller than the conductor of S: they must represent, at least, $1/e(S)$ of them.

The conjecture has been proved for a number of particular cases (see for instance [**6, 12**]). It has also been checked for semigroups of genus up to 50 by M. Bras–Amorós [**2**].

What follows is our approximation to the problem of relating $n(S)$ and $c(S)$, using the techniques introduced above, resulting in a couple of bounds of different nature.

Notation.– Given rational positive numbers $\alpha_1, ..., \alpha_n$, we define

$$P(\alpha_1, ..., \alpha_n) = \left\{ (x_1, ..., x_n) \in \mathbb{Z}_{>0}^n \mid \frac{x_1}{\alpha_1} + ... + \frac{x_n}{\alpha_n} \leq 1 \right\}$$

$$Q(\alpha_1, ..., \alpha_n) = \left\{ (x_1, ..., x_n) \in \mathbb{Z}_{\geq 0}^n \mid \frac{x_1}{\alpha_1} + ... + \frac{x_n}{\alpha_n} \leq 1 \right\}$$

and

$$p(\alpha_1, ..., \alpha_n) = \sharp (P(\alpha_1, ..., \alpha_n))$$
$$q(\alpha_1, ..., \alpha_n) = \sharp (Q(\alpha_1, ..., \alpha_n))$$

That is, $q(\alpha_1, ..., \alpha_n)$ is the number of integral points in the tetrahedron limited by the coordinate hyperplanes and

$$\frac{x_1}{\alpha_1} + ... + \frac{x_n}{\alpha_n} = 1,$$

as $p(\alpha_1, ..., \alpha_n)$ is the same thing, but discarding the points in the coordinate faces.

The relationship between these two quantities is given by the following result.

Lemma 3.1. *Under the previous conditions, if we call*

$$\alpha = \frac{1}{\alpha_1} + ... + \frac{1}{\alpha_n},$$

then

$$q(\alpha_1, ..., \alpha_n) = p(\alpha_1(1 + \alpha), ..., \alpha_n(1 + \alpha)).$$

Proof. Let us consider the following map:

$$\Phi : Q(\alpha_1, ..., \alpha_n) \longrightarrow P(\alpha_1(1 + \alpha), ..., \alpha_n(1 + \alpha))$$
$$(x_1, ..., x_n) \longmapsto (x_1 + 1, ..., x_n + 1)$$

It is well–defined, as

$$\sum_{i=1}^{n} \frac{x_i + 1}{\alpha_i(1 + \alpha)} = \frac{1}{1 + \alpha}\left(\sum_{i=1}^{n}\frac{x_i}{\alpha_i} + \sum_{i=1}^{n}\frac{1}{\alpha_i}\right) \leq 1,$$

hence $Im(\Phi) \subset P(\alpha_1(1 + \alpha), ..., \alpha_n(1 + \alpha))$.

Φ is clearly injective, but is also surjective because

$$\sum_{i=1}^{n}\frac{x_i}{\alpha_i(1 + \alpha)} \leq 1 \iff \sum_{i=1}^{n}\frac{x_i}{\alpha_i} \leq 1 + \alpha \iff \sum_{i=1}^{n}\frac{x_i - 1}{\alpha_i} \leq 1.$$

$\square$

The hunt for a good, simple estimate of $q(\alpha_1, ..., \alpha_n)$ and $p(\alpha_1, ..., \alpha_n)$ led to several results [**7, 8, 9, 15, 17, 18, 19**], finally put together in the GLY Conjeture, named after its authors Granville, Lin and Yau.

GLY Conjecture.– Assume $n \geq 3$ and let $\alpha_1 \geq ... \geq \alpha_n \geq 1$ be real numbers. Then:

- (Weak estimate) We have

$$n! \cdot p(\alpha_1, ..., \alpha_n) \leq (\alpha_1 - 1)...(\alpha_n - 1),$$

  with equality if and only if $\alpha_n = 1$.
- (Strong estimate) Given n, there is a constant $C(n)$ such that, for $\alpha_n \geq C(n)$ we have

$$n! \cdot p(\alpha_1, ..., \alpha_n) \leq A_n^n + (-1)\frac{S_1^{n-1}}{n}A_{n-1}^n + \sum_{l=2}^{n-1}(-1)^l\frac{S_l^{n-1}}{\binom{n-1}{l-1}}A_{n-l}^{n-1},$$

  where S_l^{n-1} are the Stirling numbers, and A_i^l are polynomials in $\alpha_1, ..., \alpha_l$ with degree i.

The weak version was finally proved by Yau and Zhang [**20**]. In the same paper, the authors claim the strong version has been checked computationally up to $n \leq 10$. The fact is the conjecture might be checked for a particular n, but the state–of–the–art has not changed since. According to the authors, the case $n = 10$ took weeks to be completed.

Assume then we have a numerical semigroup $S = \langle a_1, ..., a_k \rangle$ and let us consider the binomial ideal associated to S, as in the previous section

$$I = \langle\, y_i - x^{a_i} \mid i = 1, ..., k \,\rangle \subset \mathbb{Q}[x, y_1, ..., y_k].$$

Let us fix an elimination ordering for x and let us compute the Groebner basis $\mathcal{B}$ and the corresponding sets K_{q_i}. As we know

$$S \xleftrightarrow{1:1} \left[\bigcap_i \overline{K_{q_i}}\right]\bigcap\{x = 0\} \subset \mathbb{Z}_{\geq 0}^{k+1}$$

Therefore we may note

$$
\begin{aligned}
n(S) &= \sharp\{a \in S \mid a \leq f(S)\} \\
&= \sharp\left\{(0, y_1, ..., y_k) \in \left[\bigcap_i \overline{K_{q_i}}\right] \mid \sum y_i a_i \leq f(S)\right\} \subset \mathbb{Z}_{\geq 0}^{k+1},
\end{aligned}
$$

which proves that $n(S)$ is less or equal to the number of integral points in the tetrahedron defined by the coordinate hyperplanes and

$$
\frac{y_1}{f(S)/a_1} + ... + \frac{y_k}{f(S)/a_k} \leq 1.
$$

That is,

$$
n(S) \leq q\left(\frac{f(S)}{a_1}, ..., \frac{f(S)}{a_k}\right),
$$

and from the previous lemma and the Weak estimate of the GLY Conjecture,

$$
\begin{aligned}
n(S) &\leq p\left(\frac{f(S)}{a_1}\left(1 + \sum \frac{a_i}{f(S)}\right), ..., \frac{f(S)}{a_k}\left(1 + \sum \frac{a_i}{f(S)}\right)\right) \\
&= p\left(\frac{f(S) + \sum a_i}{a_1}, ..., \frac{f(S) + \sum a_i}{a_k}\right) \\
&\leq \frac{1}{k!}\prod_{j=1}^{k}\left(\frac{f(S) + \sum a_i}{a_j} - 1\right) \\
&= \frac{1}{k!\, a_1...a_k}\prod_{j=1}^{k}\left(f(S) + \sum_{i \neq j} a_i\right)
\end{aligned}
$$

We have then proved:

PROPOSITION 3.2. *Given a numerical semigrup $S = \langle a_1, ..., a_k\rangle$, we have*

$$
n(S) \leq \frac{1}{k!\, a_1...a_k}\prod_{j=1}^{k}\left(f(S) + \sum_{i \neq j} a_i\right)
$$

Hence we have actually proved a result which is, in certain sense, a reverse of Wilf's Conjecture, as we have actually proved an upper bound for $n(S)$ in terms of:

- k, which is an upper bound for $e(S)$, although it can be assumed from the beginning to be $e(S)$.
- $f(S)$.
- The generators of S.

REMARK 3.3. Note that, if we make $k = 2$ in the statement above, we get

$$
n(S) \leq \frac{1}{2a_1a_2}\left(a_1a_2 - a_1\right)\left(a_1a_2 - a_2\right) = \frac{(a_1 - 1)(a_2 - 1)}{2} = n(S),
$$

from Sylvester's result. So, in this case (where we cannot apply the GLY weak estimate, as it is valid for $k \geq 3$), the formula is still valid. Not only that, but the bound turns out to be an equality.

REMARK 3.4. Accuracy of the bound. In the following tables there are some examples of numerical semigroups, with the relevant information concerning the previous result.

As it becomes plain, the bound gets less and less accurate as n grows. A significant number of examples could be of help in order to look for a conjectural improvement, we are still far from that.

Dimension	Generators	$f(S)$	$n(S)$	Bound	Bound/$n(S)$
3	$\{5,6,11\}$	19	8	19	$\simeq 2.375$
3	$\{5,6,19\}$	14	5	10	$\simeq 2.000$
3	$\{5,7,16\}$	18	8	14	$\simeq 1.750$
3	$\{5,7,23\}$	18	7	13	$\simeq 1.857$
3	$\{6,9,20\}$	43	21	44	$\simeq 2.095$
3	$\{7,9,38\}$	40	18	28	$\simeq 1.555$
3	$\{7,9,40\}$	38	16	26	$\simeq 1.625$
3	$\{7,9,47\}$	40	17	28	$\simeq 1.647$
3	$\{7,48,50\}$	143	62	94	$\simeq 1.516$
3	$\{8,9,47\}$	46	20	31	$\simeq 1.550$
3	$\{8,9,55\}$	47	20	32	$\simeq 1.600$
3	$\{9,10,53\}$	61	28	42	$\simeq 1.500$

Dimension	Generators	$f(S)$	$n(S)$	Bound	Bound/$n(S)$
4	$\{7,11,34,37\}$	38	14	50	$\simeq 3.571$
4	$\{7,11,23,24\}$	27	8	31	$\simeq 3.875$
4	$\{7,11,23,17\}$	31	11	38	$\simeq 3.454$
4	$\{11,25,37,56\}$	101	40	110	$\simeq 2.750$
4	$\{11,25,37,115\}$	104	42	120	$\simeq 2.857$
4	$\{11,25,37,104\}$	101	40	111	$\simeq 2.775$
4	$\{9,13,19,21\}$	33	10	35	$\simeq 3.500$
4	$\{9,10,21,35\}$	43	18	59	$\simeq 3.277$
4	$\{8,11,13,15\}$	25	8	31	$\simeq 3.875$
4	$\{13,15,31,63\}$	81	34	94	$\simeq 2.764$
4	$\{13,16,33,56\}$	86	34	98	$\simeq 2.882$
4	$\{13,15,31,63\}$	81	34	94	$\simeq 2.764$

Dimension	Generators	$f(S)$	$n(S)$	Bound	Bound/$n(S)$
5	$\{7,11,31,34,37\}$	30	9	86	$\simeq 9.555$
5	$\{7,15,18,26,34\}$	38	17	112	$\simeq 6.588$
5	$\{9,10,21,35,43\}$	34	11	99	$\simeq 9.000$
5	$\{10,19,31,37,54\}$	65	25	154	$\simeq 6.160$
5	$\{8,11,13,15,20\}$	25	11	72	$\simeq 6.545$
5	$\{8,11,13,15,25\}$	20	6	53	$\simeq 8.833$
6	$\{10,19,31,37,54,65\}$	63	24	366	$\simeq 15.250$
6	$\{10,19,31,37,54,63\}$	65	26	382	$\simeq 14.692$

We will try a different approach, taking advantage of the catalogue of Groebner basis at our disposal. Let us take the lexicographic elimination ordering given by

$$x < y_k < ... < y_2 < y_1.$$

Let us fix an integer $\alpha \geq 0$, and consider

$$n(S, \alpha) = \sharp\{x \in S \mid x \leq \alpha\},$$

so in particular $n(S, f(S)) = n(S)$. We also have, as before

$$n(S, \alpha) = \sharp\left\{Y = (y_1, ..., y_k) \in \mathbb{Z}_{\geq 0}^k \mid y_i \geq 0, \sum a_i y_i \leq \alpha, \ Y \notin \left[\bigcup_i K_{q_i}\right]\right\}$$

Let us call, without further mention of the bijection $\mathcal{G}$, $N(S, \alpha)$ the previous set, whose number of points is $n(S, \alpha)$. Mind that

$$Y = (y_1, ..., y_k) \in N(S, \alpha) \implies 0 \leq y_1 \leq \frac{\alpha}{a_1}$$

Assume first that we have $\alpha \geq a_1 a_2$, the other case will be dealt with later and with some important differences. That is, for now we will consider

$$\frac{\alpha}{a_1} - a_2 \geq 0.$$

We are going to compute a bound for the set $N(S, \alpha)$ in two stages:
- First, we will construct a truncated prism C over a $(k-1)$–hypercube, which will contain all points in $N(S, \alpha)$ with $0 \leq y_1 \leq \alpha/a_1 - a_2$.
- After this, we will construct a pyramid D which will contain the rest of the integral points in $N(S, \alpha)$, and we will compute with no great difficulty the number of integral points inside this pyramid.

Let us construct C. First note that the binomials $y_i^{a_1} - y_1^{a_i} \in I$, for all $i = 2, ..., k$. As their exponents are

$$(0, ..., 0, \overset{(i)}{a_1}, 0, ..., 0) \in \mathbb{Z}_{\geq 0}^k,$$

we have that

$$(0, ..., 0, \overset{(i)}{a_1}, 0, ..., 0) \in \left[\bigcup_i K_{q_i}\right] \subset \mathbb{Z}_{\geq 0}^k.$$
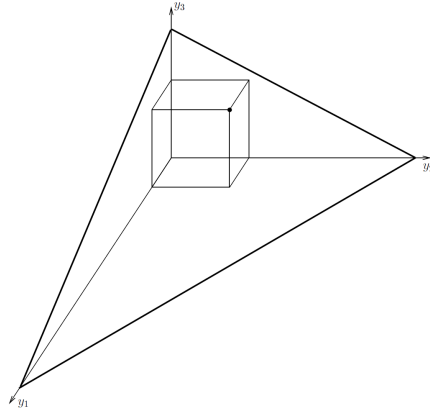
and then

$$
\begin{aligned}
N(S, \alpha) &= \left\{Y = (y_1, ..., y_k) \in \mathbb{Z}_{\geq 0}^k \mid y_i \geq 0, \sum a_i y_i \leq \alpha, \ Y \notin \left[\bigcup_i K_{q_i}\right]\right\} \\
&\subset \left\{Y = (y_1, ..., y_k) \in \mathbb{Z}_{\geq 0}^k \mid 0 \leq y_i < a_1, \text{ for } i = 2, ..., k\right\} = C_0,
\end{aligned}
$$

which is clearly a prism over a $(k-1)$–hypercube.

This bound could fit for all the set $N(S)$, but we will try to do better in the following way. First, we will compute at which point(s) the prism C_0 *hits the wall* defined by

$$a_1 y_1 + ... + a_k y_k = \alpha.$$

If we set $y_2 = ... = y_k = a_1$, then the (integral) boundary of C_0 and the wall meet at the point

$$R_0 = \left(\frac{\alpha}{a_1} - \sum_{i=2}^{k} a_i, a_1, ..., a_1 \right).$$

In order to construct a pyramid which is easier to work with, we will take a little more from C_0 before truncating it, so we will actually get out of $N(S, \alpha)$. More precisely, we will get to the point
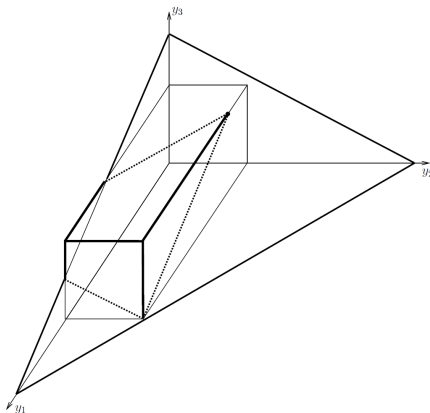
$$R_1 = \left(\frac{\alpha}{a_1} - a_2, a_1, ..., a_1 \right).$$

So, for now, what we have is

$$N(S, \alpha) \bigcap \left\{ y_1 \leq \frac{\alpha}{a_1} - a_2 \right\}$$

is contained in the truncated prism defined by

$$C = \left\{ (y_1, ..., y_k) \in \mathbb{Z}_{\geq 0}^k \mid y_1 \leq \frac{\alpha}{a_1} - a_2, \ y_i < a_1 \text{ for } i = 2, ..., k \right\}$$

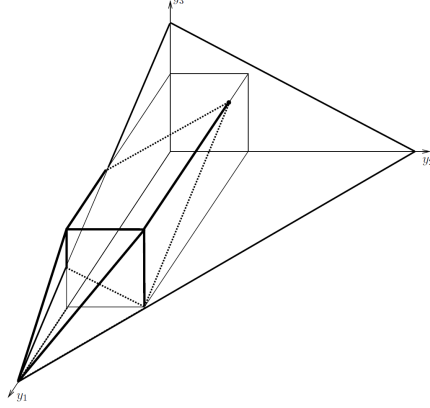Let us now build our pyramid D, which will have as its basis a $(k-1)$–convex on the hyperplane

$$y_1 = \frac{\alpha}{a_1} - a_2,$$

and its vertex at

$$V = \left(\frac{\alpha}{a_1}, 0, ..., 0 \right).$$

The precise description is

$$D = \left\{ V + \lambda_1 \left(-a_2, 0, ..., 0 \right) + \sum_{i=2}^{k} \lambda_1 \lambda_i (0, ..., 0, \overset{(i)}{a_1}, 0, ..., 0) \mid 0 \leq \lambda_i \leq 1, \ \forall i \right\}.$$

LEMMA 3.5. *Under the previous conditions, we have*

$$N(S, \alpha) \bigcap \left\{ y_1 \geq \frac{\alpha}{a_1} - a_2 \right\} \subset D.$$

PROOF. Let us take an integral point $P = (y_1, ..., y_k) \in N(S, \alpha)$, with

$$\frac{\alpha}{a_1} - a_2 \leq y_1 \leq \frac{\alpha}{a_1},$$

and let us write

$$y_1 = \frac{\alpha}{a_1} - \lambda_1 a_2 \implies \lambda_1 = \frac{\alpha/a_1 - y_1}{a_2},$$

and clearly $0 \leq \lambda_1 \leq 1$. Obviously, we have to define

$$\lambda_i = \frac{y_i}{\lambda_1 a_1}, \text{ for } i = 2, ..., k;$$

in order to write P as in the definition of D.

It is straightforward that $\lambda_i \geq 0$. On the other hand, one has that, P being in $N(S, \alpha)$,

$$\alpha \geq a_1 y_1 + ... + a_k y_k = \alpha - \lambda_1 a_1 a_2 + \sum_{i=2}^{k} a_i y_i$$

and then, for $i = 2, ..., k$;

$$a_i y_i \leq a_2 y_2 + ... + a_k y_k \leq \lambda_1 a_1 a_2 \leq \lambda_1 a_1 a_i,$$

which implies $y_i \leq \lambda_1 a_1$ and therefore $\lambda_i \leq 1$, for $i = 2, ..., k$. $\qquad\square$

We have finally proved:

PROPOSITION 3.6. *With the previous definitions and assumptions, we have*

$$N(S, \alpha) \subset C \cup D.$$

COROLLARY 3.7. *With the previous definitions and assumptions, we have*

$$n(S, \alpha) \leq \sharp \left(C \cup D \cap \mathbb{Z}_{\geq 0}^k \right).$$

The number of integral points in C is easy to compute:

$$\sharp \left(C \cap \mathbb{Z}_{\geq 0}^k \right) = a_1^{k-1} \left(\left\lfloor \frac{\alpha}{a_1} - a_2 \right\rfloor + 1 \right)$$

If a_1 does not divide α, we can alternatively express it as

$$\sharp \left(C \cap \mathbb{Z}_{\geq 0}^k \right) = a_1^{k-1} \left(\left\lceil \frac{\alpha}{a_1} \right\rceil - a_2 \right).$$

In order to find the number of integral points in D, let us fix our attention in a y_1–constant level of the pyramid. That is, fix λ_1 such that

$$\frac{\alpha}{a_1} - \lambda_1 a_2 \in \mathbb{Z},$$

and then the set

$$D \bigcap \left\{ y_1 = \frac{\alpha}{a_1} - \lambda_1 a_2 \right\} \bigcap \mathbb{Z}_{\geq 0}^k$$

is once again a $(k-1)$–hypercube determined by the vertices

$$\lambda_1(0, ..., 0, \overset{(i)}{a_1}, 0, ..., 0) \text{ for } i = 2, ..., k;$$

which have therefore $(\lfloor \lambda_1 a_1 \rfloor + 1)^{k-1}$ integral points.

All we need therefore is a precise description of the λ_1 which verify

$$\frac{\alpha}{a_1} - \lambda_1 a_2 \in \mathbb{Z}.$$

There must then be a $\lambda \in \mathbb{Z}$ such that

$$\frac{\alpha}{a_1} - \lambda_1 a_2 = \left\lfloor \frac{\alpha}{a_1} \right\rfloor - \lambda,$$

and this λ must verify $0 \leq \lambda \leq a_2 - 1$, for

$$\alpha/a_1 - a_2 < y_1 \leq \alpha/a_1$$

to hold. As

$$\lambda_1 = \frac{\lambda + \alpha/a_1 - \lfloor \alpha/a_1 \rfloor}{a_2} = \frac{\lambda + \{\alpha/a_1\}}{a_2},$$

we have the number of points at the level determined by λ is

$$\sharp \left(D \bigcap \left\{ y_1 = \left\lfloor \frac{\alpha}{a_1} \right\rfloor - \lambda \right\} \bigcap \mathbb{Z}_{\geq 0}^k \right) = \left(\left\lfloor a_1 \cdot \frac{\lambda + \{\alpha/a_1\}}{a_2} \right\rfloor + 1 \right)^{k-1}$$

and

$$\sharp \left(D \bigcap \mathbb{Z}_{\geq 0}^k \right) = \sum_{\lambda=0}^{a_2-1} \left(\left\lfloor a_1 \cdot \frac{\lambda + \{\alpha/a_1\}}{a_2} \right\rfloor + 1 \right)^{k-1}$$

THEOREM 3.8. *Let* $S = \langle a_1, ..., a_k \rangle$ *be a numerical semigroup,* $\alpha \geq a_1 a_2$ *an integer. Then*

$$n(S, \alpha) \leq a_1^{k-1} \left(\left\lfloor \frac{\alpha}{a_1} - a_2 \right\rfloor + 1 \right) + \sum_{\lambda=0}^{a_2-1} \left(\left\lfloor a_1 \cdot \frac{\lambda + \{\alpha/a_1\}}{a_2} \right\rfloor + 1 \right)^{k-1}.$$

COROLLARY 3.9. *Let $S = \langle a_1, ..., a_k \rangle$ be a numerical semigroup, $\alpha \geq a_1 a_2$ an integer. Then*

$$n(S, \alpha) \leq a_1^{k-1} \left\lfloor \frac{\alpha}{a_1} \right\rfloor$$

PROOF. Directly, extend the prism C up to $y_1 = \alpha/a_1$. Indirectly, as $0 \leq \lambda \leq a_2 - 1$ we have

$$\frac{\lambda + \{\alpha/a_1\}}{a_2} < 1$$

and therefore

$$\left\lfloor a_1 \cdot \frac{\lambda + \{\alpha/a_1\}}{a_2} \right\rfloor + 1 \leq a_1$$

hence

$$\sharp \left(D \bigcap \mathbb{Z}_{\geq 0}^k \right) \leq \sum_{\lambda=0}^{a_2-1} a^{k-1}$$

and finally this implies

$$n(S, \alpha) \leq a_1^{k-1} \left(\left\lfloor \frac{\alpha}{a_1} - a_2 \right\rfloor + 1 \right) + (a_2 - 1) a_1^{k-1} = a_1^{k-1} \left\lfloor \frac{\alpha}{a_1} \right\rfloor,$$
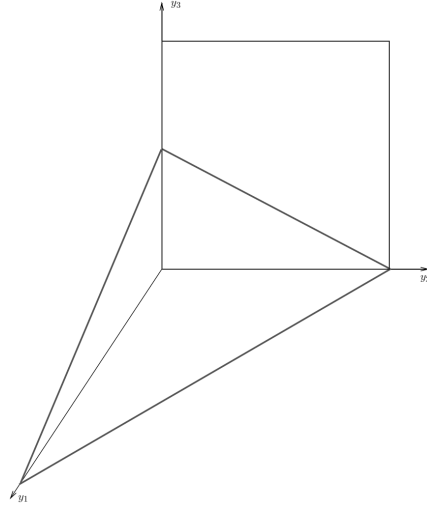
as stated. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \square$

We have been working under the assumption $\alpha \geq a_1 a_2$. The other case $\alpha \leq a_1 a_2$ or, otherwise said

$$\frac{\alpha}{a_1} - a_2 \leq 0,$$

correspond to the following geometric situation: when we construct the prism, the $(k-1)$–hypercube in the basis is already out of $n(S, \alpha)$. We can still consider a pyramid D, much in the same fashion as above, although we must not be very optimistic with respect to the accuracy of the bound.
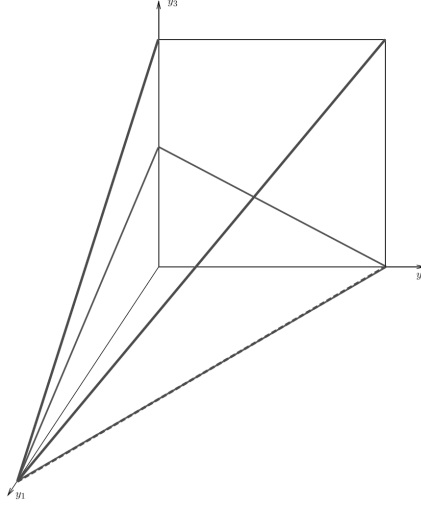
In this case, it is enough to consider the $(k-1)$–hypercube on $y_1 = 0$ to have side length α/a_2.

We will not fill the technical details for this case, which are pretty similiar to the previous one. Let us mention that now the pyramid is:

$$V = \left(\frac{\alpha}{a_1}, 0, ..., 0 \right),$$

$$D = \left\{ V + \lambda_1 \left(-\frac{\alpha}{a_1}, 0, ..., 0 \right) + \sum_{i=2}^{k} \lambda_1 \lambda_i \left(0, ..., 0, \overset{(i)}{\frac{\alpha}{a_2}}, 0, ..., 0 \right) \mid 0 \leq \lambda_i \leq 1, \ \forall i \right\}.$$

In this case, we can simply consider a certain $\lambda \in \mathbb{Z}$ such that

$$0 \leq \lambda \leq \left\lfloor \frac{\alpha}{a_1} \right\rfloor,$$

which determines as above a y_1–constant level which is again a $(k-1)$–hypercube, defined in this case by the points

$$\left(\lambda, ..., 0, \overset{(i)}{\frac{\alpha - \lambda a_1}{a_2}}, 0, ..., 0 \right), \text{ for } i = 2, ..., n.$$

The equivalent result comes from adding up integral points in each y_1– constant level and is therefore as follows:

THEOREM 3.10. *Let* $S = \langle a_1, ..., a_k \rangle$ *be a numerical semigroup,* $0 \leq \alpha \leq a_1 a_2$ *an integer. Then*

$$n(S, \alpha) \leq \sum_{\lambda=0}^{\lfloor \alpha/a_1 \rfloor} \left(\left\lfloor \frac{\alpha - \lambda a_1}{a_2} \right\rfloor + 1 \right)^{k-1}.$$

COROLLARY 3.11. *In the above conditions,*

$$n(S) \leq \sum_{\lambda=0}^{a_2} \left(\left\lfloor a_1 \frac{a_2 - \lambda}{a_2} \right\rfloor + 1 \right)^{k-1} + f(S) - a_1 a_2.$$

PROOF. As $a_1 a_2 \geq f(S)$, we can take $\alpha = a_1 a_2$ and we have that

$$n(S, a_1 a_2) = a_1 a_2 - f(S) + n(S).$$

□

Much work is yet to be done. Most probably a better version of the GLY Conjecture will lead to a more precise results and there might be wiser ways to bound $n(S)$ than the *"prism + pyramid"* method developed here.

We hope this work sheds some light to the power and usefulness of Groebner bases in the study of numerical semigroups.

4. Acknowledgments

References

[1] Adams, W.W.; Loustaunau, Ph.: *An introduction to Gröbner bases.* American Mathematical Society, 1994.

[2] Bras-Amorós, M.: Fibonacci–like behavior of the number of numerical semigroups of a given genus. *Semigroup Forum* **76** (2008) 379–384.

[3] Eisenbud, D.; Sturmfels, B.: Binomial ideals. *Duke Math. J.* **84** (1996) 1–45.

[4] García–Sánchez, P.A.; Rosales, J.C.: *Numerical semigroups.* Springer, 2009.

[5] Herzog, J.: Generators and relations of abelian semigroups and semigroup rings. *Manuscripta Math.* **3** (1970) 175–193.

[6] Kaplan, N.: Counting numerical semigroups by genus and some cases of a question of Wilf. *J. Pure Appl. Algebra* **216** (2012) 1016–1032.

[7] Lin, K.P.; Yau, S.T.: Analysis of sharp polynomial upper estimate of number of positive integral points in 4–dimensional tetrahedra. *J. Reine Angew. Math.* **547** (2002) 191–205.

[8] Lin,K.P.; Yau, S.T.: Analysis of sharp polynomial upper estimate of number of positive integral points in 5–dimensional tetrahedra. *J. Number Theory* **93** (2002) 207–234.

[9] Lin, K.P.; Yau, S.S.T.: Counting the number of integral points in general n–dimensional tetrahedra and Bernoulli polynomials. *Canad. Math. Bull.* **24** (2003) 229–241.

[10] Ramírez–Alfonsín, J.L.: Complexity of the Frobenius problem. *Combinatorica* **16** (1996) 143–147.

[11] Ramírez–Alfonsín, J.L.: *The Diophantine Frobenius problem.* Oxford University Press, 2005.

[12] Sammartano, A.: Numerical semigroups with large embedding dimension satisfy Wilf's conjecture. *Semigroup Forum* **85** (2012) 439–447.

[13] Sylvester, J.J.: Problem 7382. *Educational Times* **37** (1884) 26.

[14] Sylvester, J.J.: On the partition of numbers. *Quart. J. Pure Appl. Math.* **1** (1857) 141–152.

[15] Wang, X.; Yau, S.S.T.: On the GLY conjecture of upper estimate of positive integral points in real right-angled simplices. *J. Number Theory* **122** (2007) 184–210.

[16] Wilf, H.S.: A circle–of–lights algorithm for the money changing problem. *Amer. Math. Monthly* **85** (1978) 562–565.

[17] Xu, Y.J.; Yau, S.S.T.: A sharp estimate of number of integral points in a tetrahedron. *J. Reine Angew. Math.* **423** (1992) 199–219.

[18] Xu, Y.J.; Yau, S.S.T.: Durfee conjecture and coordinate free characterization of homogeneous singularities. *J. Differential Geom.* **37** (1993) 375–396.

[19] Xu, Y.J.; Yau, S.S.T.: A sharp estimate of number of integral points in a 4–dimensional tetrahedra. *J. Reine Angew. Math.* **473** (1996) 1–23.

[20] Yau, S.S.T.; Zhang, L.: An upper estimate of integral points in real simplices with an application to singularity theory. *Math. Res. Lett.* **13** (2006) 911–921.

Departamento de Álgebra, Universidad de Sevilla. P.O. 1160. 41080 Sevilla, Spain.
E-mail address: gmarquez@us.es

Departamento de Álgebra, Universidad de Sevilla. P.O. 1160. 41080 Sevilla, Spain.
E-mail address: tornero@us.es