An algorithm to compute generalised Feng-Rao numbers of a numerical semigroup

Manuel Delgado

CMUP
Centro de Matemática
Universidade do Porto

FACULDADE DE CIÊNCIAS
UNIVERSIDADE DO PORTO
Departamento de Matemática

Seminar of the PHD program
Coimbra, February 11th, 2011

(Joint work with J. I. Farrán, P. A. García-Sánchez and D. Llena)

Outline I

Numerical semigroups

A **numerical semigroup** S is a submonoid of $\mathbb{N} = \mathbb{Z}_{\geq 0}$ (under addition) such that $\sharp(\mathbb{N} \setminus S) < \infty$.

Definitions and notation

Let S be a numerical semigroup.

- The elements of $\mathbb{N} \setminus S$ are said to be the **gaps** of S;
- $\mathbf{g}(S) := \sharp(\mathbb{N} \setminus S)$ is the **genus** of S;
- the unique element $\mathbf{c}(S) \in S$ such that $c(S) - 1 \notin S$ and $c(S) + \ell \in S$ for all $\ell \in \mathbb{N}$ is the **conductor** of S;
- the **Frobenius number** of S is the greatest integer $\mathbf{F(S)}$ not belonging to S (i.e., $F(S) = c(S) - 1$);
- the **multiplicity** of S is the least positive integer belonging to S.

Sometimes we write **g** for $g(S)$ and **c** for $c(S)$.

Fact

Let S be a numerical semigroup. The following inequalities hold: $g(S) + 1 \leq c(S) \leq 2\,g(S)$.

Proof. The first inequality is obvious.
Let $m \in \mathbb{N}$ and consider the sets
$A = \{(r, m-r) \mid 0 \leq r \leq m\}$ and
$B = \{(h, m-h) \mid h \in \mathbb{N} \setminus S\} \cup \{(m-h, h) \mid h \in \mathbb{N} \setminus S\}$.
Note that $\sharp A = m + 1$, $\sharp B = 2g$.
If $m \geq 2g$, then $A \not\subseteq B$ and therefore A contains a pair $(r, m-r)$ such that both components belong to S, giving that $m = r + (m-r) \in S$.
It follows that all integers m such that $m \geq 2g$ belong to S and therefore $c \leq 2g$. □

We say that a numerical semigroup S is generated by a set of elements $G \subseteq S$ if every element $x \in S$ can be written as a linear combination

$$x = \sum_{g \in G} \lambda_g g,$$

where finitely many $\lambda_g \in \mathbb{N}$ are non-zero.

Remark

Let S be a numerical semigroup. $x \in S$ is said to be **irreducible** if $x = u + v$ and $u, v \in S$ implies $u \cdot v = 0$.
Every set of generators of S contains the set of irreducible elements, and this set actually generates S, so that it is usually called **the generating set** of S.
It is finite and its cardinality is called the **embedding dimension** of S.

Let S be a numerical semigroup generated by $n_1 < \cdots < n_e$. By definition, if s belongs to S, then there exists a tuple of nonnegative integers $(a_1, \ldots, a_e)$ such that $s = a_1 n_1 + \cdots + a_e n_e$.

We say that $(a_1, \ldots, a_e)$ is a **factorization** of s in S.

The **length of a factorization** $(a_1, \ldots, a_e)$ is defined as $a_1 + \ldots + a_e$.

Remark

Most of the terminology used in numerical semigroups comes from Algebraic Geometry.

For instance, if S is the Weierstrass semigroup of a curve χ at a point P, g is equal to the geometric genus of χ, and the elements of $G(S) := \mathbb{N} \setminus S$ are called the Weierstrass gaps at P.

Details on numerical semigrops may be found in the book

J.C. Rosales and P. A. García-Sánchez, "Numerical Semigroups", Springer. 2009.

For computations, one can use the following package of the computer algebra system GAP.

M. Delgado, P. A. García-Sánchez and J. Morais, "numericalsgps": a GAP package on numerical semigroups. http://www.gap-system.org/Packages/numericalsgps.html

The Frobenius problem

Frobenius problem

Given positive integers $a_1, \ldots, a_n$, with $\gcd(a_1, \ldots, a_n) = 1$, which is the greatest integer that cannot be written as a non negative linear combination of $a_1, \ldots, a_n$?

The Frobenius problem, although apparently too specialised, appears naturally in several areas of mathematics.

So, to find "formulas" or "efficient algorithms" even for some particular cases may have some interest.

Proposition 1 (Sylvester)

Let p, q be coprime positive integers. Then

$$F(< p, q >) = pq - p - q$$

Sylvester solved the case of numerical semigroups of embedding dimension 2, but no (polynomial) formula is known for semigroups of higher embedding dimension.

For much more on the Frobenius problem, one may consult a book by Ramírez Alfonsín.

J. L. Ramírez Alfonsín, The Diophantine Frobenius Problem, *Oxford Lectures Series in Mathematics and its Applications* **30**, Oxford University Press, (2005).

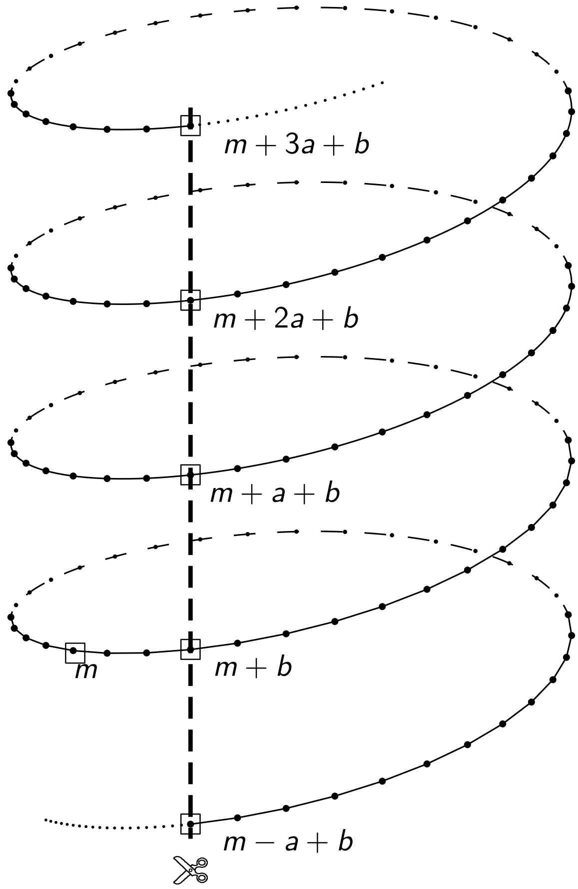
Outline I

Drawings

We can think of the integers as points disposed regularly on a cylindrical helix.

As some of the integers would be hidden, we will consider planifications of the cylinder instead.

They are usually obtained by cutting the cylinder by a vertical line passing through a point previously chosen, and this corresponds to taking a partition of the integers.



We shall use this type of drawings to depict the most relevant parts of the sets considered. For instance, if we want to highlight the elements of a numerical semigroup, we do not add any information by depicting the points below 0 and those above the conductor.

The following parallelograms highlight the elements of the semigroup $S = \langle 9, 13, 15 \rangle$, and the elements of $60 - S$, respectively.

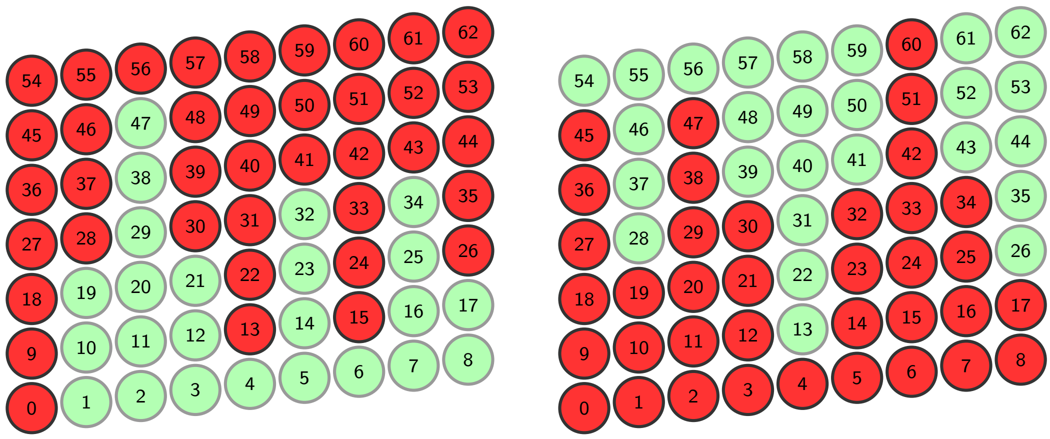
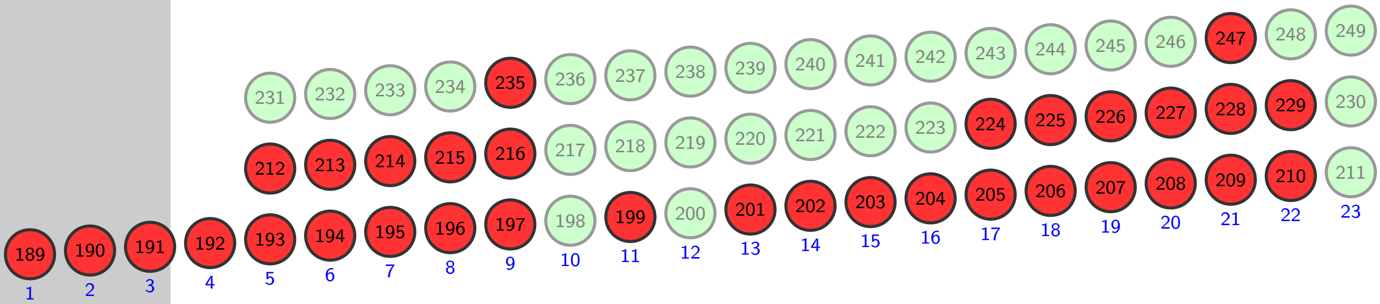


Figure: $S = \langle 9, 13, 15 \rangle$ and $60 - S$, respectively

Most times we are interested in finite sets of integers which are non smaller than a given integer m.
Suppose that the cylinder is cutted by a vertical line passing through $m+b$ and that the length of an arc of the helix is a.
In this case we prefer to draw all the points from m to $m+a+b$ at the same level.

Example

Suppose $m = 189$, $a = 19$ and $b = 4$... The following is a possible figure.



Divisors

Definition

Given $x \in S$, we say that $\alpha \in S$ **divides** x if $x - \alpha \in S$. We denote by $\mathrm{D}(x) = \{\alpha \in S \mid x - \alpha \in S\}$ the set of **divisors** of x.

It i sclear that $\mathrm{D}(x) \subseteq [0, x]$.
Furthemore, noting that $x - s \in S$ and $s - \alpha \in S$ implies $x - \alpha \in S$, we have that $s \in \mathrm{D}(x)$ implies $\mathrm{D}(s) \subseteq \mathrm{D}(x)$.

Lemma 2

$\mathrm{D}(x) = S \cap (x - S)$.

Proof. Let $\alpha \in \mathrm{D}(x)$. By definition, $\alpha \in S$ and $x - \alpha \in S$. But then $\alpha = x - (x - \alpha) \in x - S$.
Conversely, let $\alpha \in S$ be such that there exists $\beta \in S$ for which $x - \beta = \alpha$. But then $x - \alpha = \beta \in S$, proving that α divides x. ☐

We observe that elements greater than x need not to be used to compute the divisors of x. Denoting $S_x = \{n \in S \mid n \leq x\}$, we get the following:

Corollary 3

$\mathrm{D}(x) = S_x \cap (x - S_x)$.

The computation of the divisors of an element can be easily implemented due to this consequence of Lemma 2.

Algorithm 1: Divisors

Input : A numerical semigroup S, $x \in S$
Output: The divisors of x

```
S_x := {s ∈ S | s ≤ x} /* Compute the elements of S smaller
    than x                                                  */
return {s ∈ S_x | x − s ∈ S_x}
```


Note that, once we compute the elements of S smaller than x (which can easily be done if the conductor is known), the computation of the divisors is immediate.
The highlighted elements in Figure 2 represent the divisors of $60 \in \langle 9, 13, 15 \rangle$. They are obtained intersecting the highlighted elements of the pictures in Figure 1.

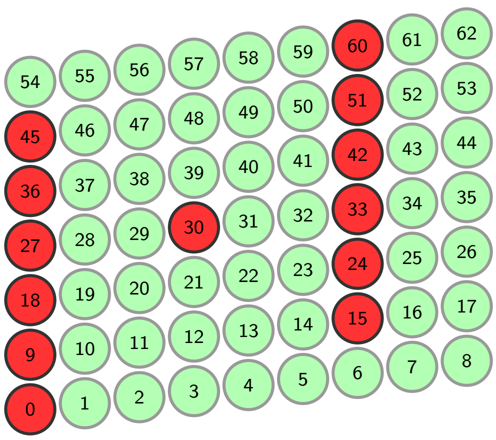


Figure: The divisors of 60 in the semigroup $S = \langle 9, 13, 15 \rangle$

A convenient visualisation of the integers
Divisors

Notation

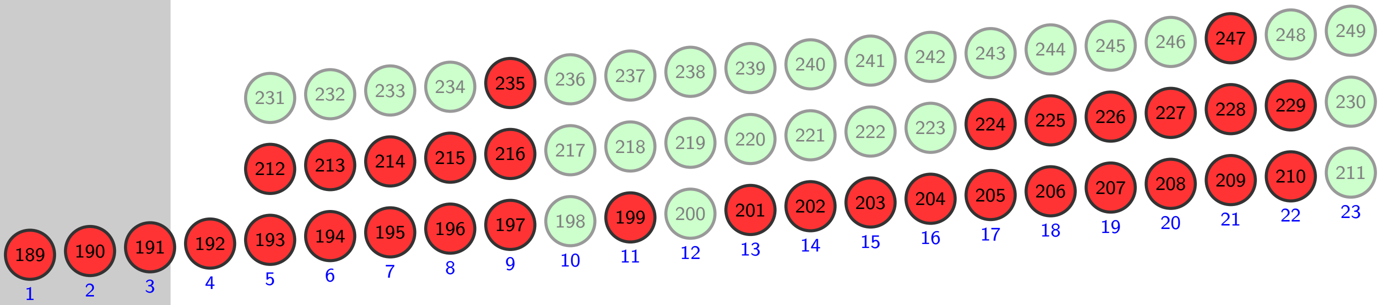
$$\mathrm{D}(m_1,\ldots,m_r)=\mathrm{D}(m_1)\cup\cdots\cup\mathrm{D}(m_r)$$

Example

Let $S=\langle 19,20,21,22,23\rangle$. The elements of

$$D(235,199,247,229)\cap[189,\infty)$$

are the highlighted elements in the following figure.



A convenient visualisation of the integers
Divisors

Let S be a numerical semigroup with conductor c and let $x\geq 2c-1$. Observe that $x-S$ contains all the integers not greater that $x-c$ and that the number of integers smaller than x not belonging to $x-S$ is precisely the genus of S.
As the number of non-negative integers not greater than x is $x+1$, one gets immediately the well known fact:

Proposition 4

If $x\geq 2c-1$, *then* $\sharp\mathrm{D}(x)=\sharp S\cap(x-S)=x+1-2g$.

Outline I

In the framework of the Theory of Error-Correcting Codes, Feng and Rao introduced a notion of distance for the Weirstrass semigroup at a rational point of an algebraic curve, with decoding purposes.
It is a purely combinatorial concept that can be defined for any numerical semigroup. Later on, that notion has been generalised and is used not only in the theory of error correcting codes, but also in cryptography.

Generalized Feng-Rao distances

Definition 5

Let S be a numerical semigroup. The (classical) **Feng-Rao distance** *of S is defined by the function*

$$\begin{array}{rcll} \delta_{FR} : S & \longrightarrow & \mathbb{N} \\ m & \mapsto & \delta_{FR}(m) := \min\{\sharp \mathrm{D}(m_1) \mid m_1 \geq m, \ \ m_1 \in S\}. \end{array}$$

There are some well-known facts about the function δ_{FR} for an arbitrary semigroup S.
An important one follows from Proposition 4:

$\delta_{FR}(m) = m + 1 - 2g$ for all $m \in S$ with $m \geq 2c - 1$.

The classical Feng-Rao distance corresponds to $r = 1$ in the following definition.

Definition 6

Let S be a numerical semigroup.
*For any integer $r \geq 1$, the r-***th Feng-Rao distance** *of S is defined by the function*

$$\begin{array}{rcll} \delta^r_{FR} : S & \longrightarrow & \mathbb{N} \\ m & \mapsto & \delta^r_{FR}(m) \end{array}$$

where

$$\delta^r_{FR}(m) = \min\{\sharp \mathrm{D}(m_1, \ldots, m_r) \mid m \leq m_1 < \cdots < m_r, \ \ m_i \in S\}.$$

Few results are known for the numbers δ^r_{FR}. The following describes the asymptotical behavior for $m >> 0$, and was proved by Farrán and Munuera [2].

Proposition 7

There exists a certain constant $E(S, r)$, depending on r and S, such that

$$\delta^r_{FR}(m) = m + 1 - 2g + E(S, r)$$

for $m \geq 2c - 1$.

Definition 8

*The constant $E(S, r)$ is called the r^{th}-**Feng-Rao number** of the semigroup S.*

Note that, when restricted to $S \cap [2c - 1, \infty)$, δ^r_{FR} is strictly increasing.

Definition 9

*Let S be a numerical semigroup an let $m \in S$. A finite subset of $S \cap [m, \infty)$ is called a (S, m)-**configuration**, or, simply, a configuration.*

*A configuration M of cardinality r is said to be **optimal** if $\delta^r_{FR}(m) = \sharp\, D(M)$.*

Recall that we already have a quite efficient algorithm to compute the divisors of an element of a numerical semigroup.

Now we will work towards finding optimal configurations.

Amenable sets

Definition 10

*Let S be a numerical semigroup with conductor c. Let $m, m_1, \dots, m_r$ be integers such that $2c - 1 \leq m = m_1 < \dots < m_r$. We say that the set $M = \{m_1, \dots, m_r\} \subseteq S$ is (S, m, r)-**amenable** if:*

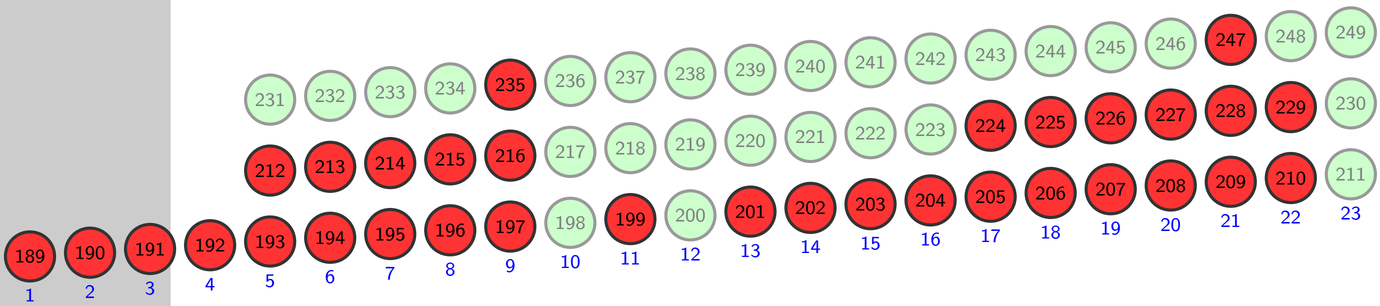
$$\text{for all } i \in \{1, \dots, r\}, \mathrm{D}(m_i) \cap [m, \infty) \subseteq M. \qquad (1)$$

We will refer to a set satisfying (1) as being *m*-**closed under division**. So, a subset of $S \cap [m, \infty)$ with cardinality r is (S, m, r)-amenable if and only if it contains m and is m-closed under division.

As a convention, the empty set is considered an $(S, m, 0)$-amenable set, for any m. When no confusion arises or only the concept is important, we say (m, r)-**amenable** set or, simply, **amenable** set.

Example 11

Let $S = \langle 19, 20, 21, 22, 23 \rangle$. Its conductor is $c = 95$. Take $m = 2c - 1 = 189$. The set M consisting of the highlighted elements of the following figure is an amenable subset of S.



Example 12

Let S be a numerical semigroup with conductor c. Let $m \geq 2c - 1$, and r a non negative integer. Then the interval $[m, m + r - 1] \cap \mathbb{N}$ is a (S, m, r)-amenable set.

The importance of amenable sets comes from the following result, which states that among the optimal configurations of cardinality r there is one (S, m, r)-amenable set.

Proposition 13

Let S be a numerical semigroup with conductor c and let $m \geq 2c - 1$. Let r be a positive integer. Among the optimal configurations of cardinality r there is one (S, m, r)-amenable set.

Proof. Let $M = \{m_1, \ldots, m_r\}$ be an optimal configuration. As δ^r_{FR} is strictly increasing when restricted to $S \cap [2c - 1, \infty)$, m cannot be less than m_1, which implies that $m_1 = m$.

Motivation Divisors Feng Rao Algorithm Application

Feng Rao numbers
Amenable sets

If M is not m-closed under division, we may assume that for some $i \in \{1, \ldots, r\}$ there exists $t \in S$ such that $m_i - t > m$ (which implies $m_i - t \in S$) and $m_i - t \notin \{m_1, \ldots, m_r\}$. As $m_i - t$ divides m_i, we have $\mathrm{D}(m_i - t) \subset \mathrm{D}(m_i)$, and thus

$$\mathrm{D}(m_1, \ldots, m_{i-1}, m_i - t, m_{i+1}, \ldots, m_r) \subseteq \mathrm{D}(m_1, \ldots, m_r).$$

In other words, we can substitute m_i by $m_i - t$ and the number of divisors does not increase.

Now we can repeat the process with the set obtained until we reach a m-closed under division set. Note that this must happen in a finite number of steps ($\mathbb{N}^r$ has no infinite descending chains). $\square$

The definition of amenable set, which seems to be suitable for proofs, does not seem to help very much to do computations unless we can prove some consequences. The following one, proving that the distances between elements is somehow controlled, guarantees that the search of the amenable sets can be done in a bounded subset of S, and therefore all r-amenable sets can be effectively computed. An algorithm will be presented (Algorithm 5).

Proposition 14

Let S be a numerical semigroup with conductor c and let $m \geq 2c - 1$. Let $M = \{m_1 < \cdots < m_r\} \subseteq S$ be an (S, m, r)-amenable set and suppose that $S = \{0 = \rho_1 < \rho_2 < \cdots\}$. Then

(a) $m_i \leq m + \rho_i$, *for all* $i \in \{1, \ldots, r\}$,

(b) $m_{i+1} - m_i \leq \rho_2$, *for all* $i \in \{1, \ldots, r-1\}$.

Proof. (a) Suppose that there exists $i_0 \in \{1, \ldots, r\}$ such that $m_{i_0} - \rho_{i_0} > m$. Let $D = \{m_{i_0} - \rho_j \mid j \in \{1, \ldots, i_0\}\}$. All the elements of D are bigger than m, that is, $D \subseteq (m, \infty)$. On the other hand, using Lemma 2, $D \subseteq \mathrm{D}(m_{i_0})$. Thus
$D \subseteq \mathrm{D}(m_{i_0}) \cap (m, \infty) \subsetneqq \{m_1, \ldots, m_{i_0}\}$. The containment is strict since $m_1 = m$. But this is absurd, since the two ends of the chain have the same cardinality.

(b) Note that $m_{i+1} - \rho_2$ is a divisor of m_{i+1}. This implies that, if $m_{i+1} - \rho_2 \geq m$, then $m_{i+1} - \rho_2 \in M$. As $m_{i+1} - \rho_2 < m_{i+1}$ and there is no element in M strictly between m_i and m_{i+1}, $m_{i+1} - \rho_2$ must be non greater than m_i. □

The following result is important for efficiency reasons.

Proposition 15

A subset $M = \{m = m_1, \ldots, m_r\}$ *of a numerical semigroup* S *is* (S, m, r)*-amenable if and only if*

$$\text{for all } i \in \{1, \ldots, r\} \text{ and } g \text{ minimal generator of } S, \quad \text{if } m_i - g \geq m, \text{ then } m_i - g \in \{m_1, \ldots, m_r\}. \tag{2}$$

Proof. Let $m_i \in M$ and $u \in \mathrm{D}(m_i) \cap [m, \infty)$, with $u \neq m_i$. We shall prove that if (2) holds, then $u \in M$, thus concluding that M is (S, m, r)-amenable. We can write $u = m_i - \gamma$. Assume as an hypothesis that $m_i - \alpha \in \mathrm{D}(m_i) \cap [m, \infty)$ implies $m_i - \alpha \in M$, for all α with factorization length lesser than the factorization length of γ. Let g be a minimal generator that divides γ. As $\gamma - g$ has smaller factorization length than γ, we have, by hypothesis, that $m_i - \gamma + g \in M$. But then, by (2), $m_i - \gamma = (m_i - \gamma + g) - g \in M$. □

Algorithm 2: (S, m, r)-amenable sets

Input : A numerical semigroup S, $m \geq 2c - 1$ and r an integer
Output: The set of (S, m, r)-amenable sets

$SM := [[m]]$`/* the set of amenable sets */`
Compute the generators $gens = \{n_1 < \cdots < n_e\}$ and the elements $\{0 = \rho_1 < \rho_2 < \cdots\}$ of S;

```
for i in [2..r] do
    newM := [];
    for x in SM do
        min := Minimum(x[Length(x)] + ρ2, m + ρi);
        for mj in [x[Length(x)] + 1..min] do
            divs := {d ∈ mj − gens | d > m} ;
            if divs ⊆ x then
                Append(newM, [Union(x, [mj])])
            ;
    SM := newM;
return SM;
```

Outline I

The ground

We got an algorithm to compute generalized Feng Rao numbers: compute the amenable sets and then the divisors of each of these sets. Not all the amenable sets are needed as will be shown.

We continue considering S a numerical semigroup minimally generated by $\{n_1 < \cdots < n_e\}$ with conductor c. Let $m \geq 2c - 1$.

The set $\{m, \ldots, m + n_e - 1\}$ is called the (S, m)-**ground**, or, simply, **ground**.

The intersection of an (S, m, r)-amenable set M with the (S, m)-ground is called the **shadow** of M.

Note that the shadow of an amenable set is amenable.

Lemma 16

Let S be a numerical semigroup minimally generated by $\{n_1 < \cdots < n_e\}$ with conductor c. Let $m \geq 2c-1$ and let $M = \{m = m_1 < \cdots < m_r\}$ be an amenable set. Let $L = M \cap [m, m+n_e)$ be the shadow of M. Then

$$\mathrm{D}(M) = (M \setminus L) \cup \mathrm{D}(L),$$

and furthermore

$$\sharp\mathrm{D}(M) = \sharp(M \setminus L) + \sharp\mathrm{D}(L).$$

Proof. The inclusion $(M \setminus L) \cup \mathrm{D}(L) \subseteq \mathrm{D}(M)$ is clear. For the other inclusion, let $x \in \mathrm{D}(M) \setminus (M \setminus L) = (\mathrm{D}(M) \setminus M) \cup L$. We want to prove that $x \in \mathrm{D}(L)$.
Since $L \subseteq \mathrm{D}(L)$, we may assume that $x \in \mathrm{D}(M) \setminus M$. Then $x \in \mathrm{D}(m_i)$ for some $i \in \{1, \ldots, r\}$ and $m_i \geq m + n_e$. As $m_i - x \in S \setminus \{0\}$, there exists $j \in \{1, \ldots, e\}$ such that $m_i - x - n_j \in S$. Hence $x \in \mathrm{D}(m_i - n_j)$.
By hypothesis M is amenable and thus $m_i - n_j \in M$, since $m_i - n_j \in \mathrm{D}(m_i) \cap [m, \infty)$. If needed, we can repeat the process until $m_i - n_j \in L$, that is, $x \in \mathrm{D}(L)$.
The second assertion follows easily since the above union is disjoint.

□

As an easy but useful consequence, we get the following:

Corollary 17

Let M and N be (m, r)-amenable sets with shadows L_M and L_N respectively. $L_M \subseteq L_N \implies \sharp\mathrm{D}(M) \leq \sharp\mathrm{D}(N)$.

Proof. Suppose that L_N is the disjoint union of L_M and a set K of cardinality k. Observe that $\sharp(M \setminus L_M) = \sharp(N \setminus L_N) + k$.
As $\mathrm{D}(L_N) = \mathrm{D}(L_M) \cup \mathrm{D}(K) \supseteq \mathrm{D}(L_M) \cup K$, it follows that $\sharp\mathrm{D}(L_N) \geq \sharp(L_M) + k$, that is, $\sharp\mathrm{D}(L_M) \leq \sharp(L_N) - k$.
$\sharp\mathrm{D}(M) = \sharp(M \setminus L_M) + \sharp\mathrm{D}(L_M) \leq \sharp(N \setminus L_N) + k + \sharp\mathrm{D}(L_N) - k = \sharp\mathrm{D}(N)$.
□

Corollary 18

Let S be a numerical semigroup minimally generated by $\{n_1 < \cdots < n_e\}$ with conductor c. Let $m \geq 2c - 1$ and let $M \subset [m, \infty)$ be an amenable set which is an optimal configuration of cardinality r. Let $L = M \cap [m, m + n_e)$ be the shadow of M. Then $\delta^r_{FR}(m) = \sharp\mathrm{D}(L) + \sharp(M \setminus L)$.

Corollary 19

In particular, if there exists an optimal configuration M of cardinality r such that $[m, m + n_e) \subseteq M$, then $[m, m + r - 1 + k] \cap \mathbb{N}$ is also an optimal configuration of cardinality $r + k$.

Proposition 20

Let S be a numerical semigroup minimally generated by $\{n_1 < \cdots < n_e\}$ with conductor c. Let $m \geq 2c - 1$ and let $M \subset [m, \infty)$ be a finite amenable set. Choose $s \geq n_e$. Let $L = M \cap [m, m+s)$, $\ell = \sharp L$, and $k = \sharp(M \setminus L)$. If $\delta_{FR}^{\ell}(m) = \sharp \mathrm{D}(L)$, then $\delta_{FR}^{\ell+k}(m) = \delta_{FR}^{\ell}(m) + k$.

Proof. By Lemma 16, we know that $\sharp \mathrm{D}(M) = \sharp(M \setminus L) + \sharp \mathrm{D}(L)$. Hence $\delta_{FR}^{\ell}(m) + k = \sharp \mathrm{D}(L) + \sharp(M \setminus L) = \sharp \mathrm{D}(M) \geq \delta_{FR}^{\ell+k}(m)$. Now assume that $\delta_{FR}^{\ell+k}(m) = \sharp D(m_1 < \cdots < m_{\ell+k})$ for some $m_1, \ldots, m_{\ell+k} \in S$. Since $\sharp D(m_1 < \cdots < m_{\ell+k}) \geq \sharp D(m_1, \ldots, m_\ell) + \sharp\{m_{\ell+1}, \ldots, m_{\ell+k}\} \geq \delta_{FR}^{\ell}(m) + k$, we conclude that $\delta_{FR}^{\ell+k}(m) = \delta_{FR}^{\ell}(m) + k$. □

In the cases where computing divisors is “easy”, finding optimal configurations is as difficult as computing generalized Feng Rao numbers. Computing generalized Feng Rao numbers is referred to as difficult in the literature...
We got an algorithm to compute generalized Feng Rao numbers.
Note that its efficiency depends on the number of amenable sets.
Due to Corollary 17, our algorithm can be sharpened, since we only need to consider one amenable set for each possible shadow.

Algorithm 3: Generalised Feng Rao numbers

Input : A numerical semigroup S, $m \in S$, $r \in \mathbb{N}$
Output: $\delta^r_{FR}(m)$

$SM := \emptyset$;
1 $AM := \{M \subset S \mid M$ is a (S, m, r)-amenable set$\}$;
`/* Compute the (m,r)-amenable sets, by making a call to Algorithm 5 */`
2 For each possible shadow s, add to SM an element of AM with shadow s, if it exists;
$\nu := m + r$; `/* an obvious upper bound */`
3 **for** M *in* SM **do**
  $D := \bigcup\{Divisors(x) \mid x \in M\}$ `/* Compute the divisors of M, by using Algorithm 1 */`
  $\nu := minimum(\sharp D, \nu)$
4 **return** ν

Outline I

This algorithm (even preliminary versions of it) has been extensively used to perform computations which gave the intuition that ultimately led to discovering a formula for the generalised Feng Rao numbers of numerical semigroups generated by intervals.

Finally, if we enumerate the elements of S in increasing order

$$S = \{\rho_1 = 0 < \rho_2 < \cdots\},$$

we note that every $x \geq c$ is the $(x+1-g)$-th element of S, that is $x = \rho_{x+1-g}$.

The last part of this paper will be devoted to semigroups generated by intervals.

Let a be a positive integer and b an integer with $0 < b < a$. Let $S = \langle a, a+1, \ldots, a+b \rangle$. Then S is a numerical semigroup with multiplicity a and embedding dimension $b+1$. As usual, let c denote the conductor of S and $m \geq 2c-1$. Membership problem for these semigroups is trivial as the following known result (and with many different formulations) shows.

Semigroups generated by intervals
pictures

Lemma 21

[?, Lemma 10, for $d = 1$] Let k and r be integers such that $0 \leq r \leq a - 1$. Then $ka + r \in S$ if and only if $r \leq kb$.

Suppose S is minimally generated by $\{n_1 < \cdots < n_e\}$. Note that if S is minimally generated by an interval $[a, a+b]$, then n_1 is a and $n_e - n_1$ is b.

Semigroups generated by intervals
pictures

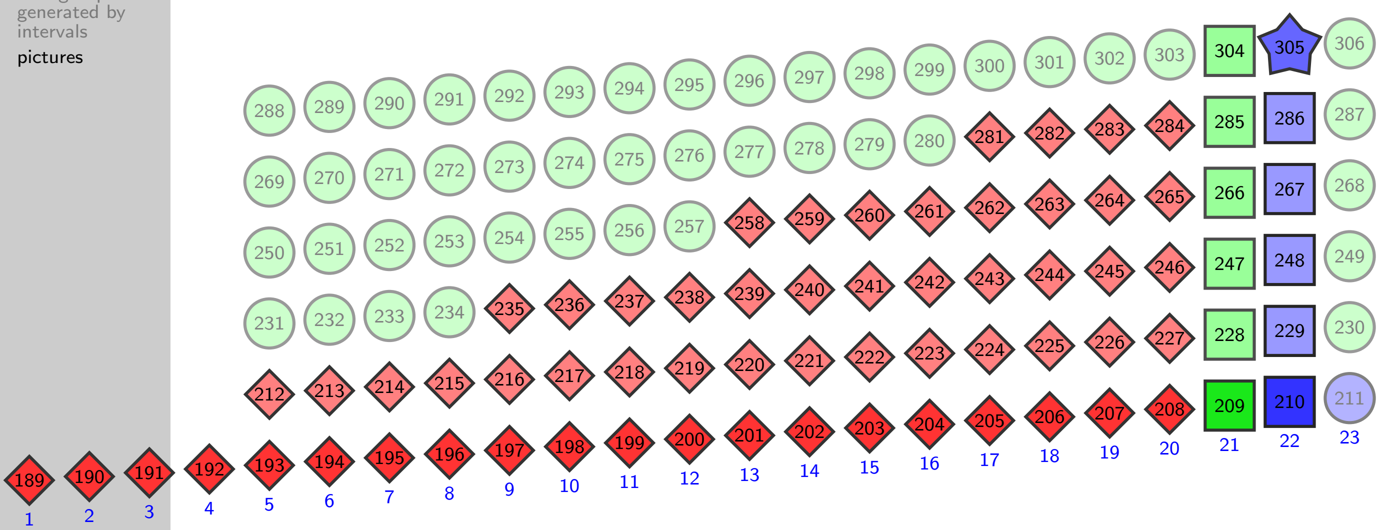


Figure: the biggest ordered amenable

Semigroups generated by intervals

pictures

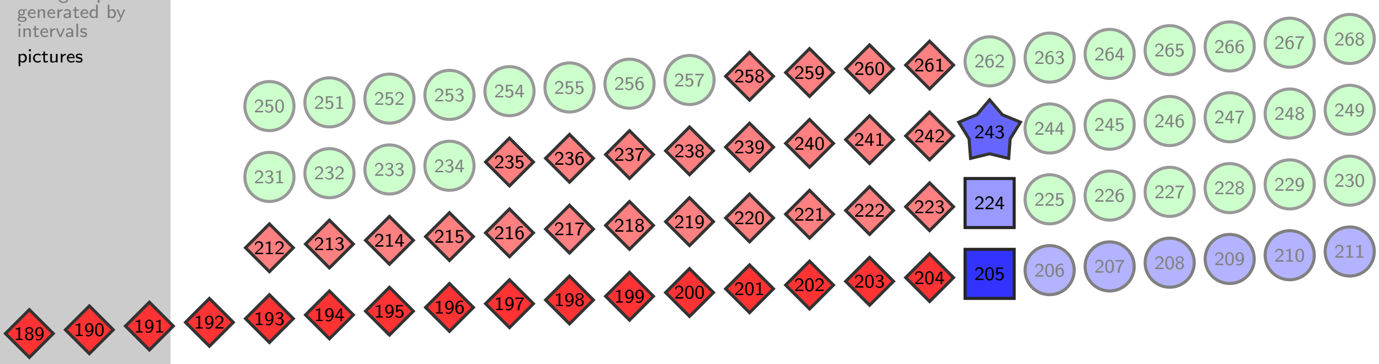


Figure: A set comming from line **??**

Semigroups generated by intervals

pictures

Figure: A set comming from line **??**

Semigroups generated by intervals
pictures

Figure: A set comming from line ??

Motivation Divisors Feng Rao Algorithm Application

Semigroups generated by intervals
pictures

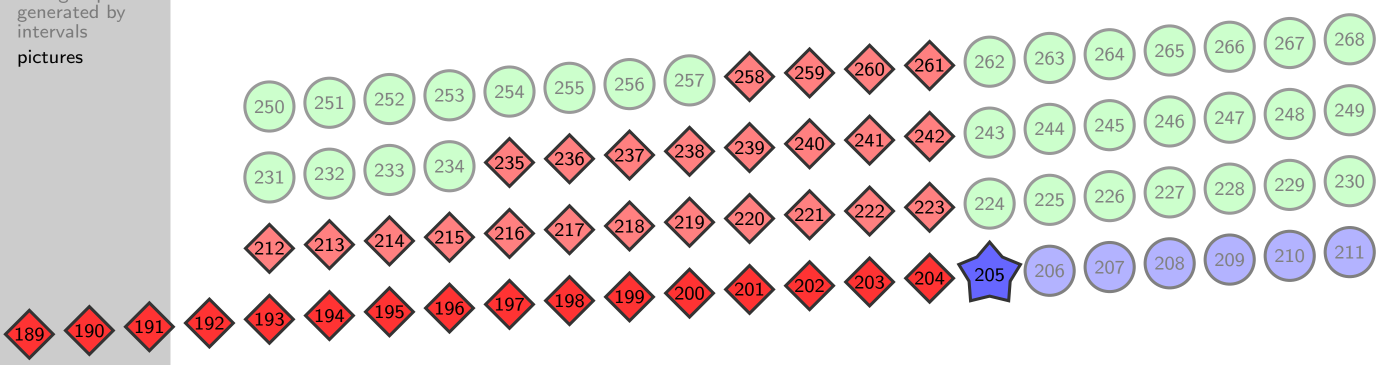


Figure: A set comming from line ??

References

The GAP Group.
GAP – Groups, Algorithms, and Programming, Version 4.4, 2004.
http://www.gap-system.org

M. Delgado, P. A. García-Sánchez and J. Morais,
"numericalsgps": a GAP package on numerical semigroups.
http://www.gap-system.org/Packages/numericalsgps.html

J.C. Rosales and P. A. García-Sánchez,
"Numerical Semigroups",
Springer. 2009.

J. I. Farrán, P. A. García-Sánchez and D. Llena,
On the Feng-Rao numbers,
Seventh Conference on Discrete Mathematics and Computer Science,
Castro Urdiales, 2010

J. I. Farrán and C. Munuera,
Goppa-like bounds for the generalized Feng-Rao distances,
Discrete Applied Mathematics **128**/1, pp. 145-156 (2003).

M. Delgado, J. I. Farrán, P. A. García-Sánchez and D. Llena,
On the generalized Feng-Rao numbers of numerical semigroups generated by intervals,
Work in progress