On the Feng-Rao numbers*

J.I. Farrán¹, P.A. García-Sánchez², and D. Llena³

¹ Universidad de Valladolid ignfar@eis.uva.es
² Universidad de Granada pedro@ugr.es
³ Universidad de Almería dlena@ual.es

Abstract. Some computations concerning the so-called Feng-Rao numbers are presented. Such numbers, for some numerical semigroup $S$ and positive integer $r$ fixed, describe the different asymptotical behaviour of the generalized Feng-Rao distances in $S$ with respect to the classical Feng-Rao distance, whose asymptotical behaviour is essentially related to the Goppa distance. These concepts naturally arise from the theory of Algebraic Geometry codes for the case of Weierstrass semigroups, but here they are studied in general for any given numerical semigroup. The main results of this paper are addressed to the computation of the Feng-Rao numbers for simple semigroups, such as those with multiplicity two and those generated by $\{a, a + 1\}$ with $a$ a positive integer.

Key words: Numerical semigroups, generalized Feng-Rao distances, Feng-Rao numbers, Algebraic Geometry codes, weight hierarchy.

1 Introduction

The theory of error-correcting codes was drastically improved by the introduction of the so-called Algebraic Geometry codes (AG codes, in short). These codes, obtained by evaluation of suitable rational functions at rational points of algebraic curves, have an excellent asymptotical behaviour, namely their asymptotical parameters go beyond the Gilbert-Varshamov bound (see [11]).

Later on, Feng and Rao introduced in [6] a very efficient decoding method for the so-called one-point AG codes. Such a code is defined as the dual of an evaluation code given by a linear map

\[ ev_D : \mathcal{L}(mP) \to \mathbb{F}_q^n \]
\[ f \mapsto (f(P_1), \ldots, f(P_n)), \]

where $P, P_1, \ldots, P_n$ are $n + 1$ distinct rational points of a certain algebraic curve $\chi$ defined over the finite field $\mathbb{F}_q$, $m$ is a positive integer, and $D = P_1 + \ldots + P_n$ and $mP$ are rational divisors on $\chi$ (see [11] for more details).

* This work has been supported by the projects MTM2007-62346, MTM2007-64704 and FQM-343
The method of Feng and Rao decodes up to half the so-called Feng-Rao distance, defined for the Weierstrass semigroup of \( \chi \) at \( P \). In particular, this number is a lower bound for the minimum distance \( d \) of the corresponding code. This bound actually improves the Goppa estimate \( d^* = m + 2 - 2g \), obtained from the Riemann-Roch theorem, \( g \) being the genus of the curve. More precisely, for the one-point AG code \( C = C_{\Omega}(D, mP) \) we have

\[
d \equiv d(C) \geq \delta_{FR}(m + 1) \geq m + 2 - 2g
\]

if \( m > 2g - 2 \), and the equality \( \delta_{FR}(m + 1) = m + 2 - 2g \) holds for \( m \gg 0 \).

Even though the Feng-Rao distance was introduced for Weierstrass semigroups and for decoding purposes, it is just a combinatorial concept that makes sense for arbitrary numerical semigroups. This problem has been broadly studied in the literature for different types of semigroups (see [2], [3] or [13]).

On the other hand, the concept of minimum distance for an error-correcting code has been generalized to the so-called generalized Hamming weights. They were introduced independently by Helleseth et al. in [9] and Wei in [16] for applications in coding theory and cryptography respectively. Afterwards, this weight hierarchy has also been useful in other coding applications, like trellis coding (see [12]), truncation and extension of linear codes (see [10] and [15]), or the Forney’s Dimension/Length profiles (see [7]).

The natural generalization of the Feng-Rao distance (called order bound in some papers) to higher weights was introduced in [8]. The computation of these generalized Feng-Rao distances turns out to be a very hard problem. Actually, very few results are known about this subject, and they are completely scattered in the literature (see for example [1], [8] or [5]).

This paper studies the asymptotical behaviour of the generalized Feng-Rao distances, that is, \( \delta_{FR}(m) \) for \( r \geq 2 \) and \( m \gg 0 \). In fact, it was proven in [5] that

\[
\delta_{FR}(m) = m + 1 - 2g + E_r
\]  

for \( m \gg 0 \) (details in the next section). The number \( E_r \equiv E(S, r) \) is called the \( r \)-th Feng-Rao number of the semigroup \( S \), and they are unknown but for very few semigroups and concrete \( r \)'s. Thus, the main purpose of this paper is precisely compute \( E(S, r) \) for concrete semigroups and as many \( r \)'s as possible.

### 2 Divisors and the generalized Feng-Rao distances

Let \( S \) be a numerical semigroup, that is, a submonoid of \( \mathbb{N} \) such that \( \sharp(\mathbb{N}\setminus\mathbb{N}) < \infty \) and \( 0 \in S \). Denote respectively by \( g := \sharp(\mathbb{N}\setminus\mathbb{N}) \) and \( c \in S \) the genus and the conductor of \( S \), being \( c \) by definition the (unique) element in \( S \) such that \( c - 1 \notin S \) and \( c + l \in S \) for all \( l \in \mathbb{N} \). Note that if \( S \) the the Weierstrass
semigroup of a curve $\chi$ at a point $P$, $g$ equals to the geometric genus of $\chi$, and the elements of $G(S) := \mathbb{N} \setminus S$ are called the Weierstrass gaps at $P$.

We obviously have $c \leq 2g$, and thus the “largest gap” of $S$ is $l_g = c - 1 \leq 2g - 1$, where $k \in \mathbb{N}$ is called a gap of $S$ if $k \notin S$. The number $l_g$ is precisely the Frobenius number of $S$, denoted by $F(S)$ in the literature. The multiplicity of a numerical semigroup is the least positive integer belonging to it.

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

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

where finitely many $\lambda_g \in \mathbb{N}$ are non-zero. In fact, it is classically known that every numerical semigroup is finitely generated, that is, we can find a finite set $G$ generating $S$. Furthermore, every generator set contains the set of irreducible elements, $m \in S$ being irreducible if $m = a + b$ and $a, b \in S$ implies $a \cdot b = 0$, and this set actually generates $S$, so that it is usually called “the” generator set of $S$, whose cardinality is called embedding dimension of $S$ (more details in [14]).

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

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

we note that every $m \geq c$ is the $(m + 1 - g)$-th element of $S$, that is $m = \rho_{m+1-g}$. We now introduce the definitions of the generalized Feng-Rao distances and summarize the known results about them.

**Definition 1.** Let $S$ be a numerical semigroup. For $m_1 \in S$, let $D(m_1) := \{p \in S \mid m_1 - p \in S\}$ and let $\nu(m_1) := |D(m_1)|$. The (classical) Feng-Rao distance of $S$ is defined by the function

$$\delta_{FR} : S \to \mathbb{N}$$

$$m \mapsto \delta_{FR}(m) := \min\{\nu(m_1) \mid m_1 \geq m, \ m_1 \in S\}.$$

Note that $D(m_1) \subseteq [0, m_1]$ and $s \in D(m_1)$ implies $D(s) \subseteq D(m_1)$.

There are some well-known facts about the functions $\nu$ and $\delta_{FR}$ for an arbitrary semigroup $S$ (see [11], [13] or [2] for further details). The most important one for our purposes is that $\delta_{FR}(m) \geq m + 1 - 2g$ for all $m \in S$ with $m \geq c$, and that equality holds if moreover $m \geq 2c - 1$.

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

**Definition 2.** Let $S$ be a numerical semigroup. For $m_1, \ldots, m_r \in S$, let

$$m = \sum_{g \in G} \lambda_g g,$$
$\text{D}(m_1,\ldots,m_r) = \text{D}(m_1) \cup \cdots \cup \text{D}(m_r) = \{ p \in S \mid m_i - p \in S, \exists i \in \{1,\ldots,r\}\}$

and $\nu(m_1,\ldots,m_r) := \sharp \text{D}(m_1,\ldots,m_r)$. For any integer $r \geq 1$, the $r$-th Feng-Rao distance of $S$ is defined by the function

$$\delta_{FR}^r : S \to \mathbb{N}$$

$$m \mapsto \delta_{FR}^r(m) := \min \{ \nu(m_1,\ldots,m_r) \mid m \leq m_1 < \cdots < m_r, m_i \in S \}.$$

Very few results are known for the numbers $\delta_{FR}^r$, and their computation is very hard from both a theoretical and computational point of view. The main result we need describes the asymptotical behaviour for $m >> 0$, and was proven in [5]. This result tells us that there exists a certain constant $E_r = E(S,r)$, depending on $r$ and $S$, such that

$$\delta_{FR}^r(m) = m + 1 - 2g + E_r$$

for $m \geq 2c - 1$. This constant is called the $r$-th Feng-Rao number of the semigroup $S$. Furthermore, it is also true that $\delta_{FR}^r(m) \geq m + 1 - 2g + E(S,r)$ for $m \geq c$ (see [5]). Somehow, this Feng-Rao number measures the difference between $\delta_{FR}^r(m)$ and $\delta_{FR}(m)$ for large enough $m$, being $E(S,1) = 0$. For the trivial semigroup with $g = 0$, it is easy to check that $E(S,r) = r - 1$.

**Remark 1.** We summarize the general properties of the Feng-Rao numbers, for a fixed $S$, $g \geq 1$ and $r \geq 2$ (see again [5] for the details):

1. The function $E(S,r)$ is non-decreasing in $r$.
2. $r \leq E(S,r) \leq \rho_r$. If furthermore $r \geq c$, then $E(S,r) = \rho_r = r + g - 1$.
3. The inclusion $\text{D}(m) \subseteq \text{D}(m + p)$, for all $p \in S$, is very useful for practical computations.

The computation of the Feng-Rao numbers is a very hard task, even in very simple examples. Only the second Feng-Rao number ($r = 2$) is computed in the literature, with either a general algorithm based on Apéry systems, or concrete formulas for simple examples by counting deserts (see [5]). More precisely, the only known formulas are

$$E(S,2) = \rho_2$$

for $S$ generated by two elements.

The purpose of this paper is to find examples for which the upper bound $E(S,r) = \rho_r$ is reached. So far, and by using different techniques, we have found two families of numerical semigroups with this property: that of numerical semigroups with multiplicity two (hyper-elliptic), and those embedding dimension two numerical semigroups generated by a positive integer $a$ and $a + 1$ (hermitian-like).

Note that in general this bound is not attained for other kinds of semigroups, not even for $r = 2$. For example, if we consider the semigroup $S = \langle 6,13,14,15,16,17 \rangle$ then $E(S,2) = 3 < \rho_2 = 6$. 

Remark 2. Following [14], for \( a, b \in S \) given, we say that \( a \) divides \( b \), and write \( a \leq_s b \), if \( b - a \in S \). The set \( D(a) \) denotes the set of divisors of \( a \) in \( S \), and for given \( m_1, \ldots, m_r \in S \), we write \( D(m_1, \ldots, m_r) = \bigcup_{i=1}^{r} D(m_i) \). Thus, from now on, we will use the term divisors to refer to the elements in the sets \( D(\cdot) \).

Since our purpose is to compute the Feng-Rao numbers and they measure the difference between the Feng-Rao distance and the Goppa distance, we will now prove some general results about how to compute \( \delta'(m) \) for \( m > 0 \). This result is useful from both the theoretical and computational point of view (it enabled us to implement the Feng-Rao distance by using the numericalsgps GAP package, [4]).

**Proposition 1.** Let \( S = \{0 = \rho_1 < \rho_2 < \cdots \} \) be a numerical semigroup with conductor \( c \). Let \( m, m_1, \ldots, m_r \) be integers such that \( 2c - 1 \leq m \leq m_1 < \cdots < m_r \). Assume that \( \delta'(m) = \sharp D(m_1, \ldots, m_r) \). Then we can choose \( m_1, \ldots, m_r \) such that

1. \( m_i \leq m + \rho_i \) for all \( i \in \{1, \ldots, r\} \),
2. \( m_{i+1} - m_i \leq \rho_2 \),
3. for all \( i \in \{1, \ldots, r\} \), \( D(m_i) \cap [m_1, \infty) \subseteq \{m_1, \ldots, m_r\} \).

**Proof.** For \( i = 1 \), we must prove that \( m_1 = m \). Note that as \( m \geq 2c - 1 \), \( \delta'(m) \) is strictly increasing in \( m \), and thus \( m \) cannot be less than \( m_1 \). For \( i \) greater than one, if \( m_i > m + \rho_i \), then for every \( j \in \{2, \ldots, i\} \) set \( A_j = \{m_1, \ldots, m_{i-1}, m_i - \rho_j, m_{i+1}, \ldots, m_r\} \). The integer \( m_i - \rho_j \) is smaller than \( m_i \), and by the pigeonhole principle, there is \( j \in \{2, \ldots, i\} \) such that \( m_i - \rho_j \not\in \{m_2, \ldots, m_{i-1}\} \). Thus \( \sharp A_j = r \), and clearly

\[
D(m_1, \ldots, m_{i-1}, m_i - \rho_j, m_{i+1}, \ldots, m_r) \subseteq D(m_1, \ldots, m_r).
\]

Now assume that there exists \( i \) such that \( m_{i+1} - m_i > \rho_2 \). Then \( m_1 < \cdots < m_i < m_{i+1} - \rho_2 < \cdots < m_t - \rho_2 \), and \( D(m_1, \ldots, m_i, m_{i+1} - \rho_2, \ldots, m_t - \rho_2) \subseteq D(m_1, \ldots, m_r) \).

Finally, assume that for some \( i \in \{1, \ldots, r\} \) there exists \( m > m_1 \) such that \( m_i - m \in S \) and \( m \not\in \{m_1, \ldots, m_r\} \). Clearly \( D(m) \subseteq D(m_i) \), and thus \( D(m_1, \ldots, m_{i-1}, m, m_{i+1}, \ldots, m_r) \subseteq D(m_1, \ldots, m_r) \). In other words, we can change \( m_i \) by \( m \) and the number of divisors does not increase. \( \square \)

For a numerical semigroup \( S \) and \( \{m_1 < \cdots < m_r\} \subseteq S \), \( D(m_1, \ldots, m_r) = (S \cap [0, m_r]) \setminus N(m_1, \ldots, m_r) \), with

\[
N(m_1, \ldots, m_r) = \{s \in S \mid s < m_r, m_i - s \not\in S, \text{ for all } i \in \{1, \ldots, r\}\}.
\]

Thus for \( m_r \) greater than or equal to \( c \),

\[
\sharp D(m_1, \ldots, m_r) = m_r + 1 - g - \sharp N(m_1, \ldots, m_r).
\]

(2)
The following result shows that if the bound $E(S, r) = \rho_r$ is reached, and $\rho_{r+1} = \rho_r + 1$, then $E(r + 1, S) = \rho_{r+1}$. This will simplify the proofs of the main two results in this manuscript.

**Proposition 2.** Under the same hypotheses as in Proposition 1, let $S$ be a numerical semigroup and $r \geq 1$ an integer. Assume that $E(S, r) = \rho_r$ and $\rho_{r+1} = \rho_r + 1$. Then

$$E(r + 1, S) = \rho_{r+1}.$$  

**Proof.** From all the above assumptions and definitions we have

$$\sharp D(m_1, \ldots, m_r) \geq m + 1 - 2g + \rho_r.$$  

On the other hand, it is obvious that $\sharp D(m_1 < \cdots < m_r < m_{r+1}) \geq \sharp D(m_1, \ldots, m_r) + 1$, for $m_{r+1} \in D(m_1, \ldots, m_r, m_{r+1}) \setminus D(m_1, \ldots, m_r)$. Combining both facts we have

$$\sharp D(m_1, \ldots, m_r, m_{r+1}) \geq m + 1 - 2g + \rho_r + 1 = m + 1 - 2g + \rho_{r+1},$$

and thus taking the minimum

$$\delta^{r+1}(m) = m + 1 - 2g + E(r + 1, S) \geq m + 1 - 2g + \rho_{r+1}.$$  

Hence, since always $E(r + 1, S) \leq \rho_{r+1}$ we obtain the equality.  

\[\Box\]

### 3 Symmetric numerical semigroups

In order to compute the Feng-Rao number $E(S, r)$, it suffices to consider $m_1 = m = 2c - 1$ (see Proposition 1). If moreover $S$ is symmetric, we can precise the previous computations in the following way.

**Proposition 3.** Let $S$ be a symmetric numerical semigroup with conductor $c$. Let $m = 2c - 1$, and let $m_1, \ldots, m_r$ be integers with $m = m_1 < \cdots < m_r$. Define, for $i \in \{1, \ldots, r\}$ and $d_i = m_r - m_{r+1-i}$. Then there is a one-to-one correspondence between $N(m_1, \ldots, m_r)$ and the set

$$\tilde{N}(d_1, \ldots, d_r) = \{ s \in S \mid s < c, s + d_i \in S \text{ for all } i \in \{1, \ldots, r\} \}.$$  

**Proof.** Note that for $s \in S$, with $s < c$, $m_i - s > m_i - c \geq 2c - 1 - c = c - 1$. Hence $m_i - s \in S$, which means that $N(m_1, \ldots, m_r) \cap [0, c)$ is empty. Thus $N(m_1, \ldots, m_r) = \{ s \in [c, m_r] \mid m_i - s \not\in S \text{ for all } i \in \{1, \ldots, r\} \}$.

For every $i \in \{1, \ldots, r\}$, set $k_i = m_i - m$. The condition $m_i - s \not\in S$ is equivalent to $c - 1 - (m_i - s) \in S$, since $S$ is symmetric. As $m_i = 2c - 1 + k_i$, $m_i - s = 2c - 1 + k_i - s$. Thus, $m_i - s \not\in S$ if and only if $s - k_i \in c + S$. Hence $N(m_1, \ldots, m_r) = \{ s \in [c, m_r] \mid s - k_i \in c + S, \text{ for all } i \in \{1, \ldots, r\} \}$. It is easy to check that the map
\[ N(m_1, \ldots, m_r) = \{ s \in k_r + S \mid s \leq c - 1 + k_r, s - k_i \in S, \forall i \in \{1, \ldots, r\} \} \]
given by \( x \mapsto x - c \) is a bijection.

Finally the set \( \{ s \in k_r + S \mid s \leq c - 1 + k_r, s - k_i \in S, \forall i \in \{1, \ldots, r\} \} \) has the same cardinality as the set \( \{ s \in S \mid s < c, s + k_r - k_i \in S, \forall i \in \{1, \ldots, r\} \} \).
The proof now follows from the definition of the \( d_i \)s.

**Corollary 1.** Under the standing hypothesis, let \( g \) be the genus of \( S \).

1. \( \sharp \mathbb{N}(d_1, \ldots, d_r) \leq g, \)
2. \( \sharp \mathbb{N}(\rho_1, \ldots, \rho_r) = g. \)

**Proof.** The first assertion follows from the symmetry of \( S \), since in this setting, the set \( S \cap [0, c) \) has \( g \) elements. Observe also that for all \( s \in S \cap [0, c) \), \( s + \rho_i \in S \) for all \( i \). Hence the set \( \mathbb{N}(\rho_1, \ldots, \rho_r) = S \cap [0, c) \). □

**Corollary 2.** If \( 2c - 1 = m = m_1 < \cdots < m_r \) are such that \( D(m_1, \ldots, m_r) = \delta^*(m) \), and \( m_r = m + \rho_r \), then

\[ E(S, r) = \rho_r. \]

**Proof.** Set \( d_i = m_r - m_{r+1-i} \) as above. From (2) and Proposition 3, \( \delta^*(m) = m + \rho_r + 1 - g - \sharp \mathbb{N}(d_1, \ldots, d_r) \), and in view of (1), \( \delta^*(m) = m + 1 - 2g + E(S, r) \).

Corollary 1 asserts that \( \sharp \mathbb{N}(d_1, \ldots, d_r) \) is at most \( g \) and this bound is reached. Thus the minimality of \( \delta^*(m) \) forces \( \sharp \mathbb{N}(d_1, \ldots, d_r) \) to be \( g \). This leads to \( E(S, r) = \rho_r. \) □

As an application of the previous results we can compute \( E(S, r) \) for \( S \) an hyper-elliptic semigroup.

**Theorem 1.** Let \( g \) be a positive integer, and let \( \langle 2, 2g + 1 \rangle = \{ 0 = \rho_1 < \rho_2 < \cdots \} \). For every \( r \geq 1 \),

\[ E(r, \langle 2, 2g + 1 \rangle) = \rho_r. \]

**Proof.** Let \( S = \langle 2, 2g + 1 \rangle \). Clearly, its conductor is \( c = 2g \) and its genus is \( g \).

In view of Proposition 2, we only have to prove the result for \( \rho_r \leq c \).

Let \( 2c - 1 = m = m_1 < \cdots < m_r \), and define \( d_i = m_r - m_{r+1-i} \) for \( i \in \{1, \ldots, r\} \). In view of Proposition 1, in order to compute \( \delta^*(m) \), we can choose \( m_{i+1} - m_i \leq 2 \) (thus \( 1 \leq d_{j+1} - d_j \leq 2 \)), and \( d_r \leq \rho_r \leq c \).

Observe that \( \sharp \mathbb{N}(d_1, \ldots, d_r) = g \) if all the \( d_i \)'s are in \( S \). If this is the case, the minimum possible value for \( \sharp \mathbb{D}(m_1, \ldots, m_r) \) is achieved in \( d_i = \rho_i \), according to (2) and Proposition 3. In this setting \( \sharp \mathbb{D}(m_1, \ldots, m_r) = m + 1 - 2g + \rho_r \).

Thus, in view of the Corollary 2, if we prove that for \( m_r < m + \rho_r \), \( \sharp \mathbb{D}(m_1, \ldots, m_r) \geq m + 1 - 2g + \rho_r \), then \( E(S, r) = \rho_r \).

Notice that if \( d_i \) does not belong to \( S \), for some \( i \), then some elements in \( S \) go out of the set \( \hat{N}(d_1, \ldots, d_r) \). More precisely, if \( d_i = c - 2k + 1 \) is the smallest of those odd numbers, then
\[ \tilde{N}(d_1, \ldots, d_r) \leq g - k, \] (3)

because 0, 2, \ldots, 2(k-1) \in S \setminus \tilde{N}(d_1, \ldots, d_r).

The condition \( m_r < m + \rho_r \) is equivalent to \( d_r < \rho_r \). If \( k = 2l \), we have to place \( d_1, \ldots, d_r \) in \( d_r + 1 \) positions from 0 to \( d_r = 2(r-l-1) \), where only \( r - l \) are even numbers, and thus at least \( l \) of the \( d_i \)'s are gaps (provided \( l \leq r-l-1 \), otherwise the configuration of \( d_i \)'s is not valid). Then the smallest gap \( d_{i_0} \) in this set is at most \( d_r - 2l + 1 \), but on the other hand there are \( l \) gaps between \( d_r \) and \( \rho_r \), and hence \( d_{i_0} \leq (\rho_r - 2l) - 2l + 1 = \rho_r - 2k + 1 \leq c - 2k + 1 \). In view of (3) and Proposition 3,

\[
\sharp D(m_1, \ldots, m_r) = m_r + 1 - g - \sharp \tilde{N}(d_1, \ldots, d_r) = \\
= m + \rho_r - k + 1 - g - \sharp \tilde{N}(d_1, \ldots, d_r) \geq m + 1 - 2g + \rho_r.
\]

If \( k = 2l - 1 \) the computations are similar. \( \Box \)

**Example 1.** For a symmetric numerical semigroup \( S \), nor \( E(2, S) \) needs to be \( \rho_2 \), nor \( E(3, S) \) is necessarily \( \rho_3 \), and so on. For example, \( E(2, \langle 6, 8, 10, 15, 17 \rangle) = 4 < 6 \), and \( E(3, \langle 4, 9, 10 \rangle) = 7 < 8 \). These computations can be performed by using the `numericalsgps` GAP package [4].

### 4 Hermitian-like numerical semigroups

In this section, we consider the Hermitian-like semigroup \( S = \langle a, a+1 \rangle \), which is symmetric, and thus the conductor is \( c = a(a-1) = 2g \). We study these semigroups in a new section because the techniques used are different from those presented for symmetric numerical semigroups.

We start by showing how many new divisors adds \( m + \lambda \) to those of \( m \).

**Proposition 4.** Let \( m \) be an integer greater than \( 2c - 1 \), and \( \lambda \) be a positive integer. Assume that \( \lambda = ka + r \), with \( k \) and \( r \) integers such that \( 0 \leq r < a \). Then

\[
D(m, m + \lambda) = D(m) \cup \\
\cup \{ m + \lambda - (ax + (a+1)y) \mid 0 \leq x < k + a + 1 - r, 0 \leq y < r \} \cup \\
\cup \{ m + \lambda - (ax + (a+1)y) \mid 0 \leq x < k - r, r \leq y < a \},
\]

and

\[
\#D(m, m + \lambda) = \#D(m) + \begin{cases} 
\lambda & \text{if } \lambda \in S, \\
r(k + a + 1 - r) & \text{otherwise}.
\end{cases}
\]

**Proof.** Take \( t \in \mathbb{N} \) such that \( m + \lambda - t \in S \) and \( m - t \not\in S \) (notice that this implies that \( m - t < c \), and consequently \( t > m - c \geq c - 1 \), which leads to \( t \in S \)). Then there exist unique \( x, y \in \mathbb{N} \), \( 0 \leq y \leq a - 1 \) such that \( m + \lambda - t = xa + y(a+1) \). Hence \( m - t = xa + y(a+1) - \lambda = (x-k+r)a + (y-r)(a+1) \). As
Finally observe that $(k + a + 1 - r)r + (k - r)(a - r) = ak + r = \lambda$, and that if $k = r$, then $r(k + a + 1 - r) = ra + r = \lambda$. Notice also that $ka + r \in \mathcal{S}$ if and only if $0 \leq r \leq k$. \hfill \Box

One can easily generalize Proposition 4 in the following way.

**Proposition 5.** For $2c - 1 \leq m_1 < m_2 < \cdots < m_{k+1}$ set $\lambda_i = m_{k+1} - m_i$, and $A_i = \{m_{k+1} - (ax + (a+1)y) \mid 0 \leq x < k_i + a + 1 - r_i, 0 \leq y < r_i\} \cup \{m_{k+1} - (ax + (a+1)y) \mid 0 \leq x < k_i - r_i, r_i \leq y < a\}$, with $k_i$ and $r_i$ integers such that $\lambda_i = k_i a + r_i$ and $0 \leq r_i < a$. Then

$$D(m_1, \ldots, m_k, m_{k+1}) = D(m_1, \ldots, m_k) \cup \bigcap_{i=1}^{k} A_i.$$

**Proof.** From the proof of Proposition 4, we see that $A_i$ represents $D(m_{k+1}) \setminus D(m_i)$. Thus the intersection of all $A_i$ is precisely $D(m_{k+1}) \setminus D(m_1, \ldots, m_k)$.

In the particular case all the $m_i$’s belong to $[m, m + a]$, we can even get a more precise description of the cardinality of their set of divisors. This case will show to be relevant later, since the number of divisors of $\{m_1, \ldots, m_r\}$ seems to be ruled by the divisors lying in $[m, m + a]$.

**Corollary 3.** For $1 \leq i_1 < \cdots < i_k \leq a$ and $m \geq 2c - 1$,

$$\#D(m, m + i_1, \ldots, m + i_k) = \#D(m) + \sum_{j=1}^{k} (i_j - i_{j-1})(a+1-i_j),$$

taking $i_0 = 0$.

**Proof.** First observe that $\#D(m, m + i_1) = \#D(m) + i_1(a+1-i_1)$, since in this case $k = 0$ in Proposition 4. In view of Proposition 5, $D(m, m + i_1, m + i_2) = D(m, m + i_1) \cup (A_1 \cap A_2)$ with $\lambda_1 = i_2$, $\lambda_2 = (i_2 - i_1)$. Thus $k_2 = 0$ and $r_2 = i_2 - i_1$, while $k_1 = 0$ and $r_1 = i_2$, if $i_2 < a$, and $k_1 = 1$ and $r_1 = 0$, otherwise. In the first setting $A_1 \cap A_2 = \{m + i_2 - (ax + (a+1)y) \mid 0 \leq x < a + 1 - i_2, 0 \leq y < i_2 - i_1\}$, and for $i_2 = a$, $A_1 \cap A_2 = \{m + i_2 - (a+1)y \mid 0 \leq y < i_2 - i_1\}$. Hence $\#D(m, m + i_1, m + i_2) = \#D(m, m + i_1) + (i_2 - i_1)(a+1-i_2) = \#D(m) + i_1(a+1-i_1) + (i_2 - i_1)(a+1-i_2)$. An easy induction concludes the proof, just taking into account that in this setting $\bigcap_{i=1}^{k} A_i = A_1 \cap A_k$. \hfill \Box

One can actually push the elements in $[m, m + a]$ to the ends of the interval and get less divisors in this way. This is described in the next result.
Lemma 1. For \(1 \leq i_1 < \cdots < i_k \leq a, m \geq 2c - 1\),
\[
\#D(m, m + i_1, \ldots, m + i_k) \geq \#D(m) + \frac{1}{2}k(2a + 1 - k).
\]

Proof. Let \(j \in \{1, \ldots, k - 1\}\), and set \(i_0 = 0\),
\[
\#D(m+i_0, \ldots, m+i_k) \geq \#D(m, \ldots, m+i_j-1, m+i_{j+1}, \ldots, m+i_k),
\]
\[
\#D(m+i_0, \ldots, m+i_k) \geq \#D(m, \ldots, m+i_j-1, m+i_{j+1}, \ldots, m+i_k),
\]
\[
\#D(m, m + i_1, \ldots, m + i_k) \geq \#D(m, m + i_1, \ldots, m + i_{k-1}, m + a).
\]

Define \(f(i_j) = \#D(m, m + i_1, \ldots, m + i_k)\). From Corollary 3, we deduce that
\[
f(i_j) - f(i_{j-1} + 1) = -(i_j - (i_{j-1} + 1))(i_j - (i_{j+1} - 1)) = f(i_j) - f(i_{j+1} - 1).
\]

Both amounts are greater than or equal to zero, and the first two inequalities follow. For \(i_k\) the difference \(f(i_k) - f(a)\) has a simpler expression, say \((i_k - i_{k-1})(a+1-i_k) - (a - i_{k-1})\), which equals \(-(i_k - (i_{k-1} + 1))(i_k - a) \geq 0\). This proves the last inequality.

After applying several times these inequalities we obtain \(\#D(m, m + i_1, \ldots, m + i_k) \geq \#D(m, m + 1, \ldots, m + i, m + j, m + j + 1, \ldots, m + a)\) with for some \(1 \leq i < j \leq a\) such that \(a + 1 - (j - i) = k\). From Corollary 3, \(D(m, m + 1, \ldots, m + i, m + j, m + j + 1, \ldots, m + a) = \#D(m) + \frac{1}{2}(a + 1 - (j - i))(a + (j - i))\), which equals \(\#D(m) + \frac{1}{2}k(2a + 1 - k)\).

Next we see that the set of divisors of elements of the form \(m + \lambda\) (with \(m \geq 2c - 1\)) that are larger than \(m\) have a triangle shape, and their cardinality depends on the basis of this triangle drawn in \([m + 1, m + a]\).

Lemma 2. Let \(i\) be a positive integer, \(0 \leq l < a\), and \(m \geq 2c - 1\). Then the set \(D(m + ia + l) \cap [m + 1, m + a]\) equals to:

(a) \(\{m + 1, \ldots, m + l, m + a + l - i + 1, \ldots, m + a\}\) if \(l < i\), and
(b) \(\{m + l - i + 1, \ldots, m + l\}\) otherwise.

Moreover,
\[
\#D(m + ia + l) \cap [m + 1, \infty] = \begin{cases} \frac{i(i+1)}{2} + l & \text{if } l \leq i, \\ \frac{(i+1)(i+2)}{2} & \text{otherwise}. \end{cases}
\]

Proof. According to the proof of Proposition 4, \(D(m + ia + l) \cap [m + 1, \infty) \subseteq \{m + ia + l - a(x + y) - y \mid 0 \leq x < a + 1 + i - l, 0 \leq y < l\} \cup \{m + ia + l - a(x + y) - y \mid 0 \leq x < i - l, l \leq y < a\} \). Thus we are looking for elements of the form \(m + ia + l - a(x + y) - y\) in \([m + 1, m + a]\), where \(x\) and \(y\) fulfill certain conditions.
- Assume that $0 \leq x < a + 1 + i - l$ and $0 \leq y < l$. Then $m + ia + l - a(x + y) - y = m + k$ for some $k \in \{0, \ldots, a\}$ if and only if $x + y = i$ and $k = l - y$. As $0 \leq y < l$, this yields $\{m + 1, \ldots, m + l\} \subseteq D(m, m + ia + l) \cap [m + 1, m + a]$, if $i > l$, and $\{m + l - i + 1, \ldots, m + l\}$ otherwise.

- For $0 \leq x < i - l$ and $l \leq y < a$, we write $m + ia + l - a(x + y) - y = m + ia + l + a - a(x + y + 1) - y$, which we want to be equal to $m + k$ for some $k \in \{0, \ldots, a\}$. Since $0 \leq l - y + a \leq a$, we deduce that $k = l - y + a$ and $i = x + y + 1$. Observe that in this setting $l \leq y < i$, and thus $\{m + a + l - i + 1, \ldots, m + a\} \subseteq D(m, m + ia + l) \cap [m + 1, m + a]$.

The proof of the second assertion follows analogously, counting now the pairs $(x, y)$ with $x + y \leq i$ and $x + y + 1 \leq i$, respectively. □

Remark 3. Let $i$ be such that $\frac{1}{2}(i + 1) < r \leq \frac{1}{2}(i + 1)(i + 2)$. Define $b(r) = i$. Then

$$\rho_r = b(r)a + \left(r - 1 - \frac{1}{2}b(r)(b(r) + 1)\right) = (r - 1) + b(r)\left(a - \frac{b(r) + 1}{2}\right).$$

By the preceding proposition $\#(D(s + \rho_r) \cap [m + 1, m + a]) = b(r)$.

The bases of the triangles can be also used to compare different elements greater than $m$ with respect to divisibility.

Lemma 3. Let $u, v, i, l$ be non negative integers and $m \geq 2e - 1$. Then $D(m + ua + v) \cap [m + 1, m + a] \subseteq D(m + ia + l) \cap [m + 1, m + a]$ if and only if $m + ua + v \in D(m + ia + l)$.

Proof. We distinguish two cases depending on the shape of $D(m + ia + l) \cap [m + 1, m + a]$.

If $i \leq l$, then $D(m + ia + l) \cap [m + 1, m + a] = \{m + l - i + 1, \ldots, m + l\}$. Thus in view of Lemma 2, if $D(m + ia + l) \cap [m + 1, m + a] \subseteq D(m + ia + l) \cap [m + 1, m + a]$, then $u \leq v$. Moreover, $v \leq l$ and $i - l \geq u - v$. Hence $i - u \geq l - v \geq 0$, and consequently $ia + l - (ua + v) = (i - u)a + (l - v) \in S$.

Assume now that $l < i$. Then by Lemma 2, $D(m + ia + l) \cap [m + 1, m + a] = \{m + 1, \ldots, m + l, m + a + l - i + 1, \ldots, m + a\}$. As $D(m + ia + l) \cap [m + 1, m + a] \subseteq D(m + ia + l) \cap [m + 1, m + a]$, it may happen that

- $D(m + ia + l) \cap [m + 1, m + a] \subseteq \{m + 1, \ldots, m + l\} = D(m + la + l) \cap [m + 1, m + a]$, and thus $m + ia + l \in D(m + la + l) \subseteq D(m + ia + l)$;
- $D(m + ia + l) \cap [m + 1, m + a] \subseteq \{m + a + l - i + 1, \ldots, m + a\}$, and then $m + ia + l \in D(m + (i - l)a) \subseteq D(m + ia + l)$;
- $v \leq l$ and $i - l \geq u - v$, and we have seen already that in this case the statement holds. □

By using this characterization we can bound the maximal number of elements over a given segment in $[m + 1, m + a]$ (with respect to divisibility).
Lemma 4. Let \( F \) be a subset of \([m + 1, m + a]\) either of consecutive integers or of the form \{m + 1, \ldots, m + u, m + v, \ldots, m + a\} for some integers \( u, v \) with \( u < v \). Then the maximal cardinality of \( D(m_1, \ldots, m_k) \cap [m + 1, \infty) \) with \( 2c - 1 \leq m = m_1 < \cdots < m_k \) such that \( D(m_1, \ldots, m_k) \cap [m + 1, m + a] = F \) is at most \( \frac{(\#F + 1)(\#F + 2)}{2} \).

Proof. If \( F = \{m + u, \ldots, m + v\} \), then \( F = D(m + (v - u + 1)a + v) \cap [m + 1, m + a] \), and if \( F = \{m + 1, \ldots, m + u, m + v, \ldots, m + a\} \), then \( F = D(m + (a + u - v + 1)a + u) \cap [m + 1, m + a] \) (Lemma 2). Define \( n = m + (v - u + 1)a + v \) in the first setting, and \( n = m + (a + u - v + 1)a + u \) in the latter. If \( D(m_1, \ldots, m_k) \cap [m + 1, m + a] = F \), then \( D(m_i) \cap [m + 1, m + a] \subseteq F \), for all \( i \). In view of Lemma 3, we get that \( m_i \in D(n) \). Hence \( D(m_1, \ldots, m_k) \subseteq D(n) \) and the proof follows by Lemma 2.

\( \square \)

Theorem 2. Let \( a \) be a positive integer.

\[ E(r, \langle a, a + 1 \rangle) = \rho_r, \]

where \( \{0 = \rho_1 < \rho_2 < \cdots < \rho_r < \cdots\} = \langle a, a + 1 \rangle \).

Proof. We can assume that in \( D(m = m_1 < m_2 < \cdots < m_r) \) there are no “gaps” below any \( m_i \), that is, for all \( i \), if \( m_i - t \in S \) for some \( t \in S \cap [m, \infty) \), then \( t = m_j \) for some \( j \) (see Proposition 1).

Define \( L = D(m_1, \ldots, m_r) \cap [m, m + a] \), which by the above assumption is a subset of \( \{m_1, \ldots, m_r\} \). It is clear that \( \#D(m_1, \ldots, m_r) \geq (r - \#L + \#D(L) \), since \( D(L) \cup (\{m_1, \ldots, m_r\} \setminus L) \subseteq D(m_1, \ldots, m_r) \).

Set \( k = \#L \). Then \( \#D(m_1, \ldots, m_r) \geq (r - k) + \#D(m, m + 1, \ldots, m + k - 1) = \#D(m) + (r - k) + \frac{1}{2}(k - 1)(2a + 2 - k) \) (Lemma 1). For \( k = b(r) + 1 \) one gets that this amount is precisely \( \#D(m + \rho_1 - \rho_2 - \rho_3, \ldots, m + \rho_r - \rho_3, m + \rho_r) = \#D(m + \rho_r) = \#D(m) + \rho_r \) (for \( m \geq 2c - 1 \); see Proposition 4). In view of Proposition 2, we only have to prove that \( E(S, r) = \rho_r \) for \( \rho_r \leq c = a(a - 1) \), whence \( b(r) \leq a - 1 \).

Next, we prove that \( k > b(r) \). Assume to the contrary that \( k \leq b(r) \). Write \( F = L \setminus \{m\} = F_1 \cup \cdots \cup F_n \) with \( F_i \) subsets of consecutive integers, and every integer in \( F_i \) is smaller than any integer in \( F_j \) whenever \( i < j \). Let \( k_i = \#F_i \) for all \( i \). Clearly, \( k - 1 = k_1 + \cdots + k_n \). If \( \{m + 1, m + a\} \subseteq F \), redefine \( F_1 \) as \( F_1 \cup F_n \), \( n \) as \( n - 1 \), and \( k_1 \) as \( k_1 + k_n \). In view of Lemma 4 the number of divisors over \( F_i \) is at most \( \frac{(k_i + 1)(k_i + 2)}{2} \). Then \( \#D(m_1, \ldots, m_r) \cap [m, \infty) \leq \sum_{i=1}^{n} \frac{(k_i + 1)(k_i + 2)}{2} \leq k \sum_{i=1}^{n} \frac{k_i + 2}{2} \leq k \frac{k+1}{2} \leq \frac{b(r)(b(r)+1)}{2} < r \) (Remark 3), and this is impossible since \( \{m_1, \ldots, m_r\} \subseteq D(m_1, \ldots, m_r) \cap [m, \infty) \).

If we write \( f(k) = (r - k) + \frac{1}{2}(k - 1)(2a + 2 - k) = (r - 1) + (k - 1)(a - \frac{k}{2}) \), \( f \) has a maximum at \( k = a + 1/2 \), and \( f(a) = f(a + 1) \). Thus if we restrict to the values of \( k \in \{1, \ldots, a + 1\} \), this function is non-decreasing with maximum at \( a \) and \( a + 1 \) (notice also that \( f(k + 1) - f(k) = a - k \)). Since we are taking \( k = \#L \), and this amount is greater than or equal to \( b(r) + 1 \), the minimum is reached at \( b(r) + 1 \).

\( \square \)
References


