

ADDITION BEHAVIOR OF A NUMERICAL SEMIGROUP

by

Maria Bras-Amorós

Abstract. — In this work we study some objects describing the addition behavior of a numerical semigroup and we prove that they uniquely determine the numerical semigroup. We then study the case of Arf numerical semigroups and find some specific results.

Résumé (Comportement de l'addition dans un semi-groupe numérique). — Dans ce travail, nous étudions des objets qui décrivent le comportement de l'addition dans un semi-groupe numérique, tout en montrant qu'ils le déterminent complètement. Ensuite, nous étudions le cas des semi-groupes numériques de type Arf et en donnons quelques résultats spécifiques.

Introduction

Let \mathbb{N}_0 denote the set of all non-negative integers. A *numerical semigroup* is a subset Λ of \mathbb{N}_0 containing 0, closed under summation and with finite complement in \mathbb{N}_0 . For a numerical semigroup Λ define the *genus* of Λ as the number $g = \#(\mathbb{N}_0 \setminus \Lambda)$ and the *conductor* of Λ as the unique integer $c \in \Lambda$ such that $c-1 \notin \Lambda$ and $c+\mathbb{N}_0 \subseteq \Lambda$. The elements in Λ are called the *non-gaps* of Λ while the elements in $\Lambda^c = \mathbb{N}_0 \setminus \Lambda$ are called the *gaps* of Λ . The *enumeration* of Λ is the unique increasing bijective map $\lambda : \mathbb{N}_0 \rightarrow \Lambda$. We will use λ_i for $\lambda(i)$.

A first object describing the addition behavior in a numerical semigroup with enumeration λ is the binary operation \oplus defined by $i \oplus j = \lambda^{-1}(\lambda_i + \lambda_j)$. We will show that this operation determines completely the numerical semigroup.

Let F/\mathbb{F} be a function field and let P be a rational point of F/\mathbb{F} . For a divisor D of F/\mathbb{F} , let $\mathcal{L}(D) = \{0\} \cup \{f \in F^* \mid (f) + D \geq 0\}$. Define $A = \bigcup_{m \geq 0} \mathcal{L}(mP)$ and let

2000 Mathematics Subject Classification. — 20M99, 94B27.

Key words and phrases. — Numerical semigroup, Arf semigroup.

This work was supported in part by the Spanish CICYT under Grant TIC2003-08604-C04-01, by Catalan DURSI under Grant 2001SGR 00219.

$\Lambda = \{-v_P(f) \mid f \in A \setminus \{0\}\} = \{-v_i \mid i \in \mathbb{N}_0\}$ with $-v_i < -v_{i+1}$. It is well known that the number of elements in \mathbb{N}_0 which are not in Λ is equal to the genus of the function field. Furthermore, $v_P(1) = 0$ and $v_P(fg) = v_P(f) + v_P(g)$ for all $f, g \in A$. Hence, Λ is a numerical semigroup. It is called the *Weierstrass semigroup* at P . Suppose moreover that P_1, \dots, P_n are pairwise distinct rational points of F/\mathbb{F}_q which are different from P and let φ be the map $A \rightarrow \mathbb{F}_q^n$ such that $f \mapsto (f(P_1), \dots, f(P_n))$. For $m \geq 0$ the *one-point Goppa code* of order m associated to P and P_1, \dots, P_n is defined as $C_m = \varphi(\mathcal{L}(\lambda_m P))^\perp$.

A second object describing the addition behavior of a numerical semigroup Λ with enumeration λ are the sequence of sets (N_i) defined by $N_i = \{j \in \mathbb{N}_0 \mid \lambda_i - \lambda_j \in \Lambda\}$ and the sequence (ν_i) defined by $\nu_i = \#N_i$. A first application of the sequence (ν_i) is on the *order bound* on the minimum distance of the code C_m , defined as $d_{\text{ORD}}^\varphi(C_m) = \min\{\nu_i \mid i > m, C_i \neq C_{i-1}\}$ and satisfying $d_{C_m} \geq d_{\text{ORD}}^\varphi(C_m)$, where d_{C_m} is the minimum distance of the code C_m [7, 10, 9]. A second application is on the definition of improved codes. Let $\mathcal{F} = \{f_i \in A \mid i \in \mathbb{N}_0\}$ be such that $v_P(f_i) = \nu_i$. Given a designed minimum distance $\delta \in \mathbb{N}_0$, define $\tilde{C}_\varphi(\delta) = [\varphi(f_i) \mid \nu_i < \delta, C_i \neq C_{i-1}]^\perp$, where $[u_1, \dots, u_n]$ is the \mathbb{F}_q -vector space spanned by u_1, \dots, u_n . This is a code improving the dimension of one-point Goppa codes while keeping the same designed minimum distance [8].

Notice that in both applications of the sequence (ν_i) its increasingness is very important. In [4] we prove that the unique numerical semigroup for which (ν_i) is strictly increasing is \mathbb{N}_0 while the only numerical semigroups for which it is non-decreasing are ordinary numerical semigroups. This gives a characterization of a class of semigroups by means of a property on the sequence (ν_i) . In this work we show that a numerical semigroup can be uniquely determined by its associated sequence (ν_i) . The proof, which was already given in [4] is constructive. So, we get an algorithm to obtain the semigroup from the sequence (ν_i) . This algorithm is very technical. Here, for the case of Arf numerical semigroups we present three new algorithms which are much more simple.

In Section 1 we show that given a numerical semigroup the implicit binary operation \oplus uniquely determines it. In Section 2 we show that given a numerical semigroup the sequence ν_i determines it uniquely and give a constructive algorithm. In Section 3 we give, for the case of Arf numerical semigroups, a much simpler construction of the semigroup from the associated sequence (ν_i) .

1. The operation \oplus determines a semigroup

Definition 1.1. — Given a numerical semigroup Λ with enumeration λ , define the binary operation \oplus in \mathbb{N}_0 by

$$i \oplus j = \lambda^{-1}(\lambda_i + \lambda_j).$$

Remark 1.2. — Let Λ be a numerical semigroup with enumeration λ , genus g and conductor c . If $g(t)$ is the number of gaps which are smaller than λ_t , then it is obvious that $\lambda_t = g(t) + t$. As a consequence,

$$\begin{aligned} \lambda_t &= g + t \text{ for all } t \geq \lambda^{-1}(c), \\ \lambda_t &< g + t \text{ for all } t < \lambda^{-1}(c). \end{aligned}$$

Notice that, in particular, $\lambda^{-1}(c) = c - g$.

Lemma 1.3. — Let Λ be a numerical semigroup with enumeration λ and conductor c . Then, for any $a \in \mathbb{N}_0$,

$$\lambda_{a+b} \geq \lambda_a + b \text{ for all } b \in \mathbb{N}_0,$$

with equality if $\lambda_a \geq c$.

Proof. — We have $\lambda_{a+b} = \lambda_a + b$ if b is such that there are no gaps between λ_a and λ_{a+b} while $\lambda_{a+b} > \lambda_a + b$ if b is such that there is at least one gap between λ_a and λ_{a+b} . If $\lambda_a \geq c$, there will be no gaps larger than λ_a and so, $\lambda_{a+b} = \lambda_a + b$ for all b , while if $\lambda_a < c$, the most we can say is $\lambda_{a+b} \geq \lambda_a + b$. \square

Lemma 1.4. — Let Λ be a numerical semigroup with enumeration λ and conductor c . Then, for any $a, b \in \mathbb{N}_0$,

$$a \oplus b \leq a + \lambda_b,$$

with equality if $\lambda_a \geq c$.

Proof. — We have $\lambda_{a \oplus b} = \lambda_a + \lambda_b$ by definition of $a \oplus b$ and $\lambda_a + \lambda_b \leq \lambda_{a+\lambda_b}$ for all b , with equality if $\lambda_a \geq c$, by Lemma 1.3. Since λ is bijective and increasing, this means $a \oplus b \leq a + \lambda_b$, with equality if $\lambda_a \geq c$. \square

Proposition 1.5. — A numerical semigroup Λ is uniquely determined by the binary operation \oplus .

Proof. — We will show that Λ is unique by proving that λ_i is uniquely determined by \oplus for all $i \in \mathbb{N}_0$. By Lemma 1.4,

$$\begin{aligned} i \oplus j &\leq j + \lambda_i \text{ for all } j, \\ i \oplus j &= j + \lambda_i \text{ for all } j \text{ with } \lambda_j \geq c. \end{aligned}$$

Therefore, $\max_j \{i \oplus j - j\}$ exists for all i , is uniquely determined by \oplus and it is exactly λ_i . \square

2. The sequence (ν_i) determines a semigroup

In this section we prove that any numerical semigroup is uniquely determined by the associated sequence (ν_i) . We will use the following well-known result on the values ν_i .

Proposition 2.1. — *Let Λ be a numerical semigroup with genus g , conductor c and enumeration λ . Let $g(i)$ be the number of gaps smaller than λ_i and let*

$$D(i) = \{l \in \Lambda^c \mid \lambda_i - l \in \Lambda^c\}.$$

Then for all $i \in \mathbb{N}_0$,

$$\nu_i = i - g(i) + \#D(i) + 1.$$

In particular, for all $i \geq 2c - g - 1$ (or equivalently, for all i such that $\lambda_i \geq 2c - 1$), $\nu_i = i - g + 1$.

Proof. — [10, Theorem 3.8.]. □

Theorem 2.2. — *Suppose that (ν_i) corresponds to the numerical semigroup Λ . Then there is no other numerical semigroup with the same sequence (ν_i) .*

Proof. — If $\Lambda = \mathbb{N}_0$ then (ν_i) is strictly increasing and there is no other semigroup with the same sequence (ν_i) (see [4]).

Suppose that Λ is not trivial. Then we can determine the genus and the conductor from the sequence (ν_i) . Indeed, let $k = 2c - g - 2$. In the following we will show how to determine k without the knowledge of c and g . Notice that $c \geq 2$ and so $2c - 2 \geq c$. This implies $k = \lambda^{-1}(2c - 2)$ and $g(k) = g$. By Proposition 2.1, $\nu_k = k - g + \#D(k) + 1$. But $D(k) = \{c - 1\}$. So, $\nu_k = k - g + 2$. By Proposition 2.1 again, $\nu_i = i - g + 1$ for all $i > k$ and so we have

$$k = \max\{i \mid \nu_i = \nu_{i+1}\}.$$

We can determine the genus as

$$g = k + 2 - \nu_k$$

and the conductor as

$$c = \frac{k + g + 2}{2}.$$

Now we know that $\{0\} \in \Lambda$ and $\{i \in \mathbb{N}_0 \mid i \geq c\} \subseteq \Lambda$ and, furthermore, $\{1, c - 1\} \subseteq \Lambda^c$. It remains to determine for all $i \in \{2, \dots, c - 2\}$ whether $i \in \Lambda$. Let us assume $i \in \{2, \dots, c - 2\}$. On one hand, $c - 1 + i - g > c - g$ and so $\lambda_{c-1+i-g} > c$. This means that $g(c - 1 + i - g) = g$ and hence

$$(1) \quad \nu_{c-1+i-g} = c - 1 + i - g - g + \#D(c - 1 + i - g) + 1.$$

On the other hand, if we define $\tilde{D}(i)$ to be

$$\tilde{D}(i) = \{l \in \Lambda^c \mid c - 1 + i - l \in \Lambda^c, i < l < c - 1\}$$

then

$$(2) \quad D(c - 1 + i - g) = \begin{cases} \tilde{D}(i) \cup \{c - 1, i\} & \text{if } i \in \Lambda^c, \\ \tilde{D}(i) & \text{otherwise.} \end{cases}$$

So, from (1) and (2),

$$i \text{ is a non-gap} \iff \nu_{c-1+i-g} = c + i - 2g + \#\tilde{D}(i).$$

This gives an inductive procedure to decide whether i belongs to Λ decreasingly from $i = c - 2$ to $i = 2$. □

This theorem suggests the following algorithm to get Λ from (ν_i) .

- Compute $k = \max\{i \mid \nu_i = \nu_{i+1}\}$.
- Compute $g = k + 2 - \nu_k$ and $c = \frac{k+g+2}{2}$.
- $\{0\} \cup \{i \in \mathbb{N}_0 \mid i \geq c\} \subseteq \Lambda$, $\{1, c - 1\} \subseteq \Lambda^c$.
- For all $i \in \{2, \dots, c - 2\}$,
 - Compute

$$\tilde{D}(i) = \{l \in \Lambda^c \mid c - 1 + i - l \in \Lambda^c, i < l < c - 1\}$$

$$- i \text{ is a non-gap} \iff \nu_{c-1+i-g} = c + i - 2g + \#\tilde{D}(i).$$

Remark 2.3. — From the proof of Theorem 2.2 we see that a semigroup can be determined by $k = \max\{i \mid \nu_i = \nu_{i+1}\}$ and the values ν_i for $i \in \{c - g + 1, \dots, 2c - g - 3\}$.

3. Arf case

A numerical semigroup Λ is said to be *Arf* if for every $x, y, z \in \Lambda$ with $x \geq y \geq z$, it holds that $x + y - z \in \Lambda$. Arf numerical semigroups have been widely studied in [1, 6, 12, 3, 2, 4]. In particular we have that a numerical semigroup is Arf if and only if for every $x, y \in \Lambda$ with $x \geq y$, it holds that $2x - y \in \Lambda$ [6]. In [11, 5, 3, 2] a study on the codes of maximum dimension among the codes in a certain class decoding the so-called generic errors leads to the following definition.

Definition 3.1. — Given a numerical semigroup Λ with enumeration λ and a non-negative integer i define

$$\Sigma_i := \{l \in \Lambda \mid l \geq \lambda_i\}.$$

We will see that the sets Σ_i are very important when studying Arf numerical semigroups. In particular the study of the codes explained above lead to new characterizations of Arf numerical semigroups [2]. Let us first state three results on general numerical semigroups related to the sets Σ_i .

Proposition 3.2. — *Given a numerical semigroup Λ and a non-negative integer i ,*

- (1) $\lambda_i + \Sigma_i \subseteq \Sigma_i + \Sigma_i$,
- (2) $\#\{j \in \mathbb{N}_0 \mid \lambda_j \notin \Sigma_i + \Sigma_i\} \leq \lambda_i + i$,
- (3) $\{j \in \mathbb{N}_0 \mid \lambda_j \notin \Sigma_i + \Sigma_i\} \subseteq \{j \in \mathbb{N}_0 \mid \nu_j \leq 2i\}$.

Proof

- (1) Obvious.