Séminaires & Congrès
11, 2005, p. 21–28

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 $g = \#(\mathbb{N}_0 \smallsetminus \Lambda)$ 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 $\Lambda^c = \mathbb{N}_0 \smallsetminus \Lambda$ are called the *gaps* of Λ. The *enumeration* of Λ is the unique increasing bijective map $\lambda : \mathbb{N}_0 \to \Lambda$. 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 $\mathcal{L}(D) = \{0\} \cup \{f \in F^* \mid (f) + D \geqslant 0\}$. Define $A = \bigcup_{m\geqslant 0} \mathcal{L}(mP)$ 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.

$\Lambda = \{-v_P(f) \mid f \in A \smallsetminus \{0\}\} = \{-v_i \mid i \in \mathbb{N}_0\}$ 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 $A \to \mathbb{F}_q^n$ such that $f \mapsto (f(P_1), \dots, f(P_n))$. For $m \geqslant 0$ 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 $d^{\varphi}_{\mathrm{ORD}}(C_m) = \min\{\nu_i \mid i > m, C_i \neq C_{i-1}\}$ and satisfying $d_{C_m} \geqslant d^{\varphi}_{\mathrm{ORD}}(C_m)$, 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 $v_P(f_i) = v_i$. Given a designed minimum distance $\delta \in \mathbb{N}_0$, define $\widetilde{C}_\varphi(\delta) = [\varphi(f_i) \mid \nu_i < \delta, C_i \neq C_{i-1}]^\perp$, 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,

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

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 $a \in \mathbb{N}_0$,*

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

with equality if $\lambda_a \geqslant c$.

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 $\lambda_a \geqslant c$, 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 $\lambda_{a+b} \geqslant \lambda_a + b$. □

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

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

with equality if $\lambda_a \geqslant c$.

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

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,

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

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

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

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 $c \geqslant 2$ and so $2c-2 \geqslant c$. 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 $\{i \in \mathbb{N}_0 \mid i \geqslant c\} \subseteq \Lambda$ 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

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

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

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

then

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

So, from (1) and (2),

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

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 $c = \frac{k+g+2}{2}$.
– $\{0\} \cup \{i \in \mathbb{N}_0 \mid i \geqslant c\} \subseteq \Lambda$, $\{1, c-1\} \subseteq \Lambda^c$.
– For all $i \in \{2, \ldots, c-2\}$,
  – Compute

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

  – i is a non-gap $\Longleftrightarrow \nu_{c-1+i-g} = c + i - 2g + \#\widetilde{D}(i)$.

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 $i \in \{c-g+1, \ldots, 2c-g-3\}$.

3. Arf case

A numerical semigroup Λ is said to be *Arf* if for every $x, y, z \in \Lambda$ with $x \geqslant y \geqslant z$, 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 $x \geqslant y$, 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

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

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

Proof

(1) Obvious.

(2) By 1., $\#\{j \in \mathbb{N}_0 \mid \lambda_j \notin \Sigma_i + \Sigma_i\} \leqslant \#\{j \in \mathbb{N}_0 \mid \lambda_j \notin \lambda_i + \Sigma_i\}$. On the other hand, note that $\lambda_i + \Sigma_i = \{\lambda_i + \lambda_k \mid i \leqslant k \leqslant c-g-1\} \sqcup \{l \in \mathbb{N}_0 \mid l \geqslant \lambda_i + c\}$. So,

$$\begin{aligned}\#\{j \in \mathbb{N}_0 \mid \lambda_j \notin \lambda_i + \Sigma_i\} = \#\{j \in \mathbb{N}_0 \mid \lambda_j \leqslant \lambda_i + c - 1\}&\\ - \#\{\lambda_i + \lambda_k \mid i \leqslant k \leqslant c-g-1\}&\\ = \lambda_i + c - g - c + g + i = \lambda_i + i.&\end{aligned}$$

(3) If $\nu_j > 2i$ then there exist at least $2i+1$ elements $\lambda_k < \lambda_j$ such that $\lambda_j - \lambda_k = \lambda_{k'} \in \Lambda$. Let the smallest ones of such elements be

$$\lambda_0 = 0 < \lambda_{k_1} < \cdots < \lambda_{k_i}.$$

In particular, $\lambda_{k_i} \geqslant \lambda_i$. Then the largest of such elements are

$$\lambda_j - \lambda_{k_i} < \cdots < \lambda_j - \lambda_{k_1} < \lambda_j$$

and all of them are larger than or equal to λ_{k_i}. So, $\lambda_j - \lambda_{k_i} \in \Lambda$ and $\lambda_j - \lambda_{k_i} \geqslant \lambda_{k_i}$. Hence, $\lambda_j = \lambda_{k_i} + (\lambda_j - \lambda_{k_i}) \in \Sigma_i + \Sigma_i$. □

The same three results can be more refined for the case of Arf numerical semigroups. This is what we state in next proposition.

Proposition 3.3. — *For a numerical semigroup Λ, the condition of being Arf is equivalent to each of the following conditions.*

(1) $\lambda_i + \Sigma_i = \Sigma_i + \Sigma_i$ *for all* $i \in \mathbb{N}_0$,
(2) $\#\{j \in \mathbb{N}_0 \mid \lambda_j \notin \Sigma_i + \Sigma_i\} = \lambda_i + i$ *for all* $i \in \mathbb{N}_0$,
(3) $\{j \in \mathbb{N}_0 \mid \lambda_j \notin \Sigma_i + \Sigma_i\} = \{j \in \mathbb{N}_0 \mid \nu_j \leqslant 2i\}$ *for all* $i \in \mathbb{N}_0$.

Proof

(1) If Λ is Arf and $i \in \mathbb{N}_0$ then for any $\lambda_j, \lambda_k \in \Sigma_i$, $\lambda_j + \lambda_k - \lambda_i \in \Lambda$. Moreover, $\lambda_j + \lambda_k - \lambda_i \geqslant \lambda_i$ and $\lambda_j + \lambda_k - \lambda_i \in \Sigma_i$. So, $\Sigma_i + \Sigma_i - \lambda_i \subseteq \Sigma_i$ and, by Proposition 3.2, $\lambda_i + \Sigma_i = \Sigma_i + \Sigma_i$. Now, if $\lambda_i + \Sigma_i = \Sigma_i + \Sigma_i$ holds for all $i \in \mathbb{N}_0$, then for all $\lambda_j \geqslant \lambda_k \geqslant \lambda_i$, $\lambda_j + \lambda_k - \lambda_i \in \Sigma_i + \Sigma_i - \lambda_i = \Sigma_i$. So, $\lambda_j + \lambda_k - \lambda_i \in \Lambda$.

(2) The proof of this item can be carried out using 1. and a reasoning analogous to that in the proof of Proposition 3.2.

(3) Suppose Λ is Arf. If $\lambda_j \in \Sigma_i + \Sigma_i$ then $\lambda_j = \lambda_k + \lambda_l$ for some $k, l \geqslant i$. Now, since Λ is Arf, $\lambda_j - \lambda_m = \lambda_k + \lambda_l - \lambda_m \in \Lambda$ for all $m \leqslant i$ and $\lambda_j - \lambda_m = \lambda_{m'}$ with $m' \geqslant i$. This gives at least $2i+1$ integers m such that $\lambda_j - \lambda_m \in \Lambda$. On the other hand, suppose that Λ is such that $\nu_j \geqslant 2i+1$ for all j with $\lambda_j \in \Sigma_i + \Sigma_i$. In particular, $2\lambda_i \in \Sigma_i + \Sigma_i$ and so, $\nu_{i \oplus i} \geqslant 2i+1$. Notice that for all $j < k$ with $\lambda_j + \lambda_k = 2\lambda_i$, we have $\lambda_j < \lambda_i$ and $\lambda_i < \lambda_k$. The inequality $\nu_{i \oplus i} \geqslant 2i+1$ means then that there exist at least i elements in the semigroup smaller than λ_i that can be substracted to $2\lambda_i$. But these are all elements smaller than λ_i because there are only i. So, $2\lambda_i - \lambda_j \in \Lambda$ for all $j \leqslant i$. □

We can now present three new algorithms to construct an Arf numerical semigroup from the sequence (ν_i) which are much easier than the algorithm presented in Section 2.

Theorem 3.4. — *Let Λ be an Arf numerical semigroup different from $\mathbb{N}_0$, with genus g, conductor c and enumeration λ. The semigroup Λ can be got from (ν_i) by the following three algorithms:*

Algorithm 1: *For all $i \in \mathbb{N}_0$, $\lambda_i = \#\{j \in \mathbb{N}_0 \mid \nu_j \leqslant 2i\} - i$.*

Algorithm 2:

- $\lambda_0 = 0$.
- *For all $i \geqslant 1$,*

$$\lambda_i = \lambda_{i-1} + \#\{j \in \mathbb{N}_0 \mid \nu_j = 2i-1\} + \#\{j \in \mathbb{N}_0 \mid \nu_j = 2i\} - 1.$$

Algorithm 3:

- *Let $k = \max\{j \mid \nu_j = \nu_{j+1}\}$, then $c - g = \frac{\nu_k}{2}$ and $g = k + 2 - \nu_k$.*
- $\lambda_0 = 0$.
- *For all $1 \leqslant i \leqslant c - g$,*

$$\lambda_i = \max\{k \mid \nu_k \leqslant 2i\} - (c-g) + 1.$$

- *For all $i > c - g$,*

$$\lambda_i = i + g.$$

Proof. — It follows from Proposition 3.3. In particular, algorithm 1 and 2 follow from Proposition 3.3 (2) and Proposition 3.3 (3) while algorithm 3 follows from Proposition 3.3 (1) and Proposition 3.3 (3). □

Conclusion

We proved that both the binary operation $\oplus$ and the sequence (ν_i) uniquely determine the corresponding numerical semigroup. Now it would be interesting to find which sequences of positive integers correspond to the sequence (ν_i) of a numerical semigroup. This could lead us to a deeper study of the Feng-Rao bound on the minimum distance of one-point codes.

References

[1] V. Barucci, D.E. Dobbs & M. Fontana – *Maximality properties in numerical semigroups and applications to one-dimensional analytically irreducible local domains*, Mem. Amer. Math. Soc., vol. 125, no. 598, American Mathematical Society, 1997.

[2] M. Bras-Amorós – Improvements to evaluation codes and new characterizations of Arf semigroups, in *Applied algebra, algebraic algorithms and error-correcting codes (Toulouse, 2003)*, Lecture Notes in Comput. Sci., vol. 2643, Springer, Berlin, 2003, p. 204–215.

[3] M. Bras-Amorós – Improving Evaluation Codes, Ph.D. Thesis, Universitat Politècnica de Catalunya, Barcelona, 2003.

[4] M. Bras-Amorós – Acute semigroups, the order bound on the minimum distance, and the Feng-Rao improvements, *IEEE Trans. Inform. Theory* **50** (2004), no. 6, p. 1282–1289.

[5] M. Bras-Amorós & M.E. O'Sullivan – The correction capability of the Berlekamp-Massey-Sakata algorithm with majority voting, submitted, 2004.

[6] A. Campillo, J.I. Farrán & C. Munuera – On the parameters of algebraic-geometry codes related to Arf semigroups, *IEEE Trans. Inform. Theory* **46** (2000), no. 7, p. 2634–2638.

[7] G.-L. Feng & T.R.N. Rao – A simple approach for construction of algebraic-geometric codes from affine plane curves, *IEEE Trans. Inform. Theory* **40** (1994), no. 4, p. 1003–1012.

[8] ______, Improved geometric Goppa codes. I. Basic theory, *IEEE Trans. Inform. Theory* **1** (1995), no. 6 part 1, p. 1678–1693, special issue on algebraic geometry codes.

[9] T. Høholdt, J.H. van Lint & R. Pellikaan – Algebraic Geometry codes, North-Holland, Amsterdam, 1998, p. 871–961.

[10] C. Kirfel & R. Pellikaan – The minimum distance of codes in an array coming from telescopic semigroups, *IEEE Trans. Inform. Theory* **1** (1995), no. 6 part 1, p. 1720–1732, special issue on algebraic geometry codes.

[11] M.E. O'Sullivan – Decoding of Hermitian codes: Beyond the minimum distance bound, Preprint, 2001.

[12] J.C. Rosales, P.A. García-Sánchez, J.I. García-García & M.B. Branco – Arf numerical semigroups, *J. Algebra* **276** (2004), p. 3–12.

M. Bras-Amorós, Universitat Autònoma de Barcelona, 08193-Bellaterra, Catalonia, Spain
E-mail : maria.bras@uab.es • *Url :* www.ccd.uab.es/~mbras