Des. Codes Cryptogr. (2009) 53:111–118
DOI 10.1007/s10623-009-9297-8

On numerical semigroups and the redundancy of improved codes correcting generic errors

Maria Bras-Amorós

Received: 24 March 2008 / Revised: 23 April 2009 / Accepted: 24 April 2009 /
Published online: 13 May 2009

Abstract We introduce a new sequence τ associated to a numerical semigroup similar to the ν sequence used to define the order bound on the minimum distance and to describe the Feng–Rao improved codes. The new sequence allows a nice description of the optimal one-point codes correcting generic errors and to compare them with standard codes and with the Feng–Rao improved codes. The relation between the τ sequence and the ν sequence gives a new characterization of Arf semigroups and it is shown that the τ sequence of a numerical semigroup unequivocally determines it.

Keywords Algebraic code · Generic error · Numerical semigroup

Mathematics Subject Classifications (2000) 94B27 · 20M14 · 20M10 · 14G50 · 11T71

1 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 $\mathbb{N}_0$. The *enumeration* of Λ is the unique increasing bijective map $\lambda : \mathbb{N}_0 \to \Lambda$. Usually λ_i is used instead of $\lambda(i)$.

Given a rational point P of a curve with Weierstrass semigroup $\Lambda = \{\lambda_0 < \lambda_1 < \lambda_2 < \dots\}$ one can find an infinite basis $z_0, z_1, \dots, z_i, \dots$ of the ring of functions having poles only at P such that $v_P(z_i) = -\lambda_i$. Consider a set of rational points $P_1, \dots, P_n$ different from P. To each finite subset $W \subseteq \mathbb{N}_0$ we associate the one-point code $C_W =< (z_i(P_1), \dots, z_i(P_n)) : i \in W >^{\perp}$. By extension, we say that W is the set of parity checks of C_W.

The ν *sequence* of a numerical semigroup with enumeration λ is defined by $\nu_i = \#\{j \in \mathbb{N}_0 : \lambda_i - \lambda_j \in \Lambda\}$. When the numerical semigroup is the Weierstrass semigroup at a point

Communicated by Peter Wild.

M. Bras-Amorós (✉)
Universitat Rovira i Virgili, Tarragona, Catalonia, Spain
e-mail: maria.bras@urv.cat

of a curve, this sequence is used to define optimal one-point codes correcting a given number of errors using the Berlekamp–Massey–Sakata algorithm with majority voting. Indeed, the minimum set $\widetilde{R}(t)$ of parity checks that are needed to correct t errors is given by $\widetilde{R}(t) = \{i \in \mathbb{N}_0 : \nu_i < 2t+1\}$ [7,9]. The codes determined by $\widetilde{R}(t)$ are called Feng–Rao improved codes. The ν sequence is also used to define the order bound on the minimum distance for one-point codes [6,9,10]. An interesting fact about the ν sequence of a numerical semigroup is that it characterizes the numerical semigroup in the sense that no other numerical semigroup has the same ν sequence [2]. However, any finite part of the ν sequence of a numerical semigroup is shared by infinitely many numerical semigroups [3]. Other results on the ν sequence can be found in [2,11,13].

We say that the points $P_{i_1}, \ldots, P_{i_t}$ ($P_{i_j} \neq P$) are *generically distributed* if no function generated by $z_0, \ldots, z_{t-1}$ vanishes in all of them. In the context of one-point codes, *generic errors* are those errors whose non-zero positions correspond to generically distributed points. Generic errors of weight t can be a very large proportion of all possible errors of weight t [8]. Thus, by restricting the errors to be corrected to generic errors the decoding requirements will be weaker and we still will be able to correct almost all errors. In [4,12] there is a description of the minimum set $\widetilde{R}^*(t)$ of parity checks that are needed to correct generic errors of weight t. The minimum set of parity checks is $\widetilde{R}^*(t) = \{i \in \mathbb{N}_0 : \lambda_i \neq \lambda_j + \lambda_k$ for any $j, k \geq t\}$.

In Section 2 we will define the new sequence τ of a numerical semigroup. It will allow us to describe $\widetilde{R}^*(t)$ in terms of τ in a similar way to the way $\widetilde{R}(t)$ is described in terms of ν. Then, by studying the monotonicity of τ we can compare the codes determined by $\widetilde{R}^*(t)$ with standard codes and by studying the relation between the sequences ν and τ we can compare the codes determined by $\widetilde{R}^*(t)$ with the Feng–Rao improved codes.

In the next sections we give new proofs of results that are already known on the comparison of $\widetilde{R}^*(t)$ and $\widetilde{R}(t)$ and new results on (1) the comparison of the codes given by $\widetilde{R}^*(t)$ and standard codes; (2) the relation between ν and τ and new characterizations of Arf semigroups; (3) the characterization of numerical semigroups by means of τ.

Section 3 is devoted to the monotonicity of τ. We show that the only numerical semigroups for which τ is always non-decreasing are ordinary semigroups. For non-ordinary semigroups we find the largest position at which the τ sequence is decreasing.

Section 4 is devoted to the relation between the sequences ν and τ. We show that $\tau_i \geq \lfloor \frac{\nu_i - 1}{2} \rfloor$ for all $i \in \mathbb{N}_0$, that $\tau_i = \lfloor \frac{\nu_i - 1}{2} \rfloor$ from a certain value of i, and that $\tau_i = \lfloor \frac{\nu_i - 1}{2} \rfloor$ for all $i \in \mathbb{N}_0$ if and only if Λ is Arf. This adds a new characterization of Arf semigroups in the context of algebraic geometry codes like the ones in [1,4,5].

Finally in Section 5 we show that, as well as the ν sequence, the τ sequence of a numerical semigroup determines it. However, any finite part of it is shared by infinitely many numerical semigroups.

2 The τ sequence and the redundancy of improved codes correcting generic errors

Definition 1 Given a numerical semigroup Λ with enumeration λ define its τ *sequence* by

$$\tau_i = \max\{j \in \mathbb{N}_0 : \text{ exists } k \text{ with } j \leq k \leq i \text{ and } \lambda_j + \lambda_k = \lambda_i\}.$$

Notice that if $N_i = \{j \in \mathbb{N}_0 : \lambda_i - \lambda_j \in \Lambda\}$ then τ_i is the largest element j in N_i with $\lambda_j \leq \lambda_i/2$. In particular, if $\lambda_i/2 \in \Lambda$ then $\tau_i = \lambda^{-1}(\lambda_i/2)$. Notice also that τ_i is 0 if and only if λ_i is either 0 or a generator of Λ.

Table 1 ν and τ sequences of the numerical semigroups generated by 4, 5 and by 6, 7, 8, 17

(a) <4,5>				(b) <6,7,8,17>			
i	λ_i	ν_i	τ_i	i	λ_i	ν_i	τ_i
0	0	1	0	0	0	1	0
1	4	2	0	1	6	2	0
2	5	2	0	2	7	2	0
3	8	3	1	3	8	2	0
4	9	4	1	4	12	3	1
5	10	3	2	5	13	4	1
6	12	4	1	6	14	5	2
7	13	6	2	7	15	4	2
8	14	6	2	8	16	3	3
9	15	4	2	9	17	2	0
10	16	5	3	10	18	4	1
11	17	8	3	11	19	6	2
12	18	9	4	12	20	8	3
13	19	8	4	13	21	8	3
14	20	9	5	14	22	8	3
15	21	10	4	15	23	8	3
16	22	12	5	16	24	9	4
17	23	12	5	17	25	10	4
18	24	13	6	18	26	11	5
19	25	14	6	19	27	12	5
20	26	15	7	20	28	13	6
21	27	16	7	21	29	14	6
22	28	17	8	22	30	15	7
23	29	18	8	23	31	16	7
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

Example 2 In Table 1 we show the ν sequence and the τ sequence of the numerical semigroups generated by 4, 5 and generated by 6, 7, 8, 17.

One difference between the τ sequence and the ν sequence is that, while in the ν sequence not all non-negative integers need to appear, in the τ sequence all of them appear. Notice for instance that 7 does not appear in the ν sequence of the numerical semigroup generated by 4 and 5 nor the numerical semigroup generated by 6, 7, 8, 17. The reason for which any non negative integer j appears in the τ sequence is that if $\lambda_i = 2\lambda_j$ then $\tau_i = j$. Furthermore, the smallest i for which $\tau_i = j$ corresponds to $\lambda_i = 2\lambda_j$.

Lemma 3 *The set $\widetilde{R}^*(t)$ of the parity checks defining a correction capability optimized code correcting all generic errors of weight t is*

$$\widetilde{R}^*(t) = \{i \in \mathbb{N}_0 : \tau_i < t\}.$$

Proof It is shown in [4,12] that $i \in \widetilde{R}^*(t)$ if and only if λ_i can not be represented as a sum $\lambda_j + \lambda_k$ for any $j, k \geq t$. So, proving the lemma is equivalent to proving that $\tau_i \geq t$ if and only if $\lambda_i = \lambda_j + \lambda_k$ for some $j, k \geq t$, which follows from the definition of τ_i. □

3 Comparison of improved codes with standard codes correcting generic errors

Standard evaluation codes are those codes for which the set of parity checks corresponds to all the elements up to a given order. Thus, the standard evaluation code with maximum dimension correcting t generic errors is defined by the set of checks $R^*(t) = \{i \in \mathbb{N}_0 : i \leq m(t)\}$ where $m(t) = \max\{i \in \mathbb{N}_0 : \tau_i < t\}$. Then, by studying the monotonicity of the τ sequence we can compare $\widetilde{R}^*(t)$ and $R^*(t)$ and the associated codes.

Let us introduce some new notations that we will use from now on. Given a numerical semigroup Λ, the elements in the complement $\mathbb{N}_0 \backslash \Lambda$ are called the *gaps* of the numerical semigroup and $\#\mathbb{N}_0 \backslash \Lambda$ is its *genus*. The *conductor* of Λ is the unique integer $c \in \Lambda$ such that $c - 1 \notin \Lambda$ and $c + \mathbb{N}_0 \subseteq \Lambda$. We say that a numerical semigroup is *ordinary* if it is equal to $\{0\} \cup \{i \in \mathbb{N}_0 : i \geq c\}$ for some non-negative integer c. If moreover $c = 0$ then the numerical semigroup is $\mathbb{N}_0$ and in this case we say that it is the *trivial* semigroup. For a non-trivial semigroup, the non-gap previous to the conductor is the *dominant*. Usually we use g, c, d for the genus, the conductor and the dominant of a numerical semigroup. Notice that $\lambda_{c-g} = c$ and $\lambda_{c-g-1} = d$.

It is easy to check that for the trivial numerical semigroup one has $\tau_{2i} = \tau_{2i+1} = i$ for all $i \in \mathbb{N}_0$. That is, the τ sequence is

$$0, 0, 1, 1, 2, 2, 3, 3, 4, 4, 5, 5, \ldots$$

The next proposition determines the τ sequence of all non-trivial ordinary semigroups.

Proposition 4 *The non-trivial ordinary numerical semigroup with conductor c has τ sequence given by*

$$\tau_i = \begin{cases} 0 & \text{if } i \leq c \\ \lfloor \frac{i-c+1}{2} \rfloor & \text{if } i > c \end{cases}$$

Proof Suppose that the numerical semigroup has enumeration λ. On one hand, $\lambda_1, \ldots, \lambda_c$ are all generators and thus $\tau_i = 0$ for $i \leq c$. For $i > c$, $\lambda_i = c + i - 1 \geq 2c$. So, if λ_i is even (which is equivalent to $c + i$ being odd) then $\tau_i = \lambda^{-1}(\frac{\lambda_i}{2}) = \frac{c+i-1}{2} - c + 1 = \frac{i-c+1}{2} = \lfloor \frac{i-c+1}{2} \rfloor$. If λ_i is odd (which is equivalent to either both c and i being even or being odd) then $\tau_i = \lambda^{-1}(\frac{\lambda_i - 1}{2}) = \frac{c+i-2}{2} - c + 1 = \frac{i-c}{2} = \lfloor \frac{i-c+1}{2} \rfloor$. □

Remark 5 The formula in Proposition 4 can be recursively described by $\tau_j = 0$ for all $j \leq c$ and, for all $i > 0$,

$$\begin{cases} \tau_{c+2i+1} = \tau_{c+2i} + 1 \\ \tau_{c+2i+2} = \tau_{c+2i+1} \end{cases}$$

The next proposition gives, for non-ordinary semigroups, the smallest index m for which τ is non-decreasing from τ_m on. We will use the notation $\lfloor a \rfloor_\Lambda$ to denote the semigroup floor of a non-negative integer a, that is, the largest non-gap of Λ which is at most a.

Proposition 6 *Let Λ be a non-ordinary semigroup with dominant d and let $m = \lambda^{-1}(2d)$, then*

(1) $\tau_m = c - g - 1 > \tau_{m+1}$,
(2) $\tau_i < c - g - 1$ *for all* $i < m$,
(3) $\tau_i \leq \tau_{i+1}$ *for all* $i > m$.

Proof For Statement 1 notice that both $2d$ and $2d + 1$ belong to Λ because they must be larger than the conductor. Furthermore, $\tau_{\lambda^{-1}(2d)} = \lambda^{-1}(d) = c - g - 1$ while $\tau_{\lambda^{-1}(2d+1)} = \tau_{\lambda^{-1}(2d)+1} < \lambda^{-1}(d)$ because $d + 1 \notin \Lambda$.

Statement 2 follows from the fact that if $\lambda_i < 2d$ then $\tau_i < \lambda^{-1}(d) = c - g - 1$.

For Statement 3 suppose that $i > m$. Notice that $2d$ is the largest non-gap that can be written as a sum of two non-gaps both of them smaller than the conductor c. Then if $j \leq k \leq i$ and $\lambda_j + \lambda_k = \lambda_i$ it must be $\lambda_k \geq c$ and so $\tau_i = \lambda^{-1}(\lfloor \lambda_i - c \rfloor_\Lambda)$. Since both λ^{-1} and $\lfloor \cdot \rfloor_\Lambda$ are non-decreasing, so is τ_i for $i > m$. □

Corollary 7 *The only numerical semigroups for which the τ sequence is non-decreasing are ordinary semigroups.*

A direct consequence of Corollary 7 is that the standard code determined by $R^*(t)$ is always worse than the improved code determined by $\widetilde{R}^*(t)$ at least for one value of t unless the corresponding numerical semigroup is ordinary. An analogous result is proved in [2, Corollary 7.5] for Feng-Rao improved codes. In this case, Feng-Rao improved codes actually improve standard codes for any numerical semigroup except for ordinary semigroups. From Proposition 6 we can derive that $\widetilde{R}^*(t)$ and $R^*(t)$ coincide from a certain point and we can find this point. We summarize the results of this section in the next Corollary.

Corollary 8 (1) $\widetilde{R}^*(t) \subseteq R^*(t)$ *for all* $t \in \mathbb{N}_0$.
(2) $\widetilde{R}^*(t) = R^*(t)$ *for all* $t \geq c - g$.
(3) $\widetilde{R}^*(t) = R^*(t)$ *for all* $t \in \mathbb{N}_0$ *if and only if the associated numerical semigroup is ordinary.*

Proof Statement 1 is a consequence of the definition of $R^*(t)$. Statement 2 is clear if the associated semigroup is ordinary. Otherwise it follows from the fact proved in Proposition 6 that the largest value of τ_i before it starts being non-decreasing is precisely $c - g - 1$ and that before that all values of τ_i are smaller than $c - g - 1$. Statement 3 is a consequence of Corollary 7. □

4 Comparison of improved codes correcting generic errors with Feng–Rao improved codes

In next theorem we compare τ_i with $\lfloor \frac{\nu_i - 1}{2} \rfloor$ and this will give a new characterization of Arf semigroups. Notice that $t \leq \lfloor \frac{\nu_i - 1}{2} \rfloor$ is the requirement for the majority voting step to obtain the syndromes of order up to i when correcting t errors [9, Proposition 6.11].

Recall that a numerical semigroup Λ with enumeration λ is Arf if $\lambda_i + \lambda_j - \lambda_k \in \Lambda$ for all non-negative integers i, j, k with $i \geq j \geq k$.

In this section we will use several times the fact that if $j \geq c - g$ then $\lambda_j = j + g$. This follows from the definitions of c and g.

Theorem 9 *Let Λ be a numerical semigroup with conductor c, genus g, and associated sequences τ and ν. Then*

(1) $\tau_i \geq \lfloor \frac{\nu_i - 1}{2} \rfloor$ *for all* $i \in \mathbb{N}_0$,
(2) $\tau_i = \lfloor \frac{\nu_i - 1}{2} \rfloor$ *for all* $i \geq 2c - g - 1$,
(3) $\tau_i = \lfloor \frac{\nu_i - 1}{2} \rfloor$ *for all* $i \in \mathbb{N}_0$ *if and only if* Λ *is Arf.*

Proof Let λ be the enumeration of Λ.

(1) For $i \in \mathbb{N}_0$ let $N_i = \{j \in \mathbb{N}_0 : \lambda_i - \lambda_j \in \Lambda\}$ and suppose that the elements in N_i are ordered $N_{i,0} < N_{i,1} < N_{i,2} < \cdots < N_{i,\nu_i - 1}$. On one hand $\tau_i = N_{i, \lfloor \frac{\nu_i - 1}{2} \rfloor}$. On the other hand $N_{i,j} \geq j$ and this finishes the proof of the first statement.
(2) The result is obvious for the trivial semigroup. Thus we can assume that $c \geq g + 1$. Notice that $\tau_i = N_{i, \lfloor \frac{\nu_i - 1}{2} \rfloor} = \lfloor \frac{\nu_i - 1}{2} \rfloor$ if and only if all integers less than or equal to $\lfloor \frac{\nu_i - 1}{2} \rfloor$ belong to N_i. Now let us prove that if $i \geq 2c - g - 1$ then all integers less than or equal to $\lfloor \frac{\nu_i - 1}{2} \rfloor$ belong to N_i. Indeed, if $j \leq \lfloor \frac{\nu_i - 1}{2} \rfloor$ then $\lambda_j \leq \lambda_i/2$ and $\lambda_i - \lambda_j \geq \lambda_i - \lambda_i/2 = \lambda_i/2 \geq c$. So $\lambda_i - \lambda_j \in \Lambda$.
(3) Suppose that Λ is Arf. We want to show that for any non-negative integer i, all non-negative integers less than or equal to $\lfloor \frac{\nu_i - 1}{2} \rfloor$ belong to N_i. By definition of τ_i there exists k with $\tau_i \leq k \leq i$ and $\lambda_{\tau_i} + \lambda_k = \lambda_i$. Now, if j is a non-negative integer with $j \leq \lfloor \frac{\nu_i - 1}{2} \rfloor$, by Statement 1 it also satisfies $j \leq \tau_i$. Then $\lambda_i - \lambda_j = \lambda_{\tau_i} + \lambda_k - \lambda_j \in \Lambda$ by the Arf property, and so $j \in N_i$.
On the other hand, suppose that $\tau_i = \lfloor \frac{\nu_i - 1}{2} \rfloor$ for all non-negative integer i. This means that all integers less than or equal to τ_r belong to N_r for any non-negative integer r. If $i \geq j \geq k$ then $\tau_{\lambda^{-1}(\lambda_i + \lambda_j)} \geq j \geq k$ and by hypothesis $k \in N_{\lambda^{-1}(\lambda_i + \lambda_j)}$, which means that $\lambda_i + \lambda_j - \lambda_k \in \Lambda$. This implies that Λ is Arf. □

Lemma 10 *Let Λ be a numerical semigroup with enumeration λ, conductor $c > 2$, genus g, and dominant d. Then*

(1) $\tau_{(2c-g-2)+2i} = \tau_{(2c-g-2)+2i+1} = (c - g - 1) + i$ *for all* $i \geq 0$
(2) *At least one of the following statements holds*

- $\tau_{(2c-g-2)-1} = c - g - 1$
- $\tau_{(2c-g-2)-2} = c - g - 1$

Proof (1) If $i \geq 1$ then $\lambda_{(2c-g-2)+2i} = 2c - 2 + 2i$ and $\lambda_{(2c-g-2)+2i}/2 = c - 1 + i \in \Lambda$. So $\tau_{(2c-g-2)+2i} = \lambda^{-1}(c-1+i) = c-1+i-g$. On the other hand, $\lambda_{(2c-g-2)+2i+1} = 2c-2+2i+1 = (c-1+i)+(c-1+i+1)$ and so $\tau_{(2c-g-2)+2i+1} = \lambda^{-1}(c-1+i) = c - 1 + i - g$.
If $i = 0$ then $\lambda_{(2c-g-2)+2i} = \lambda_{2c-g-2}$ and since $c > 2$ this is equal to $2c - 2$. Now $\lambda_{2c-g-2}/2 = c - 1$ and the largest non-gap which is at most $c - 1$ is d. On the other hand, $\lambda_{2c-g-2} - d = 2c-2-d \geq c$ because $c \geq d+2$. Consequently $\lambda_{2c-g-2} - d \in \Lambda$ and $\tau_{2c-g-2} = \lambda^{-1}(d) = c - g - 1$. Similarly, the largest non-gap which is at most $\lambda_{2c-g-1}/2$ is d and $\lambda_{2c-g-1} - d = 2c - 1 - d \in \Lambda$. So, $\tau_{2c-g-1} = c - g - 1$.
(2) If $c = 3$ then $g = 2$ and $\lambda_{(2c-g-2)-2} = \lambda_0$ and $\tau_{(2c-g-2)-2} = 0 = c-g-1$. Assume $c \geq 4$. If $d = c-2$ then $\lambda_{(2c-g-2)-2} = 2c-4 = 2d$, so $\tau_{(2c-g-2)-2} = \lambda^{-1}(d) = c-g-1$. If $d = c-3$ then $\lambda_{(2c-g-2)-1} = 2c-3 = d+c$, so $\tau_{(2c-g-2)-1} = \lambda^{-1}(d) = c-g-1$. Suppose now $d \leq c - 4$. In this case $\lambda_{(2c-g-2)-2}/2 = c - 2$, which is between d and c, and $\lambda_{(2c-g-2)-2} - d = 2c - 4 - d \geq c$. So $\lambda_{(2c-g-2)-2} - d \in \Lambda$. This makes $\tau_{(2c-g-2)-2} = \lambda^{-1}(d) = c - g - 1$. □

Statement 1 of Lemma 10 for the case when $i > 0$ is a direct consequence of Theorem 9 and [10, Theorem 3.8] which states that $\nu_i = i - g + 1$ for $i \geq 2c - g - 1$.

Finally, Theorem 9 together with Lemma 10 has the next corollary, which was already stated with other proofs in [1,4]. Here the proof has been simplified due to the use of the τ-sequence. The importance of the result is that it shows that the improved codes correcting generic errors do always require at most as many checks as the Feng–Rao improved codes correcting any kind of errors. It also states conditions under which their redundancies are equal and characterizes Arf semigroups as the unique semigroups for which there is no improvement.

Corollary 11 (1) $\widetilde{R}^*(t) \subseteq \widetilde{R}(t)$ *for all* $t \in \mathbb{N}_0$.
(2) $\widetilde{R}^*(t) = \widetilde{R}(t)$ *for all* $t \geq c - g$.
(3) $\widetilde{R}^*(t) = \widetilde{R}(t)$ *for all* $t \in \mathbb{N}_0$ *if and only if the associated numerical semigroup is Arf.*

Proof Statements 1 and 3 follow immediately from Theorem 9 and the fact that $\widetilde{R}(t) = \{i \in \mathbb{N}_0 : \left\lfloor \frac{\nu_i - 1}{2} \right\rfloor < t\}$ and $\widetilde{R}^*(t) = \{i \in \mathbb{N}_0 : \tau_i < t\}$. For statement 2., we can use that for $i \geq 2c - g - 1$, $\tau_i = \lfloor \frac{\nu_i - 1}{2} \rfloor$ (Theorem 9) and that for $i \geq 2c - g - 1$, $\tau_i \geq c - g - 1$ (Lemma 10), being $c - g - 1$ the largest value of τ_j before it starts being non-decreasing (Proposition 6). □

5 Characterization of a numerical semigroup by its τ sequence

In this section we show that a numerical semigroup is determined by its τ sequence. An analogous result for the ν sequence can be found in [2, Theorem 8.1].

Lemma 12 *The trivial semigroup is the unique numerical semigroup with* τ *sequence equal to* $0, 0, 1, 1, 2, 2, 3, 3, 4, 4, 5, 5, \ldots$.

Proof It is enough to check that for any other numerical semigroup there is a value in the τ sequence that appears at least three times. If $c = 2$ then $\tau_0 = \tau_1 = \tau_2 = 0$. If $c > 2$, by Lemma 10, $\tau_{2c-g-2} = \tau_{2c-g-1}$ and they are equal to at least one of τ_{2c-g-3} and τ_{2c-g-4}. □

Theorem 13 *The* τ *sequence of a numerical semigroup determines it.*

Proof Let k be the minimum integer such that $\tau_{k+2i} = \tau_{k+2i+1}$ and $\tau_{k+2i+2} = \tau_{k+2i+1} + 1$ for all $i \in \mathbb{N}_0$. If $k = 0$, by Lemma 12, $\Lambda = \mathbb{N}_0$. Assume $k > 0$.

By Lemma 10, if $c > 2$, $k = 2c - g - 2$ and $\tau_k = c - g - 1$. So,

$$\begin{cases} c = k - \tau_k + 1 \\ g = k - 2\tau_k \end{cases}$$

This result can be extended to the case $c = 2$ since in this case $c = 2$, $g = 1$, $k = 1$ and $\tau_k = 0$.

This determines $\lambda_i = i + g$ for all $i \geq c - g$. Now we can determine λ_{c-g-1}, λ_{c-g-2}, and so on using that the smallest j for which $\tau_j = i$ corresponds to $\lambda_j = 2\lambda_i$. That is, $\lambda_i = \frac{1}{2}\min\{\lambda_j : \tau_j = i\}$. □

We have just seen that any numerical semigroup is uniquely determined by its τ sequence. The next proposition shows that no finite subset of τ can determine the numerical semigroup. This result is analogous to [3, Proposition 2.2.]. In this case it refers to the ν sequence instead of the τ sequence.

Proposition 14 *Let r be a positive integer. Let Λ be a numerical semigroup with enumeration λ and let m be an integer with $m \geq 2$. Define the semigroup $\Lambda' = m\Lambda \cup \{i \in \mathbb{N}_0 \mid i \geq m\lambda_r\}$ and let τ^{Λ} and $\tau^{\Lambda'}$ be the τ sequence corresponding to Λ and Λ' respectively. Then $\tau_i^{\Lambda'} = \tau_i^{\Lambda}$ for all $i \leq r$ and $\Lambda' \neq \Lambda$.*

Proof It is obvious that $\Lambda' \neq \Lambda$. Let λ' be the enumeration of Λ'. For all $i \leq r$, $\lambda'_i = m\lambda_i$. In particular, if $j \leq i \leq r$, then it exists k with $j \leq k \leq i$ and $\lambda_j + \lambda_k = \lambda_i$ if and only if it exists k with $j \leq k \leq i$ and $\lambda'_j + \lambda'_k = \lambda'_i$. Hence, by the definition of the τ sequence, $\tau_i^{\Lambda'} = \tau_i^{\Lambda}$. □

As a consequence of Proposition 14, although the sequence τ of a numerical semigroup uniquely determines it, any subset $(\tau_i)_{0 \leq i \leq r-1}$ is exactly the set of the first r values of the τ sequence of infinitely many semigroups. In fact, by varying m among the positive integers, we get an infinite set of semigroups, all of them sharing the first r values in the τ sequence.

Acknowledgment This work was partly supported by the Spanish Government through projects CONSOLIDERINGENIO 2010 CSD2007-00004 "ARES" and TSI2007-65406-C03-01 "E-AEGIS", and by the Government of Catalonia under Grant 2005 SGR 00446. The author would like to thank Anna de Mier for her careful reading and for her suggestion to simplify the proof of Theorem 9.

References

1. Bras-Amorós M.: 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, pp. 204–215. Springer, Berlin (2003).
2. Bras-Amorós M.: Acute semigroups, the order bound on the minimum distance, and the Feng-Rao improvements. IEEE Trans. Inform. Theory **50**(6), 1282–1289 (2004).
3. Bras-Amorós M.: A note on numerical semigroups. IEEE Trans. Inform. Theory **53**(2), 821–823 (2007).
4. Bras-Amorós M., O'Sullivan M.E.: The correction capability of the Berlekamp-Massey-Sakata algorithm with majority voting. Appl. Algebra Engrg. Comm. Comput. **17**(5), 315–335 (2006).
5. Campillo A., Farrán J.I., Munuera C.: On the parameters of algebraic-geometry codes related to Arf semigroups. IEEE Trans. Inform. Theory **46**(7), 2634–2638 (2000).
6. Feng G.L., Rao T.R.N.: A simple approach for construction of algebraic-geometric codes from affine plane curves. IEEE Trans. Inform. Theory **40**(4), 1003–1012 (1994).
7. Feng G.-L., Rao T.R.N.: Improved geometric Goppa codes. I. Basic theory. IEEE Trans. Inform. Theory **41**(6, part 1), 1678–1693 (1995). Special issue on algebraic geometry codes.
8. Hansen J.P.: Dependent rational points on curves over finite fields—Lefschetz theorems and exponential sums. In: International Workshop on Coding and Cryptography (Paris, 2001). Electron. Notes Discrete Math., vol. 6, pp. 13 (electronic). Elsevier, Amsterdam (2001).
9. Høholdt T., van Lint J.H., Pellikaan R.: Algebraic geometry of codes. In: Handbook of Coding Theory, vols. I, II, pp. 871–961. North-Holland, Amsterdam (1998).
10. Kirfel C., Pellikaan R.: The minimum distance of codes in an array coming from telescopic semigroups. IEEE Trans. Inform. Theory **41**(6, part 1), 1720–1732 (1995). Special issue on algebraic geometry codes.
11. Munuera C., Torres F.: A note on the order bound on the minimum distance of AG codes and acute semigroups. Adv. Math. Commun. **2**(2), 175–181 (2008).
12. O'Sullivan M.E.: A generalization of the Berlekamp-Massey-Sakata algorithm. Unpublished article (2001).
13. Pellikaan R., Torres F.: On Weierstrass semigroups and the redundancy of improved geometric Goppa codes. IEEE Trans. Inform. Theory **45**(7), 2512–2519 (1999).