symmetry

MDPI

Article

Ideals of Numerical Semigroups and Error-Correcting Codes

Maria Bras-Amorós

Department of Computer Science and Mathematics, Universitat Rovira i Virgili, 43007 Tarragona, Catalonia, Spain; maria.bras@urv.cat

Received: 8 October 2019; Accepted: 11 November 2019; Published: 14 November 2019

Abstract: Several results relating additive ideals of numerical semigroups and algebraic-geometry codes are presented. In particular, we deal with the set of non-redundant parity-checks, the code length, the generalized Hamming weights, and the isometry-dual sequences of algebraic-geometry codes from the perspective of the related Weierstrass semigroups. These results are related to cryptographic problems such as the wire-tap channel, t-resilient functions, list-decoding, network coding, and ramp secret sharing schemes.

Keywords: numerical semigroup; Weierstrass semigroup; semigroup ideal; error-correcting code; algebraic-geometry code

1. Introduction

In a previous survey chapter [1], numerical semigroups were presented together with some of the related classical problems, and their importance for algebraic-geometry codes was explained. In particular, numerical semigroups can be used to establish decoding conditions, are useful to define bounds for the minimum distance of codes, and to improve the code dimension. In this contribution, which is a continuation of that chapter, we will present some results relating ideals of numerical semigroups and the set of non-redundant parity-checks, the code length, the generalized Hamming weights, and the isometry-dual sequences of algebraic-geometry codes. The reader not familiar with algebraic geometry may be interested in the introductory sections of [1].

The organization of this contribution is as follows. Section 2 introduces numerical semigroups and states basic notions, in particular the Frobenius number and symmetric semigroups, which will be important in the following sections. Section 3 presents ideals of numerical semigroups and some results connecting the maximum gap of an ideal with the size of the complement of the ideal. Maximum sparse ideals are defined as those ideals for which this maximum gap is maximum restricted to a given size of the complement, and this connects with symmetric semigroups. Section 4 presents one-point algebraic-geometry codes and relates redundant checks with ideals of numerical semigroups. Section 5 deals with the Geil–Matsumoto bound for the number of points a curve can have and so with the length of codes. Section 6 deals with the sequences of one-point algebraic-geometry codes that satisfy the isometry-dual property and the effects of puncturing such sequences. The results are derived from the results on maximum sparse ideals of numerical semigroups. Section 7 deals with the generalized Hamming weights of algebraic-geometry codes by means of Feng–Rao numbers and Weierstrass semigroups. These results are related to cryptographic problems such as the wire-tap channel or ramp secret sharing schemes.

2. Numerical Semigroups

2.1. Basic Notions

A *numerical semigroup* is a subset Λ of $\mathbb{N}_0$ that contains 0, contains any finite sum of its elements, and its complement in $\mathbb{N}_0$ is finite. Weierstrass semigroups are indeed numerical semigroups.

The *genus* of a numerical semigroup Λ is the amount $g = \#(\mathbb{N}_0 \setminus \Lambda)$. The elements belonging to the semigroup Λ are its *non-gaps* while the positive elements in its complement are its *gaps*. There is a unique increasing bijective map $\lambda : \mathbb{N}_0 \longrightarrow \Lambda$. We call it the *enumeration* of Λ, and the notation λ_i will be used for $\lambda(i)$.

The *generators* of a semigroup are those nonzero elements in the semigroup that are not the result of adding two other nonzero elements in the semigroup. The whole set of generators is necessarily finite and coprime. Conversely, if a finite set G of positive integers is coprime, the set of finite sums of the elements in G is called the *semigroup generated* by G and it is denoted by $\langle G \rangle$.

2.2. Frobenius Number and Symmetric Semigroups

The *conductor* of a numerical semigroup Λ is the least integer in the semigroup for which all integers larger than it belong to the semigroup. The conductor minus one is then the maximum gap of the numerical semigroup, which is called the *Frobenius number* of the semigroup. It can be easily proved using the Pigeonhole Principle that the conductor is at most twice the genus. The semigroups that attain this bound are called *symmetric semigroups*. The symmetry of a semigroup Λ comes from the fact that, if the Frobenius number F and the genus g of the semigroup satisfy $F = 2g - 1$, then the semigroup satisfies $i \in \Lambda \iff F - i \notin \Lambda$.

2.3. Semigroups Generated by Two Integers

Weierstrass semigroups generated by two integers are very common as is the case in hyperelliptic curves or Geil's norm-trace curves [2]. Most important, for any coprime positive integers a and b, one can find a curve with a point whose Weierstrass semigroup is $\langle a, b \rangle$ [3].

Sylvester's formula [4] states that the Frobenius number of the semigroup $\langle a, b \rangle$ is $ab - a - b$, while its genus is $\frac{(a-1)(b-1)}{2}$. Hence, semigroups generated by two positive integers satisfy the symmetry property.

Example 1 (Hermitian curve $\mathcal{H}_q$)**.** *Let q be a prime power. The Hermitian curve $\mathcal{H}_q$ over $\mathbb{F}_{q^2}$ is defined by the affine equation $x^{q+1} = y^q + y$ and homogeneous equation $X^{q+1} - Y^q Z - Y Z^q = 0$. The point $P_\infty = (0 : 1 : 0)$ is the unique point of $\mathcal{H}_q$ at infinity. It can be proved (see, for instance, [1]) that $v_{P_\infty}(\frac{Z}{Y}) = q + 1$ and $v_{P_\infty}(\frac{X}{Z}) = -q$. Hence, the Weierstrass semigroup Λ at P_∞ contains the semigroup generated by $q, q + 1$ whose complement in $\mathbb{N}_0$ has $\frac{q(q-1)}{2} = g$ elements. Since we know that the complement of Λ in $\mathbb{N}_0$ also has g elements, this means that both semigroups are the same. For further details on the Hermitian curve, see [3,5].*

3. Ideals of Numerical Semigroups

3.1. Ideals

A subset I of a numerical semigroup Λ is an *ideal* of Λ if $I + \Lambda \subseteq I$. We say that I is a *proper* ideal of Λ if $I \neq \Lambda$. Because of the finiteness of the complement of Λ and the definition of an ideal, the complement of an ideal (either with respect to the ideal or with respect to $\mathbb{N}_0$) must be finite as well. Hence, we can consider the largest integer in the complement of an ideal (with respect to $\mathbb{N}_0$). It is called the *Frobenius number* of the ideal.

Next, we will prove an upper bound on the Frobenius number of an ideal which extends the upper bound for the Frobenius number of a numerical semigroup that is twice the genus minus one. Indeed, we will see that the Frobenius number of an ideal is less than or equal to the number of elements in

the semigroup which do not belong to the ideal plus the double of the genus of the semigroup minus one. Notice that, if we take the ideal to be the whole semigroup, then we get the already known bound for the Frobenius number of a numerical semigroup. Hence, this result, stated in Theorem 1, can be seen as a generalization of the upper bound for the Frobenius number of the numerical semigroup. The ideals for which the Frobenius number attains the bound are called *maximum sparse* ideals. All the results in this section were first proved in [6].

3.2. The Frobenius Number of an Ideal

Suppose that Λ is a numerical semigroup and that I is an ideal of Λ. The *difference* of the ideal I with respect to Λ is the number of elements in $\Lambda \setminus I$. One can prove (see [3], Lemma 5.15) that, in the case of principal ideals, that is, ideals of the form $a + \Lambda$ for some nonnegative integer a, the difference is exactly a. From this, it is straightforward to deduce that the Frobenius number of $a + \Lambda$ is less than or equal to twice the genus of the semigroup plus a (which is the difference) minus one. This will be generalized to the bound in Theorem 1 for any ideal. Furthermore, the semigroups for which the bound is attained will be characterized.

3.3. Upper Bounding the Frobenius Number of an Ideal

For each nonnegative integer i, define $D(i) = \{\lambda_j \leq \lambda_i : \lambda_i - \lambda_j \in \Lambda\}$. The set $D(i)$ is often called the set of divisors of λ_i, and its cardinality is denoted $\nu_i = \#D(i)$. The sequence ν_i has many implications in coding theory. It is fundamental in the computation of bounds for the minimum distance of algebraic-geometry codes based on a single point as well as in the optimization of the redundancy of those codes. Its properties and applications can be seen in [7–14] and in the survey [1]. As a curiosity, it was proved in [7,15] that the set of elements of a numerical semigroup is determined by its ν sequence. However, it was proved in [8] that, given a finite subset of values of the ν sequence, it is contained in the ν sequence of infinitely many numerical semigroups. We will see how the sets $D(i)$ are related to ideals of semigroups. Next, we present two lemmas proved by Barucci in [16] and by Høholdt, van Lint, and Pellikaan in [3], respectively, and the main theorem that can be derived from the two lemmas.

Lemma 1 ([16]). *Every ideal of a numerical semigroup Λ can be expressed as an intersection of finitely many irreducible ideals and irreducible ideals are expressible as $\Lambda \setminus D(i)$ for some i.*

Lemma 2 (([3] Theorem 5.24)). *Let $g(i)$ be the number of gaps in the interval from 1 to $\lambda_i - 1$ and let $G(i)$ be the number of pairs of gaps whose sum equals λ_i. Then, $\nu_i = i - g(i) + G(i) + 1$.*

Theorem 1. *Suppose that I is an ideal of a numerical semigroup of genus g so that $\Lambda \setminus I$ has d elements. Then, $d + 2g + i \in I$ for all $i \geq 0$. Equivalently, the Frobenius number of I is less than or equal to $d + 2g - 1$.*

Proof. It is straightforward to see that the intersection of two ideals satisfying the result also satisfies the result. Now, by Lemma 1, it will be enough to show that the result holds for the ideals expressible as $I = \Lambda \setminus D(i)$. Equivalently, $\nu_i + 2g \geq \max\{c, \lambda_i + 1\}$, with c the conductor of Λ. This holds if $c \geq \lambda_i + 1$ since $c \leq 2g$. Otherwise, if $\lambda_i + 1 > c$, then $g(i) = g$, $\lambda_i = i + g$, and as a consequence of Lemma 2, $\nu_i + 2g = (i - g + G(i) + 1) + 2g = i + g + 1 + G(i) = \lambda_i + 1 + G(i) \geq \lambda_i + 1$. □

The ideals for which the Frobenius number attains the previous bound will be called *maximum sparse* ideals.

3.4. Maximum Sparse Ideals

In next theorem, we characterize the ideals that are maximum sparse.

Theorem 2. *The statements that follow are equivalent for an ideal I with difference $d > 0$ of a semigroup Λ with genus g:*

1. *The Frobenius number of the ideal I equals $d + 2g - 1$.*
2. *$I = \Lambda \setminus D(i)$ for some i such that $G(i) = 0$.*

Proof. On one hand, let the Frobenius number of the ideal I be $d + 2g - 1$. If I is a non-trivial intersection of the ideals I' and I'', whose differences are, respectively, d' and d'', then the difference d of I is strictly larger than both d' and d''. If $d + 2g - 1$ is not an element of I, then it is neither an element of I' nor an element of I'', but the value $d + 2g - 1$ is strictly larger than both $d' + 2g - 1$ and $d'' + 2g - 1$. This contradicts Theorem 1. This implies, by Lemma 1, that I is of the form $\Lambda \setminus D(i)$ for some i. Now, $d = v_i$ because $I = \Lambda \setminus D(i)$. If λ_i is smaller than c, then $v_i + 2g - 1 \geq = 2g \geq c$, hence $d + 2g - 1 \in I$, contradicting our assumption. Consequently, $\lambda_i \geq c$ and by Lemma 2, $v_i = i - g + G(i) + 1$. Thus, $d + 2g - 1 = i + g + G(i) = \lambda_i + G(i)$. However, $d + 2g - 1 \notin I$, and so $G(i) = 0$.

On the other hand, suppose I is of the form $\Lambda \setminus D(i)$ for some i with $G(i) = 0$, and so $d = v_i$. By the former remarks, since $G(i) = 0$, one deduces that $\lambda_i = i + g$ and, by Lemma 2, it follows that $d + 2g - 1 = \lambda_i \notin I$. □

Example 2 (Weierstrass semigroup of $\mathcal{H}_4$)**.** *The Weierstrass semigroup of $\mathcal{H}_4$ is $\Lambda = \{0, 4, 5, 8, 9, 10, 12, 13, \dots\}$. We wish to find all the maximum sparse ideals of Λ. Since the Frobenius number of Λ is 11 and $11 + 11 = 22 = \lambda_{16}$, it holds that $G(16) > 0$ while $G(i) = 0$ for all $i \geq 17$. This implies that all ideals of the form $\Lambda \setminus D(i)$ with $i \geq 17$ are maximum sparse. Let us see now whether $G(i) = 0$ for all i with $6 \leq i \leq 15$. On one hand, $G(6) > 0$ since $\lambda_6 = 12 = 11 + 1$; $G(7) > 0$ since $\lambda_7 = 13 = 11 + 2$; $G(8) > 0$ since $\lambda_8 = 14 = 11 + 3$; $G(9) = 0$ because the difference between 15 and any gap is a non-gap, indeed, $\{15 - 1 = 14, 15 - 2 = 13, 15 - 3 = 12, 15 - 6 = 9, 15 - 7 = 8, 15 - 11 = 4\} \subseteq \Lambda$; $G(10) = 0$ because the difference between 16 and any gap is a non-gap, indeed, $\{16 - 1 = 15, 16 - 2 = 14, 16 - 3 = 13, 16 - 6 = 10, 16 - 7 = 9, 16 - 11 = 5\} \subseteq \Lambda$; $G(11) > 0$ since $\lambda_{11} = 17 = 11 + 6$; $G(12) > 0$ since $\lambda_i = 18 = 11 + 7$; $G(13) = 0$ because the difference between 19 and any gap is a non-gap, indeed, $\{19 - 1 = 18, 19 - 2 = 17, 19 - 3 = 16, 19 - 6 = 13, 19 - 7 = 12, 19 - 11 = 8\} \subseteq \Lambda$. $G(14) = 0$ because the difference between 20 and any gap is a non-gap, indeed, $\{20 - 1 = 19, 20 - 2 = 18, 20 - 3 = 17, 20 - 6 = 14, 20 - 7 = 13, 20 - 11 = 9\} \subseteq \Lambda$. $G(15) = 0$ because the difference between 21 and any gap is a non-gap, indeed, $\{21 - 1 = 20, 21 - 2 = 19, 21 - 3 = 18, 21 - 6 = 15, 21 - 7 = 14, 21 - 11 = 10\} \subseteq \Lambda$.*

Hence, all maximum sparse ideals are $I_9 = \Lambda \setminus D(9) = \{4, 8, 9, 12, 13, 14, 16, 17, 18, 19, 20, 21, 22, \dots\}$, where $D(9) = \{0, 5, 10, 15\}$, $d = 4$, and $d + 2g - 1 = 15$; $I_{10} = \Lambda \setminus D(10) = \{5, 9, 10, 13, 14, 15, 17, 18, 19, 20, 21, 22, \dots\}$, where $D(10) = \{0, 4, 8, 12, 16\}$, $d = 5$, and $d + 2g - 1 = 16$; $I_{13} = \Lambda \setminus D(13) = \{8, 12, 13, 16, 17, 18, 20, 21, 22, \dots\}$, where $D(13) = \{0, 4, 5, 9, 10, 14, 15, 19\}$, $d = 8$, and $d + 2g - 1 = 19$; $I_{14} = \Lambda \setminus D(14) = \{9, 13, 14, 17, 18, 19, 21, 22, \dots\}$, where $D(14) = \{0, 4, 5, 8, 10, 12, 15, 16, 20\}$, $d = 9$, and $d + 2g - 1 = 20$; $I_{15} = \Lambda \setminus D(15) = \{10, 14, 15, 18, 19, 20, 22, \dots\}$, where $D(15) = \{0, 4, 5, 8, 9, 12, 13, 16, 17, 21\}$, $d = 10$, and $d + 2g - 1 = 21$; $I_{17} = \Lambda \setminus D(17) = \{12, 16, 17, 20, 21, 22, 24, \dots\}$, where $D(17) = \{0, 4, 5, 8, 9, 10, 13, 14, 15, 18, 19, 23\}$, $d = 12$, and $d + 2g - 1 = 23$; and finally $\Lambda \setminus D(i)$ for all $i > 17$. Here, $D(i) = \{0, 4, 5, 8, 9, 10, 12, 13, \dots, i + 6 - 12, i + 6 - 10, i + 6 - 9, i + 6 - 8, i + 6 - 5, i + 6 - 4, i + 6\}$, $d = i - 5$, and $d + 2g - 1 = i + 6$.

The next corollary characterizes maximum sparse ideals of symmetric semigroups.

Corollary 1. *Maximum sparse ideals of a symmetric semigroup are exactly the principal ideals of the semigroup.*

Proof. It has already been explained that the difference of the principal ideal $a + \Lambda$ is exactly a, and so it is obvious that principal ideals of symmetric semigroups are maximum sparse.

Suppose now that I is a maximum sparse ideal of a symmetric semigroup Λ. If $I = \Lambda$, the result is obvious. Otherwise, by Theorem 2, $I = \Lambda \setminus D(i)$ for some i with $G(i) = 0$. Let a be the minimum

element of I. Since $I = \Lambda \setminus D(i)$, the difference $\lambda_i - a$ is a gap of Λ. By the minimality of a, the gap $\lambda_i - a$ must be the Frobenius number F of Λ since, otherwise, $\lambda_i - F$ would be an element in Λ (because $G(i) = 0$) not in $D(i)$ and, so, an element of I smaller than a. Now, it remains to see that any element $\mu \in \Lambda \setminus D(i)$ belongs to $a + \Lambda$. Indeed, $\mu - a = \mu - (\lambda_i - F) = F - (\lambda_i - \mu)$. Since $\mu \notin D(i)$, we have $(\lambda_i - \mu) \notin \Lambda$ and, by the symmetry of Λ, we have $F - (\lambda_i - \mu) \in \Lambda$. Thus, $\mu - a \in \Lambda$. □

Example 3 (Weierstrass semigroup of $\mathcal{H}_4$)**.** *The Weierstrass semigroup of the point at infinity of $\mathcal{H}_4$ is generated by two integers and so it is symmetric. The previous corollary in this case can be checked for the set of maximum sparse ideals listed in Example 2.*

Remark 1. *It is important to remark that the hypothesis in Corollary 1 is necessary. A counterexample can be found in the semigroup $\Lambda = \{0, 4, 8, 9, \dots\}$, of Frobenius number 7 and genus 6, and so, not symmetric. The semigroup Λ has the ideal $I = \{9, 10, 11, 13, 14, 15, 17, \dots\}$, which equals $\Lambda \setminus D(10) = \Lambda \setminus \{0, 4, 8, 12, 16\}$. The ideal I has difference $d = 5$ and Frobenius number $16 = d + 2g - 1$. Hence, I is a maximum sparse ideal, but it is not principal because it is, indeed, $I = (9 + \Lambda) \cup \{10, 11, 14, 15\}$.*

3.5. The Ideal of Frobenius Numbers of Sparse Ideals

The next lemma shows that the Frobenius numbers of the maximum sparse ideals of a numerical semigroup constitute in turn another ideal of the numerical semigroup.

Lemma 3. *The nonzero non-gaps λ_i such that $G(i) = 0$ constitute an ideal L of Λ.*

Proof. First of all, notice that $G(i) = 0$ is not satisfied if λ_i is smaller than the conductor. Indeed, if λ_i is smaller than the conductor c, then there must be a gap a smaller than λ_i with $\lambda_i - a < \lambda_1$, since, otherwise, λ_i would not be smaller than the conductor. Now, $\lambda_i - a$ must be a positive gap and $\lambda_i = (\lambda_i - a) + a$, a contradiction with $G(i) = 0$. Hence, the elements in L are equal than or equal to the conductor of Λ.

It remains to show that, if $\lambda_i \in L$, then $\lambda_i + \lambda_j \in L$ for any $\lambda_j \in \Lambda$. Assume that $\lambda_j \neq 0$. Let k be such that $\lambda_i + \lambda_j = \lambda_k$. Suppose that $\lambda_k \notin L$, that is, $G(k) \neq 0$. Then, there are two gaps a, a' with $\lambda_k = a + a'$. Note that both $a, a' < \lambda_i = \lambda_k - \lambda_j$ since λ_i is greater than or equal to c. From $a + a' = \lambda_k$, we have $\lambda_j < a, a' < \lambda_i$. Then, $a - \lambda_j$ does not belong to Λ because, otherwise, $a = \lambda_j + (a - \lambda_j) \in \Lambda + \Lambda \subseteq \Lambda$. In particular, $(a - \lambda_j) + a'$ is a sum of two gaps equal to $a + a' - \lambda_j = \lambda_k - \lambda_j = \lambda_i$, a contradiction with $G(i) = 0$. □

4. One-Point Algebraic-Geometry Codes

In coding theory, by a *linear code* of length n, it is meant a linear subspace C of $\mathbb{F}_q^n$, with $\mathbb{F}_q$ the field of order q, for some prime power q. Its dimension is usually denoted k. The *dual code* of a linear code is its orthogonal space. It has the same length than C and dimension $n - k$. A knowledge of the dual code is useful in most decoding algorithms. To compare two different vectors of $\mathbb{F}_q^n$, one counts the number of differing positions and this number is referred to as the *Hamming distance* between the two vectors. The *weight* of a vector is defined as its Hamming distance to the all-zero vector. An important parameter of a code is its *minimum distance*, representing the minimum of the Hamming distances between each pair of different vectors in the code. The *correction capability* of a code tells how far we can go from any code vector with the guarantee that we will not get closer to a code vector different than the originary one. The correction capability is exactly $\lfloor \frac{d-1}{2} \rfloor$ if the minimum distance of the code is d.

An important class of error-correcting codes are the algebraic-geometry codes. Let $\mathcal{X}$ be a smooth irreducible algebraic curve over $\mathbb{F}_q$ and let Q be a rational point of $\mathcal{X}$. Let Λ be the Weierstrass semigroup at Q and let $A = \bigcup_{m \geq 0} L(mQ)$ be the ring of rational functions of $\mathcal{X}$ only having poles at Q. There exists a basis $z_0, z_1, \dots, z_i, \dots$ of A such that $v_Q(z_i) = -\lambda_i$. Now, for each collection

of rational points $P_1, \ldots, P_n$, all of them different from Q, and each set of indices $B \subseteq \mathbb{N}_0$, define the *one-point* code $C_B =< (z_i(P_1), \ldots, z_i(P_n)) : i \in B >$. The elements in the set B are called *parity checks* of C_B and the one-point code is said to be classical if $B = \{0, 1, \ldots, m\}$. We will use C_m to refer to $C_{\{0,\ldots,m\}}$. In the present survey, we consider only the codes C_m. Ref. [1] is a survey on results related to the minimum distance, the error-correction capability, and the redundancy of the codes C_B from the perspective of Weierstrass semigroups. In that case we considered, though, the dual codes $< (z_i(P_1), \ldots, z_i(P_n)) : i \in B >^{\perp}$.

It can be shown that $C_m = \{(f(P_1), \ldots, f(P_n)) : f \in L(\lambda_m Q)\}$. Note that it can be the case that $C_m = C_{m-1}$. The next lemma is stated in other words in ([17], Corollary 3.3).

Lemma 4. *Suppose that Λ is the Weierstrass semigroup at a rational point Q and define $\Lambda^* = \{0\} \cup \{m \in \mathbb{N}, m > 0 : C_m \neq C_{m-1}\} = \{m_0 = 0, m_1, \ldots, m_n\}$. Then, the set $\Lambda \setminus \Lambda^*$ is an ideal of Λ.*

5. Ideals and the Length of Algebraic-Geometry Codes

From the previous definition of algebraic-geometry codes, we see that the length of a code defined over an algebraic smooth irreducible curve is conditioned by the number of points of the curve. Thus, bounding the number of points of smooth irreducible curves becomes an important problem of algebraic-geometry codes.

5.1. The Geil–Matsumoto Bound

Define $N_q(g)$ as the maximum number of points an irreducible smooth curve of genus g can have over the finite field of q elements. The Hasse–Weil bound is $|N_q(g) - q - 1| \leqslant 2g\sqrt{q}$ ([18], Theorem V.2.3), which is refined by Serre's bound $|N_q(g) - q - 1| \leqslant g\lfloor 2\sqrt{q} \rfloor$ ([18], Theorem V.3.1). The web page [19] is devoted to give the best known examples of curves with many points for any fixed pair q, g.

Suppose that, for an irreducible smooth curve $\mathcal{X}$ over $\mathbb{F}_q$, we not only know its genus but also the Weierstrass semigroup Λ at a given point. We may wonder, with this assumption, how many points $\mathcal{X}$ can have. For this goal, we define $N_q(\Lambda)$ to be the maximum number of possible points. The first bound is due to Lewittes [20], and it uses only the first element λ_1 of Λ different than 0. It is $N_q(\Lambda) \leqslant L_q(\Lambda) := q\lambda_1 + 1$. On the other hand, Geil and Matsumoto [21] proved that

$$N_q(\Lambda) \leqslant GM_q(\Lambda) := \#(\Lambda \setminus \cup_{\lambda_i \text{ generator of } \Lambda}(q\lambda_i + \Lambda)) + 1. \tag{1}$$

Using the fact that

$$\#(\Lambda \setminus (q\lambda_1 + \Lambda)) = q\lambda_1, \tag{2}$$

proved in [3,21], one can deduce Lewittes' bound from the Geil–Matsumoto bound.

Remark 2. *The set $\Lambda \setminus \cup_{\lambda_i \text{ generator of } \Lambda}(q\lambda_i + \Lambda)$ is the complement of an ideal of Λ. Hence, any advance in the comprehension of ideals of numerical semigroups may result in new bounds for the length of algebraic-geometry codes.*

For a numerical semigroup generated by two coprime integers a, b, it can be proved [22] that the Geil–Matsumoto bound is exactly as follows:

$$GM_q(\langle a, b \rangle) = \sum_{n=0}^{a-1} \min\left(q, \left\lceil \frac{q-n}{a} \right\rceil \cdot b\right) + 1 \tag{3}$$

$$= \begin{cases} qa + 1 & \text{if } q \leqslant \lfloor \frac{q}{a} \rfloor b, \\ (q \bmod a)q + (a - (q \bmod a))\lfloor \frac{q}{a} \rfloor b + 1 & \text{if } \lfloor \frac{q}{a} \rfloor b < q \leqslant \lceil \frac{q}{a} \rceil b, \\ ab\lceil \frac{q}{a} \rceil - (a - (q \bmod a))b + 1 & \text{if } q > \lceil \frac{q}{a} \rceil b. \end{cases} \tag{4}$$

5.2. Coincidences of Lewittes's and the Geil–Matsumoto Bound

It was proved by Beelen and Ruano in ([23], Proposition 9) that, if $q \in \Lambda$, then the Lewittes and the Geil–Matsumoto bounds coincide. For two-generated semigroups, Equation (3) implies that both bounds coincide if and only if $q \leqslant \lfloor \frac{q}{a} \rfloor b$. Otherwise, the Lewittes bound is improved by the Geil–Matsumoto bound. This result for two-generated semigroups can be generalized to semigroups of any number of generators (larger than or equal to two). This is the goal of this subsection. The results are taken from [22].

Theorem 3. *Let $\Lambda = \langle \lambda_1, \ldots, \lambda_n \rangle$ with $\lambda_1 < \lambda_i$ for all $i > 1$. The next statements are equivalent*

1. $GM_q(\Lambda) = L_q(\Lambda)$;
2. $\Lambda \setminus \cup_{i=1}^{n}(q\lambda_i + \Lambda) = \Lambda \setminus (q\lambda_1 + \Lambda)$;
3. $q(\lambda_i - \lambda_1) \in \Lambda$ *for all* $i > 1$.

Proof. By Equation (2), it is straightforward to prove that 2 implies 1. The reverse implication follows from the inclusion $\Lambda \setminus \cup_{i=1}^{n}(q\lambda_i + \Lambda) \subseteq \Lambda \setminus (q\lambda_1 + \Lambda)$ and the equality $GM_q(\Lambda) = L_q(\Lambda)$, which, by Equation (2), implies that $\#(\Lambda \setminus \cup_{i=1}^{n}(q\lambda_i + \Lambda)) = \#(\Lambda \setminus (q\lambda_1 + \Lambda))$.

For the equivalence of the last two statements, notice that $q(\lambda_i - \lambda_1) \in \Lambda$ for all $i > 1 \iff q\lambda_i \in q\lambda_1 + \Lambda$ for all $i > 1 \iff q\lambda_i + \Lambda \subseteq q\lambda_1 + \Lambda$ for all $i > 1 \iff \Lambda \setminus \cup_{i=1}^{n}(q\lambda_i + \Lambda) = \Lambda \setminus (q\lambda_1 + \Lambda)$. □

Notice that Theorem 3 implies Beelen–Ruano's result since $q \in \Lambda$ implies $q(\lambda - \lambda_1) \in \Lambda$ for all $\lambda \in \Lambda$.

From Theorem 3, it makes sense to analyze the conditions under which $q(\lambda_i - \lambda_1) \in \Lambda$ for some $i > 1$. Notice that, if $\gcd(\lambda_1, \lambda_i) = d$, then $\{x\lambda_1 + y\lambda_i : x, y \in \mathbb{N}_0\} = d\langle \frac{\lambda_1}{d}, \frac{\lambda_i}{d} \rangle$, where, by $d\langle \frac{\lambda_1}{d}, \frac{\lambda_i}{d} \rangle$, we mean the set $\{d\lambda : \lambda \in \langle \frac{\lambda_1}{d}, \frac{\lambda_i}{d} \rangle\}$. Obviously, $d\langle \frac{\lambda_1}{d}, \frac{\lambda_i}{d} \rangle \subseteq \Lambda$. The next lemma is proved in [22].

Lemma 5. *If $\gcd(\lambda_1, \lambda_i) = d$, then $q(\lambda_i - \lambda_1) \in d\langle \frac{\lambda_1}{d}, \frac{\lambda_i}{d} \rangle$ if and only if $qd \leqslant \lfloor \frac{qd}{\lambda_1} \rfloor \lambda_i$. In particular, if $q \leqslant \lfloor \frac{q}{\lambda_1} \rfloor \lambda_i$, then $q(\lambda_i - \lambda_1) \in d\langle \frac{\lambda_1}{d}, \frac{\lambda_i}{d} \rangle$.*

Now, one can deduce the next result.

Proposition 1. *Suppose $\lambda_1 < \lambda_2 < \cdots < \lambda_n$ and let $\Lambda = \langle \lambda_1, \lambda_2, \ldots, \lambda_n \rangle$. If $q \leqslant \lfloor \frac{q}{\lambda_1} \rfloor \lambda_2$ then $GM_q(\Lambda) = L_q(\Lambda)$.*

Remark 3. *We have seen that for two-generated semigroups the converse is also true. For semigroups with any number of generators, the converse is not true in general. As a counterexample, let $\Lambda = \langle 5, 7, 18 \rangle = \{0, 5, 7, 10, 12, 14, 15, 17, 18, \ldots\}$ and consider $q = 9$. We have $\Lambda \setminus \cup_{\lambda_i \text{ generator of } \Lambda}(q\lambda_i + \Lambda) = \{0, 5, 7, 10, 12, 14, 15, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 46, 47, 48, 49, 51, 53, 54, 56, 58, 61\} = \Lambda \setminus (q\lambda_1 + \Lambda)$. Hence, $GM_q(\langle 5, 7, 18 \rangle) = 46$, which coincides with $L_q(\langle 5, 7, 18 \rangle)$. Observe though that q, which is 9 is strictly larger than $\lfloor \frac{q}{\lambda_1} \rfloor \lambda_2$, which is 7.*

5.3. Simplified Computation

In [22], it was investigated whether the computation of the number $\Lambda \setminus \cup_{\lambda_i \text{ generator of } \Lambda}(q\lambda_i + \Lambda)$ could be performed as the simpler computation of $\Lambda \setminus \cup_{i \in J}(q\lambda_i + \Lambda)$ for some proper subset of indices $J \subseteq \{1, \ldots, n\}$. This is the purpose of the next lemma.

Lemma 6. *Suppose that $\Lambda = \langle \lambda_1, \ldots, \lambda_n \rangle$ and let $J \subseteq \{1, \ldots, n\}$ be an index subset. The following statements are equivalent*

1. $\Lambda \setminus \cup_{i=1}^{n}(q\lambda_i + \Lambda) = \Lambda \setminus \cup_{i \in J}(q\lambda_i + \Lambda)$;

2. *For all $i \notin J$ there exists $1 \leqslant j \leqslant n$, $j \in J$ such that $q(\lambda_i - \lambda_j) \in \Lambda$.*

The next lemma is a consequence of the previous one.

Lemma 7. *Suppose that $\Lambda = \langle \lambda_1, \ldots, \lambda_n \rangle$, where $\lambda_1 < \lambda_2 < \cdots < \lambda_n$ and suppose that $\lambda_1 < q$.*

1. *If λ_j is the maximum of the generators that are strictly smaller than $\frac{q}{\lfloor \frac{q}{\lambda_1} \rfloor}$, then $\Lambda \setminus \cup_{i=1}^{n}(q\lambda_i + \Lambda) = \Lambda \setminus \cup_{i=1}^{j}(q\lambda_i + \Lambda)$.*
2. *If λ_j is the maximum of the generators that are strictly smaller than $2\lambda_1 - 1$, then $\Lambda \setminus \cup_{i=1}^{n}(q\lambda_i + \Lambda) = \Lambda \setminus \cup_{i=1}^{j}(q\lambda_i + \Lambda)$.*

Proof. The first statement follows directly from Lemma 5 and Lemma 6. To prove the second statement, assume that $q = x\lambda_1 + y$, where $x \geq 1$ and y are integers. Then, $\frac{q}{\lfloor \frac{q}{\lambda_1} \rfloor} = \lambda_1 + \frac{y}{x}$ and the statement is a consequence of the inequalities $x \geqslant 1$ and $y \leqslant \lambda_1 - 1$. □

We call *Geil–Matsumoto generators* those generators that are strictly smaller than $2\lambda_1 - 1$. As follows from the previous results, to compute the Geil–Matsumoto bound, one only needs to subtract the ideals $q\mu + \Lambda$ from Λ for μ a Geil–Matsumoto generator. Because of the fact that, in general, one needs to subtract the ideals $q\lambda + \Lambda$ for *all* generators λ, this gives a computational improvement. In [22], we observed that, although it decreases with the genus, the portion of non-Geil–Matsumoto generators remains still significant for genus 25 with a portion of more than 30%.

We notice that Lemma 7 is a direct consequence of Lemma 6. We leave it as an open research problem to find other consequences of Lemma 6 to find further computational improvements.

6. Ideals and Isometry-Dual Sequences of One-Point Algebraic-Geometry Codes

6.1. Characterization of Isometry-Dual Sequences of Algebraic-Geometry Codes by Means of Sparse Ideals

We say that the codes $C, D \subseteq \mathbb{F}_q^n$ are isometric with respect to x, for $x \in \mathbb{F}_q^n$ if $D = \chi_x(C)$, where χ_x is the map $\chi_x : \mathbb{F}_q^n \to \mathbb{F}_q^n$ defined component-wise by $\chi_x(v) = x * v$. More generally, we say that the sequence $(C^{(i)})_{i=0,\ldots,n}$ of codes satisfies the *isometry-dual condition* if a vector $x \in (\mathbb{F}_q^*)^n$ exists so that $C^{(i)}$ is x-isometric to $\left(C^{(n-i)}\right)^{\perp}$ for every $i = 0, 1, \ldots, n$. Suppose now that $P_1, \ldots, P_n, Q$ are different rational points of a projective, smooth, irreducible curve of genus g and let $C_m = \{(f(P_1), \ldots, f(P_n)) : f \in L(mQ)\}$. As it has been previously stated, if Λ is the Weierstrass semigroup at Q and $\Lambda^* = \{0\} \cup \{m \in \mathbb{N}, m > 0 : C_m \neq C_{m-1}\} = \{m_0 = 0, m_1, \ldots, m_n\}$, then $\Lambda \setminus \Lambda^*$ is an ideal of Λ. Furthermore, Geil, Munuera, Ruano, and Torres proved the next lemma for $n > 2g + 2$ (in a different but equivalent formulation). The strict inequality was improved to a non-strict inequality in [24].

Lemma 8 (([17] Proposition 4.3.)). *Let $\Lambda^* = \{m_0, \ldots, m_n\}$ be as defined with $n \geq 2g + 2$. The sequence of codes $C_{m_0}, C_{m_1}, \ldots, C_{m_n}$ satisfies the isometry-dual poperty whenever $2g + n - 1 \in \Lambda^*$. Equivalently, the sequence $C_{m_0}, C_{m_1}, \ldots, C_{m_n}$ satisfies the isometry-dual property if and only if the ideal $\Lambda \setminus \Lambda^*$ is maximum sparse.*

6.2. Inclusion Relationship of Sparse Ideals

As seen in Theorem 2, a proper ideal I of Λ is maximum sparse if and only if I is of the form $\Lambda \setminus D(i)$ for some integer i satisfying $G(i) = 0$. The next lemma states the relationship between Frobenius numbers of maximum sparse ideals of a given numerical semigroup when the ideals satisfy inclusion relationships.

Lemma 9. *For two proper maximum sparse ideals I, I' of a numerical semigroup Λ with Frobenius numbers $\lambda_i, \lambda_{i'}$, the following statements are equivalent:*

1. $I \subseteq I'$;
2. $\Lambda \setminus I' \subseteq \Lambda \setminus I$;
3. $D(i') \subseteq D(i)$;
4. $\lambda_i - \lambda_{i'} \in \Lambda$;
5. $\#(\Lambda \setminus I) - \#(\Lambda \setminus I') \in \Lambda$.

Proof. The equivalence of statements (1) and (2) is obvious. Since I, I' are proper maximum sparse ideals, $D(i) = \Lambda \setminus I$ and $D(i') = \Lambda \setminus I'$. Hence, statement (2) and statement (3) are equivalent. Statement (3) is equivalent to $\lambda_{i'} \in D(i)$, which, in turn, is equivalent to statement (4). Statements (4) and (5) are equivalent since $\lambda_i = 2g - 1 + \#(\Lambda \setminus I)$ and $\lambda_{i'} = 2g - 1 + \#(\Lambda \setminus I')$. Hence, $\lambda_i - \lambda_{i'} = \#(\Lambda \setminus I) - \#(\Lambda \setminus I')$. □

6.3. Puncturing Sequences of Isometry-Dual One-Point Algebraic-Geometry Codes

We wonder now whether the isometry-dual property is inherited after puncturing sequences of one-point algebraic-geometry codes. We proved in the next theorem a necessary condition for the inheritance of the isometric-dual property. In particular, in order to mantain the property, the number of evaluating points that are supressed when puncturing must be a non-gap of the associated Weierstrass semigroup. This result was proved first in [24].

Theorem 4. *Suppose now that $P_1, \ldots, P_n, Q$ are different rational points of a projective, smooth, irreducible curve of genus g. Let Λ be the Weierstrass semigroup at Q, let $C_m = \{(f(P_1), \ldots, f(P_n)) : f \in L(mQ)\}$, and let $\Lambda^* = \{0\} \cup \{m \in \mathbb{N}, m > 0 : C_m \neq C_{m-1}\} = \{m_0 = 0, m_1, \ldots, m_n\}$. Suppose that the sequence $C_{m_0}, \ldots, C_{m_n}$ holds the isometry-dual property. Consider a subset $\{P_{i_1}, \ldots, P_{i_{n'}}\} \subseteq \{P_1, \ldots, P_n\}$, with $2g + 2 \leq n' < n$, the punctured codes $C'_m = \{(f(P_{i_1}), \ldots, f(P_{i_{n'}})) : f \in L(mQ)\}$, and the associated index set $(\Lambda^*)' = \{0\} \cup \{m \in \mathbb{N}, m > 0 : C'_m \neq C'_{m-1}\} = \{m'_1 = 0, m'_2, \ldots, m'_{n'}\}$. If the code sequence $\{0\}, C'_{m'_1}, C'_{m'_2}, \ldots, C_{m'_{n'}}$ also holds the isometry-dual property, then $n - n' \in \Lambda$.*

Proof. By hypothesis, the set $\Lambda \setminus \Lambda^*$ is a maximum sparse ideal. If the sequence $\{0\}, C'_{m'_1}, \ldots, C_{m'_{n'}}$ also holds the isometry-dual preperty, then so is $\Lambda \setminus (\Lambda^*)'$. We have $(\Lambda^*)' \subseteq \Lambda^*$ because $C'_m \neq C'_{m-1}$ implies $C_m \neq C_{m-1}$. Consequently, $\Lambda \setminus (\Lambda^*)' \supseteq \Lambda \setminus \Lambda^*$. Using Lemma 9, we can conclude that $\#\Lambda^* - \#(\Lambda^*)' = n - n' \in \Lambda$. □

7. Ideals and Generalized Hamming Weights

The number of nonzero coordinates of a word coincides with the cardinality of the support of the one-dimension vector it generates. Hence, the minimum distance of a linear code can be thought as the minimum number of elements the support of a one-dimension linear space can have. This is generalized to the so-called Hamming weights, which are defined, for each given dimension as the minimum size of the support of the linear subspaces of that dimension. The generalized Hamming weights for algebraic-geometry codes have been analyzed in [25–27]. Applications of generalized Hamming weights appear in a variety of fields of communications. Wei [28] first used the notion to analyze the performance of Ozarow–Wuyner's wire-tap channel of type II [29] and in connection to t-resilient functions. In [30], there is an update of the connections of generalized Hamming weights with the wire-tap channel using network coding. The reference [31] generalizes the notion for network coding. Generalized Hamming weights have applications also in the area of list decoding [32,33]. In particular, Guruswami showed that his (e, L)-list decodibility notion in the case of erasures is equivalent to the generalized Hamming weights for linear codes. Generalized Hamming weights have also been used to bound the covering radius of linear codes [34] and for secure secret sharing based

on linear codes [35,36]. One further related notion is that of relative generalized Hamming weights, where only the support of subspaces with no intersection with a given subspace are considered. They are applied to bound the information leakage in linear ramp secret sharing schemes. They were proposed in [37] and analyzed for algebraic-geometry codes in [38,39].

Heijnen and Pellikaan introduced in [40] the generalized order bounds for the generalized Hamming weights of dual one-point algebraic-geometry codes in terms of Weierstrass semigroups. Farrán and Munuera showed the existence of a constant, which they named the Feng–Rao number, depending only on the dimension of the Hamming weights and the Weierstrass semigroup, which completely determined the order bounds for codes of rate low enough. The references [41–44] deal with the generalized order bounds and the Feng–Rao numbers related to particular classes of semigroups.

We will present a new bound on the generalized Hamming weights that was first proved in [6]. It uses a lower bound on the Feng–Rao numbers derived from the upper bound for the Frobenius number of an ideal of a semigroup that we presented in Theorem 1. It is obtained through the analysis of intervals of consecutive gaps of Weierstrass semigroups. The idea of consecutive gaps was already used in [45] to bound the minimum distance of one-point codes and in [46] to bound the generalized Hamming weights for primal codes.

7.1. Feng–Rao Numbers

In Section 3.3, we introduced the ν sequence of a numerical semigroup Λ counting the number of pairs of non-gaps whose sum equals a given non-gap. The minimum distance of the dual one-point code $C_m^{\perp}$ associated with a rational point Q with Weierstrass semigroup Λ and associated sequence ν is bounded by the order (or Feng–Rao) bound defined as $\delta(m) = \min\{\nu_i : i > m\}$ [3,10,47]. Some results about the computation of the order bound can be found in [3,7,11–14,48].

The order bound for the minimum distance is generalized to any dimension r by the r-th order bound for the generalized r-th generalized Hamming weight. In this case, define $D(i_1, \ldots, i_r) = D(i_1) \cup \cdots \cup D(i_r)$. Then, the r-th order bound is defined as $\delta_r(m) = \min\{\#D(i_1, \ldots, i_r) : i_1, \ldots, i_r > m\}$. This definition was introduced in [40]. Farrán and Munuera proved in [49] that, for each integer $r \geq 2$ and for each numerical semigroup Λ, there exists a constant $E_r = E(\Lambda, r)$, the so-called r-th *Feng–Rao number*, satisfying that

1. $\delta_r(m) = m - g + E_r + 2$ for every m with $\lambda_m \geq 2c - 2$ ([49], Theorem 3),
2. $\delta_r(m) \geq m - g + E_r + 2$ for every m with $\lambda_m \geq c$ ([49], Theorem 8),

where g and c stand respectively for the genus and the conductor of Λ. This is indeed an extension of the Goppa bound in which case $r = 1$ and $E_r = 0$ ([3], Theorem 5.24). The constant E_r satisfies

3. $r \leq E_r \leq \lambda_{r-1}$ if $g > 0$ (and $r \geq 2$) ([49], Proposition 5),
4. $E_r = \lambda_{r-1}$ if $r \geq c$ ([49], Proposition 5),
5. $E_r = r - 1$ if $g = 0$.

In [41,49,50], one can find more results related to the Feng–Rao numbers.

We will use Theorem 1 to describe a new lower bound for the Feng–Rao number E_r. The new bound is strictly better than the bound $E_r \geq r$ for semigroups having more than two intervals of gaps and dimensions $r > 2$.

7.2. Bound on the Feng–Rao Numbers

To prove the new bound, we first need the next lemma, whose proof can be found in [6], and then we can state the theorem with the bound. The proof of the theorem uses that $\delta_r(m)$ counts the number of elements of a numerical semigroup not belonging to an ideal and the bound of Theorem 1.

Lemma 10. *Let*

$$\mathcal{A}(r,\ell,a_1,a_r)=\{A\subset\mathbb{N}_0:\#A=r,\min(A)=a_1,\max(A)=a_r,A \text{ contains at least } \ell \text{ consecutive integers}\}.$$

For every $A\in\mathcal{A}$, *let* $\alpha(A)=\max\{a\in A: a+1-\ell,\dots,a\in A\}$. *Then,* $\min\alpha(A)=\max\{a_1+\ell-1, a_1+(\ell-1)(a_1-a_r)+\ell(r-1)\}$.

Theorem 5. *Suppose that* $n_{\ell-1}$ *is the number of intervals of at least* $\ell-1$ *consecutive gaps of* Λ, *for* ℓ *an integer larger than* 1. *Then,*

$$E_r \geq \min\left\{r+\left\lceil\frac{r}{\ell-1}\right\rceil-2, r+\left\lceil\frac{(\ell-1)n_{\ell-1}}{\ell}\right\rceil-1\right\}. \tag{5}$$

Proof. By definition of $\delta_r(m)$, there exist integers $i_1,\dots,i_r$ with $m<i_1<\cdots<i_r$ such that $\delta_r(m)=\#D(i_1,\dots,i_r)$. The integers $i_1,\dots,i_r$ minimize $\#D(i_1,\dots,i_r)$. Denote A the set $\{i_1,\dots,i_r\}$. Suppose that the integer m is at least $2c-g-1$. From the definition of E_r, we have $\delta_r(m)=m-g+E_r+2$.

As the set A minimizes the amount $\#D(i_1,\dots,i_r)$, then $i_1=m+1$. Now, one can apply Theorem 1 to the ideal $\Lambda\setminus D(i_1,\dots,i_r)$, and obtain $(m-g+E_r+2)+(2g-1)\geq\lambda_{i_r}=g+i_r$. One can reorganize the inequality and obtain

$$i_r\leq m+E_r+1. \tag{6}$$

If we assume that A has no ℓ consecutive integers, then

$$i_r\geq m+r+\left\lceil\frac{r-(\ell-1)}{\ell-1}\right\rceil. \tag{7}$$

Then, by inequality (6), $E_r\geq r+\left\lceil\frac{r}{\ell-1}\right\rceil-2$. On the other hand, assume that A has at least ℓ consecutive integers. Suppose that i_j is the maximum integer belonging to A so that $i_j-\ell+1,\dots,i_j\in A$ and so $i_{j-\ell+1}=i_j-\ell+1,\dots,i_{j-1}=i_j-1$ and $\lambda_{i_{j-\ell+1}}=\lambda_{i_j}-\ell+1,\dots,\lambda_{i_{j-1}}=\lambda_{i_j}-1$. Let $\Gamma=\{\lambda\in\Lambda:\lambda+1,\dots,\lambda+\ell-1\notin\Lambda\}$. In particular, if λ is an element of Γ, it must be strictly smaller than the conductor c of Λ. Obviously, $\#\Gamma=n_{\ell-1}$. If $\lambda\in\Gamma$, then $(\lambda_{i_j}-1)-\lambda\in D(i_{j-1})\setminus D(i_j)$, …, $(\lambda_{i_j}-\ell+1)-\lambda\in D(i_{j-\ell+1})\setminus D(i_j)$, and so $\{\lambda_{i_j}-\lambda-1,\lambda_{i_j}-\lambda-2,\dots,\lambda_{i_j}-\lambda-\ell+1\}\subseteq D(i_{j-\ell+1},\dots,i_{j-1})\setminus D(i_j)$. In fact, $\cup_{\lambda\in\Gamma}\{\lambda_{i_j}-\lambda-1,\dots,\lambda_{i_j}-\lambda-\ell+1\}\subseteq D(i_{j-\ell+1},\dots,i_{j-1})\setminus D(i_j)$ and the sets in this union are disjoint. Indeed, for $\lambda,\lambda'\in\Gamma$, with $\lambda>\lambda'$, it holds $\lambda-\lambda'\geq\ell$. Then, $\min\{\lambda_{i_j}-\lambda'-1,\dots,\lambda_{i_j}-\lambda'-\ell+1\}=\lambda_{i_j}-\lambda'-\ell+1\geq\lambda_{i_j}-\lambda+1>\max\{\lambda_{i_j}-\lambda-1,\dots,\lambda_{i_j}-\lambda-\ell+1\}$. Hence,

$$\#D(i_1,\dots,i_r)\geq\#D(i_{j-\ell+1},\dots,i_j)\geq(\ell-1)n_{\ell-1}+v_{i_j}=(\ell-1)n_{\ell-1}+i_j-g+1. \tag{8}$$

Since $D(i_1,\dots,i_r)=m-g+E_r+2$, we get that $m-g+E_r+2\geq(\ell-1)n_{\ell-1}+i_j-g+1$, so

$$E_r\geq(\ell-1)n_{\ell-1}+i_j-m-1. \tag{9}$$

Now, by Lemma 10, and by the maximality of j,

$$i_j\geq\max\{i_1+\ell-1, i_1+(\ell-1)(i_1-i_r)+\ell(r-1)\}. \tag{10}$$

This implies

$$i_j\geq i_1+\ell-1, \tag{11}$$

and

$$i_j\geq i_1+(\ell-1)(i_1-i_r)+\ell(r-1). \tag{12}$$

On one side, we can use inequality (9) and inequality (11), and obtain $E_r \geq (\ell-1)(n_{\ell-1}+1)$. On the other side, we can use inequality (9) and inequality (12), and then inequality (6), as follows:

$$\begin{aligned} E_r &\geq (\ell-1)n_{\ell-1} + i_1 + (\ell-1)(i_1 - i_r) + \ell(r-1) - m - 1 \\ &= (\ell-1)n_{\ell-1} + (\ell-1)(i_1 - i_r) + \ell(r-1) \\ &\geq (\ell-1)n_{\ell-1} - (\ell-1)E_r + \ell(r-1), \end{aligned}$$

from where we can conclude that $E_r \geq r - 1 + \left\lceil \frac{(\ell-1)n_{\ell-1}}{\ell} \right\rceil$.

At this point, we have shown that either $E_r \geq r + \left\lceil \frac{r}{\ell-1} \right\rceil - 2$ or $E_r \geq \max\{(\ell-1)(n_{\ell-1}+1), r + \left\lceil \frac{(\ell-1)n_{\ell-1}}{\ell} \right\rceil - 1\}$, depending on whether A has or does not have ℓ consecutive integers. Hence, we deduce the bounds that follow:

$$\begin{aligned} E_r &\geq \min\{r + \left\lceil \frac{r}{\ell-1} \right\rceil - 2, (\ell-1)(n_{\ell-1}+1)\}, \\ E_r &\geq \min\{r + \left\lceil \frac{r}{\ell-1} \right\rceil - 2, r + \left\lceil \frac{(\ell-1)n_{\ell-1}}{\ell} \right\rceil - 1\}. \end{aligned}$$

Let us see that the second bound is always at least as good as the first one. Hence, the first bound can be ignored. Indeed, if $r + \left\lceil \frac{r}{\ell-1} \right\rceil - 2 \leq r + \left\lceil \frac{(\ell-1)n_{\ell-1}}{\ell} \right\rceil - 1$, then we are done. Otherwise, if $r + \left\lceil \frac{r}{\ell-1} \right\rceil - 2 > r + \left\lceil \frac{(\ell-1)n_{\ell-1}}{\ell} \right\rceil - 1$, then we need to prove that $r + \left\lceil \frac{(\ell-1)n_{\ell-1}}{\ell} \right\rceil - 1 \geq (\ell-1)(n_{\ell-1}+1)$.

If $r + \left\lceil \frac{r}{\ell-1} \right\rceil - 2 > r + \left\lceil \frac{(\ell-1)n_{\ell-1}}{\ell} \right\rceil - 1$, then $\left\lceil \frac{r}{\ell-1} \right\rceil > \left\lceil \frac{(\ell-1)n_{\ell-1}}{\ell} \right\rceil + 1$, which implies that $\frac{r}{\ell-1} > \frac{(\ell-1)n_{\ell-1}}{\ell} + 1$, and so $r > (\ell-1)(\frac{(\ell-1)n_{\ell-1}}{\ell} + 1) = (\ell-1)((n_{\ell-1}+1) - \frac{n_{\ell-1}}{\ell})$. This implies $r + \frac{(\ell-1)n_{\ell-1}}{\ell} > (\ell-1)(n_{\ell-1}+1)$, and so $r + \left\lceil \frac{(\ell-1)n_{\ell-1}}{\ell} \right\rceil - 1 \geq (\ell-1)(n_{\ell-1}+1)$, as desired. □

Remark 4. *The bound in Theorem 5 only improves the bound $E_r \geq r$ when $\ell < r/2 + 1$ and $n_{\ell-1} > 0$.*

7.3. Bound on the Generalized Hamming Weights

Corollary 2. *Let $\ell \geq 2$ and let m satisfy $\lambda_m \geq c$. Then, $\delta_r(m) \geq m + 2 - g + \min\left\{r - 2 + \left\lceil \frac{r}{\ell-1} \right\rceil, r - 1 + \left\lceil \frac{(\ell-1)n_{\ell-1}}{\ell} \right\rceil\right\}$.*

Remark 5. *From bound (5), taking $\ell = 2$, we deduce that, if n is the number of intervals of (at least one) gaps of Λ, then*

$$E_r \geq \min\{2(r-1), r + \lceil n/2 \rceil - 1\}. \tag{13}$$

Remark 6. *If $n \leq 2$ or $r = 2$, the bound in the previous remark equals the bound $E_r \geq r$. In any other case, this new bound is better.*

Corollary 3. *If the Weierstrass semigroup Λ has n intervals of gaps and its conductor is c, then, for every integer m such that $\lambda_m \geq c$,*

$$\delta_r(m) \geq \begin{cases} m - g + 2r, & \text{if } r \leq \lceil n/2 \rceil + 1, \\ m - g + r + \lceil n/2 \rceil + 1 & \text{otherwise.} \end{cases}$$

7.4. Sharpness of the Bound

If one analyzes the proof of Theorem 5, it can be seen that the bound (5) may only be sharp if

1. The inequality (6) is indeed an equality. That bound is obtained when one applies Theorem 1 to the ideal $\Lambda \setminus D(i_1, \ldots i_r)$. The inequality being an equality means applying Theorem 2 to the same ideal that $D(i_1, \ldots, i_r) = D(i_r)$. Hence, $i_1, \ldots, i_{r-1} \subseteq i_r - \Lambda$ and so, $i_r - i_{r-1} \geq \lambda_1$.

2. Either inequality (7) or both inequality (8) and inequality (10) are indeed equalities. In this case, $i_r - i_{r-1} \leq 2$.

From these observations, one can conclude that the bound may be sharp only if the Weierstrass semigroup Λ is a hyperelliptic semigroup, that is, a semigroup containing 2. For hyperelliptic semigroups, it was proved in ([50], Theorem 1) that $E_r = \lambda_{r-1} = 2(r-1)$. On the other hand, the bound (5) for the unique hyperelliptic semigroup of genus g is

$$E_r \geq \begin{cases} r-1, & \text{if } \ell > 2, \\ 2(r-1), & \text{if } \ell = 2 \text{ and } r-1 \leq \lceil g/2 \rceil, \\ r + \lceil g/2 \rceil - 1, & \text{if } \ell = 2 \text{ and } r-1 > \lceil g/2 \rceil. \end{cases}$$

Thus, we conclude that the bound is sharp if and only if $\ell = 2$, the Weierstrass semigroup Λ is hyperelliptic, and $r \leq \lceil g/2 \rceil + 1$.

7.5. The Bound Applied to the Hermitian Curve

The weight hierarchy of $\mathcal{H}_q$ has already been studied in [27,51]. However, for its simplicity, we wanted to give a description of n_ℓ. As we have seen before, the Weierstrass semigroup at the rational point at infinity is generated by q and $q+1$. Its weight hierarchy was studied in [42]. The semigroup generated by q and $q+1$ is $\{0\} \cup \{q, q+1\} \cup \{2q, 2q+1, 2q+2\} \cup \cdots \cup \{(q-2)q, \ldots, (q-2)q + (q-2)\} \cup \{k \in \mathbb{N}_0 : k \geq (q-1)q\}$. In this case, the lengths of the intervals of consecutive gaps are $q-1, q-2, \ldots, 1$. Thus,

$$n_\ell = \begin{cases} q - \ell, & \text{if } 1 \leq \ell \leq q, \\ 0, & \text{if } \ell \geq q. \end{cases}$$

It is left as an open question to compare the results in [41] with the bound proved in Theorem 5, using these values of n_ℓ.

8. Further Reading

It was our purpose to cite within the text the bibliography related to each specific section. However, the reader may be interested in some more general references. The books [52–54] have many results on numerical semigroups. Algebraic-geometry codes have been widely explained in different books such as [18,55,56] or in chapter [57]. For a general theory of one-point codes, their decoding, and also some of their relationships with Weierstrass semigroups, chapter [3] is probably the most important reference. Finally, chapter [1] is a survey of results on numerical semigroups, their classification, characterization and counting, and their relationship with algebraic-geometry codes from the perspective of decoding algorithms, their parameters such as the minimum distance, and the optimization of their redundancy under particular decoding restrictions.

9. Conclusions

Numerical semigroups play an important role in the analysis of error-correcting codes. More specifically, additive ideals of numerical semigroups are involved in determining non-redundant parity-checks, the code length, the generalized Hamming weights, and the isometry-dual sequences of algebraic-geometry codes. These results have been presented in this survey in a unified framework.

Funding: This work was partly supported by the Catalan Government under grant 2017 SGR 00705, by the Spanish Ministry of Economy and Competitivity under grant TIN2016-80250-R, and by Universitat Rovira i Virgili under grant OPEN2019.

Acknowledgments: The author would like to thank Michael E. O'Sullivan and Kwankyu Lee for many helpful discussions. She would also like to thank the coauthors of the main papers involved in this contribution: Kwankyu Lee, Albert Vico-Oton, Euijin Hong, and Iwan Duursma.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Bras-Amorós, M. Numerical semigroups and codes. In *Algebraic Geometry Modeling in Information Theory*; Volume 8 of Ser. Coding Theory Cryptol.; World Science Publisher: Hackensack, NJ, USA, 2013; pp. 167–218.
2. Geil, O. On codes from norm-trace curves. *Finite Fields Appl.* **2003**, *9*, 351–371. [CrossRef]
3. Høholdt, T.; van Lint, J.H.; Pellikaan, R. Algebraic geometry codes. In *Handbook of Coding Theory*; North-Holland: Amsterdam, The Netherlands, 1998; Volumes I and II, pp. 871–961.
4. Sylvester, J.J. Mathematical questions with their solutions. *Educ. Times* **1884**, *41*, 21.
5. Stichtenoth, H. A note on Hermitian codes over GF(q^2). *IEEE Trans. Inform. Theory* **1988**, *34*, 1345–1348. [CrossRef]
6. Bras-Amorós, M.; Lee, K.; Vico-Oton, A. New lower bounds on the generalized Hamming weights of AG codes. *IEEE Trans. Inform. Theory* **2014**, *60*, 5930–5937. [CrossRef]
7. Bras-Amorós, M. Acute semigroups, the order bound on the minimum distance, and the Feng-Rao improvements. *IEEE Trans. Inform. Theory* **2004**, *50*, 1282–1289. [CrossRef]
8. Bras-Amorós, M. A note on numerical semigroups. *IEEE Trans. Inform. Theory* **2007**, *53*, 821–823. [CrossRef]
9. Bras-Amorós, M.; O'Sullivan, M. On semigroups generated by two consecutive integers and improved Hermitian codes. *IEEE Trans. Inform. Theory* **2007**, *53*, 2560–2566. [CrossRef]
10. Kirfel, C.; Pellikaan, R. The minimum distance of codes in an array coming from telescopic semigroups. *IEEE Trans. Inform. Theory* **1995**, *41*, 1720–1732. [CrossRef]
11. Munuera, C.; Torres, F. A note on the order bound on the minimum distance of AG codes and acute semigroups. *Adv. Math. Commun.* **2008**, *2*, 175–181.
12. Oneto, A.; Tamone, G. On numerical semigroups and the order bound. *J. Pure Appl. Algebra* **2008**, *212*, 2271–2283. [CrossRef]
13. Oneto, A.; Tamone, G. On the order bound of one-point algebraic geometry codes. *J. Pure Appl. Algebra* **2009**, *213*, 1179–1191. [CrossRef]
14. Oneto, A.; Tamone, G. On some invariants in numerical semigroups and estimations of the order bound. *Semigroup Forum* **2010**, *81*, 483–509. [CrossRef]
15. Bras-Amorós, M. Addition behavior of a numerical semigroup. In *Arithmetic, Geometry and Coding Theory (AGCT 2003)*; Volume 11 of Sémin. Congr.; Société Mathématique de France: Paris, France, 2005; pp. 21–28.
16. Barucci, V. Decompositions of ideals into irreducible ideals in numerical semigroups. *J. Commut. Algebra* **2010**, *2*, 281–294. [CrossRef]
17. Geil, O.; Munuera, C.; Ruano, D.; Torres, F. On the order bounds for one-point AG codes. *Adv. Math. Commun.* **2011**, *5*, 489–504.
18. Stichtenoth, H. *Algebraic Function Fields and Codes*; Universitext; Springer: Berlin, Germany, 1993.
19. Geer, G.V.; Howe, E.W.; Lauter, K.E.; Ritzenthaler, C. Tables of Curves with Many Points. Available online: http://www.manypoints.org (accessed on 4 November 2019).
20. Lewittes, J. Places of degree one in function fields over finite fields. *J. Pure Appl. Algebra* **1990**, *69*, 177–183. [CrossRef]
21. Geil, O.; Matsumoto, R. Bounding the number of $\mathbb{F}_q$-rational places in algebraic function fields using Weierstrass semigroups. *J. Pure Appl. Algebra* **2009**, *213*, 1152–1156. [CrossRef]
22. Bras-Amorós, M.; Vico-Oton, A. On the Geil-Matsumoto bound and the length of AG codes. *Des. Codes Cryptogr.* **2014**, *70*, 117–125. [CrossRef]
23. Beelen, P.; Ruano, D. Bounding the number of points on a curve using a generalization of Weierstrass semigroups. *Des. Codes Cryptogr.* **2013**, *66*, 221–230. [CrossRef]
24. Bras-Amorós, M.; Duursma, I.; Hong, E. Isometry-dual flags of AG codes. 2019, submitted.
25. Munuera, C. On the generalized Hamming weights of geometric Goppa codes. *IEEE Trans. Inform. Theory* **1994**, *40*, 2092–2099. [CrossRef]
26. Munuera, C. Generalized Hamming weights and trellis complexity. In *Advances in Algebraic Geometry Codes*; Martinez-Moro, E., Munuera, C., Ruano, D., Eds.; World Scientific: Singapore, 2008; pp. 363–390.
27. Yang, K.; Kumar, P.V.; Stichtenoth, H. On the weight hierarchy of geometric Goppa codes. *IEEE Trans. Inform. Theory* **1994**, *40*, 913–920. [CrossRef]
28. Wei, V.K. Generalized Hamming weights for linear codes. *IEEE Trans. Inform. Theory* **1991**, *37*, 1412–1418. [CrossRef]

29. Ozarow, L.H.; Wyner, A.D. Wire-tap channel II. In *Advances in Cryptology (Paris, 1984)*; Volume 209 of Lecture Notes in Comput. Sci.; Springer: Berlin, Germany, 1985; pp. 33–50.
30. Rouayheb, S.E.; Soljanin, E.; Sprintson, A. Secure network coding for wiretap networks of type II. *IEEE Trans. Inform. Theory* **2012**, *58*, 1361–1371. [CrossRef]
31. Ngai, C.K.; Yeung, R.W.; Zhang, Z. Network generalized Hamming weight. *IEEE Trans. Inform. Theory* **2011**, *57*, 1136–1143. [CrossRef]
32. Gopalan, P.; Guruswami, V.; Raghavendra, P. List decoding tensor products and interleaved codes. In Proceedings of the 2009 ACM International Symposium on Theory of Computing, Bethesda, MD, USA, 31 May–2 June 2009; ACM: New York, NY, USA, 2009; pp. 13–22.
33. Guruswami, V. List decoding from erasures: bounds and code constructions. *IEEE Trans. Inform. Theory* **2003**, *49*, 2826–2833. [CrossRef]
34. Janwa, H.; Lal, A.K. On generalized Hamming weights and the covering radius of linear codes. In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*; Volume 4851 of Lecture Notes in Comput. Sci.; Springer: Berlin, Germany, 2007; pp. 347–356.
35. Cruz, R.D.; Meyer, A.; Sole, P. An extension of Massey scheme for secret sharing. In Proceedings of the Information Theory Workshop, Dublin, Ireland, 30 August–3 September 2010.
36. Kurihara, J.; Uyematsu, T. Strongly-secure secret sharing based on linear codes can be characterized by generalized Hamming weight. In Proceedings of the 49th Annual Allerton Conference Communication, Control, and Computing, Monticello, IL, USA, 28–30 September 2011.
37. Luo, Y.; Mitrpant, C.; Vinck, A.J.H.; Chen, K. Some new characters on the wire-tap channel of type II. *IEEE Trans. Inform. Theory* **2005**, *51*, 1222–1229. [CrossRef]
38. Geil, O.; Martin, S.; Matsumoto, R.; Ruano, D.; Luo, Y. Relative generalized Hamming weights of one-point algebraic geometric codes. *IEEE Trans. Inform. Theory* **2014**, *60*, 5938–5949. [CrossRef]
39. Lee, K. Bounds for generalized Hamming weights of general AG codes. *Finite Fields Appl.* **2015**, *34*, 265–279. [CrossRef]
40. Heijnen, P.; Pellikaan, R. Generalized Hamming weights of q-ary Reed-Muller codes. *IEEE Trans. Inform. Theory* **1998**, *44*, 181–196. [CrossRef]
41. Delgado, M.; Farrán, J.I.; García-Sánchez, P.A.; Llena, D. On the generalized Feng-Rao numbers of numerical semigroups generated by intervals. *Math. Comp.* **2013**, *82*, 1813–1836. [CrossRef]
42. Delgado, M.; Farrán, J.I.; García-Sánchez, P.A.; Llena, D. On the weight hierarchy of codes coming from semigroups with two generators. *IEEE Trans. Inform. Theory* **2014**, *60*, 282–295. [CrossRef]
43. Farrán, J.I.; García-Sxaxnchez, P.A.; Heredia, B.A. On the second Feng-Rao distance of algebraic geometry codes related to Arf semigroups. *Des. Codes Cryptogr.* **2018**, *86*, 2893–2916. [CrossRef]
44. Farrán, J.I.; García-Sxaxnchez, P.A.; Heredia, B.A.; Leamer, M.J. The second Feng-Rao number for codes coming from telescopic semigroups. *Des. Codes Cryptogr.* **2018**, *86*, 1849–1864. [CrossRef]
45. García, A.; Kim, S.J.; Lax, R.F. Consecutive Weierstrass gaps and minimum distance of Goppa codes. *J. Pure Appl. Algebra* **1993**, *84*, 199–207. [CrossRef]
46. Tang, L. Consecutive Weierstrass gaps and weight hierarchy of geometric Goppa codes. *Algebra Colloq.* **1996**, *3*, 1–10.
47. Feng, G.L.; Rao, T.R.N. A simple approach for construction of algebraic-geometric codes from affine plane curves. *IEEE Trans. Inform. Theory* **1994**, *40*, 1003–1012. [CrossRef]
48. Campillo, A.; Farrán, J.I. Computing Weierstrass semigroups and the Feng-Rao distance from singular plane models. *Finite Fields Appl.* **2000**, *6*, 71–92. [CrossRef]
49. Farrán, J.I.; Munuera, C. Goppa-like bounds for the generalized Feng-Rao distances. *Discrete Appl. Math.* **2003**, *128*, 145–156. [CrossRef]
50. Farrán, J.I.; Sánchez, P.A.G.A.; Llena, D. On the Feng-Rao numbers. In *VII Jornadas de Matemática Discreta y Algorítmica*; CIEM: Castro Urdiales, Spain, 7–9 July 2010.
51. Barbero, A.I.; Munuera, C. The weight hierarchy of Hermitian codes. *SIAM J. Discrete Math.* **2000**, *13*, 79–104. [CrossRef]
52. Assi, A.; García-Sánchez, P.A. *Numerical Semigroups and Applications*; Volume 1 of RSME Springer Series; Springer: Cham, Switzerland, 2016.
53. Alfonsín, J.L.R. *The Diophantine Frobenius Problem*; Volume 30 of Oxford Lecture Series in Mathematics and its Applications; Oxford University Press: Oxford, UK, 2005.

54. Rosales, J.C.; García-Sánchez, P.A. *Numerical Semigroups*; Volume 20 of Developments in Mathematics; Springer: New York, NY, USA, 2009.
55. Pretzel, O. *Codes and Algebraic Curves*; Volume 8 of Oxford Lecture Series in Mathematics and its Applications; The Clarendon Press Oxford University Press: New York, NY, USA, 1998.
56. Van Lint, J.H.; van der Geer, G. *Introduction to Coding Theory and Algebraic Geometry*; Volume 12 of DMV Seminar; Birkhäuser: Basel, Switzerland, 1988.
57. Munuera, C.; Olaya-León, W. An introduction to algebraic geometry codes. In *Algebra for Secure and Reliable Communication Modeling*; Volume 642 of Contemp. Math.; American Mathematical Society: Providence, RI, USA, 2015; pp. 87–117.