ON WEIERSTRASS SEMIGROUPS AND THE REDUNDANCY OF IMPROVED GEOMETRIC GOPPA CODES

RUUD PELLIKAAN AND FERNANDO TORRES

Appeared in:
IEEE Trans. Inform. Theory , vol. 45, pp. 2512-2519, Nov. 1999

Abstract. Improved geometric Goppa codes have a smaller redundancy and the same bound on the minimum distance as ordinary algebraic geometry codes. For an asymptotically good sequence of function fields we give a formula for the redundancy.

1. Introduction

Improved geometric Goppa codes were introduced in [6] where certain parity checks of algebraic geometry codes were deleted and the same bound on the minimum distance remained valid. The Feng-Rao or order bound [5] for one point codes can be computed in terms of the Weierstrass semigroup of the point [10, 11]. In this paper we give a formula for the redundancy of improved geometric Goppa code in terms of properties of the semigroup. This is applied to an asymptotically good sequence of function fields [7, 8] with points with known Weierstrass semigroups [16]. Finally a negative result is obtained, saying that for a large class of cases the improvements do not give rise to asymptotic improvements.

2. Improved geometric Goppa codes

Let R be an $\mathbb{F}_q$-algebra with a *weight function* $\rho : R \to \mathbb{N}_0 \cup \{-\infty\}$, [10, Definition 3.5]. That is to say

- $(O.0)$ $\rho(f) = -\infty$ if and only if $f = 0$,
- $(O.1)$ $\rho(\lambda f) = \rho(f)$ for all nonzero $\lambda \in \mathbb{F}_q$,
- $(O.2)$ $\rho(f+g) \leq \max\{\rho(f), \rho(g)\}$ and equality holds when $\rho(f) \neq \rho(g)$,
- $(O.3)$ $\rho(fg) = \rho(f) + \rho(g)$,
- $(O.4)$ If $\rho(f) = \rho(g)$, then there exists a nonzero $\lambda \in \mathbb{F}_q$ such that $\rho(f - \lambda g) < \rho(g)$,

for all $f, g \in R$.

Date: July 27, 1998. Revised March 11, 1999.

Let R be the affine coordinate ring of an affine algebraic curve over $\mathbb{F}_q$, that is absolutely irreducible with exactly one rational point Q at infinity. Let F be the field of fractions of R. Then F is a function field. Let v_Q be the valuation on F at P. The function $\rho : R \to \mathbb{N}_0 \cup \{-\infty\}$, defined by $\rho(f) = -v_Q(f)$ is a weight function. It is shown that all $\mathbb{F}_q$-algebras with a weight function are of this type, see [13].

Let H be the *semigroup* of (R, ρ). So $m \in H$ if and only if there exists a nonzero $f \in R$ such that $m = \rho(f)$. Let $(\rho_l : l \in \mathbb{N})$ be the strictly increasing sequence that enumerates H. So $H = \{\rho_l : l \in \mathbb{N}\}$ and $\rho_l < \rho_{l+1}$ for all $l \in \mathbb{N}$.

If the affine curve is moreover nonsingular, then we have an equivalent description in the language of function fields [17]. Let F be a function field with $\mathbb{F}_q$ as field of constants. For Q a $\mathbb{F}_q$-rational place of F, let $H(Q)$ be the *Weierstrass semigroup* of Q. So $m \in H(Q)$ if and only if there exists an $f \in F$ such that f has no poles outside Q and f has pole order m at Q. Let $K_\infty(Q)$ be the ring of all function $f \in F$ that have no poles outside Q. Then $(K_\infty(Q), -v_Q)$ is an $\mathbb{F}_q$-algebra with a weight function and $H(Q)$ as semigroup.

A numerical semigroup, that is to say a sub semigroup of $\mathbb{N}_0$, is the semigroup of some $\mathbb{F}_q$-algebra with a weight function. For instance, take for a given sub semigroup $H \subset \mathbb{N}_0$ the vector space R generated by the monomials $\{x^i | i \in H\}$. Then R is an $\mathbb{F}_q$-algebra with weight function the degree function, and H as semigroup. Not all numerical semigroups are realizable as the Weierstrass semigroup of a point of a nonsingular curve, see [1, 18].

Let R be the affine coordinate ring of an affine algebraic curve over $\mathbb{F}_q$, that is absolutely irreducible with exactly one rational point Q at infinity. Let $\mathcal{P} = \{P_1, \ldots, P_n\}$ be a set of n distinct affine $\mathbb{F}_q$-rational points of the curve. Consider the evaluation map

$$ev_{\mathcal{P}} : R \longrightarrow \mathbb{F}_q^n$$

defined by $ev_{\mathcal{P}}(f) = (f(P_1), \ldots, f(P_n))$. Let v_Q be the discrete valuation at Q. Let $L(mQ) = \{\ f \in R\ :\ v_Q(f) \geq -m\ \}$.

Definition 2.1. Define

$$E_l = ev_{\mathcal{P}}(L(\rho_l Q))\,.$$

Let C_l be the dual code of E_l in $\mathbb{F}_q^n$ with respect to the inner product $\mathbf{x} \cdot \mathbf{y} = \sum x_i y_i$.

Remark 2.2. In case the curve is nonsingular the codes E_l and C_l defined by $\mathcal{P}$ and $\rho_l Q$ are so called *one point geometric Goppa* codes or *one point algebraic geometry* codes and are also denoted by $C_L(\mathcal{P}, \rho_l Q)$ and $C_\Omega(\mathcal{P}, \rho_l Q)$, respectively. See [17, 19].

Let g be the *genus* of the function field F. Then g is equal to the number of gaps of $H(Q)$. The number $l + 1 - g$ is called the *Goppa designed minimum distance* of C_l and is denoted by $d_G(l)$. It is a lower bound on the minimum distance of C_l.

Definition 2.3. Let $\nu_l = \#\{(i, j) \in \mathbb{N}^2 :\ \rho_i + \rho_j = \rho_{l+1}\}$.

Definition 2.4. Let

$$d_{ORD}(l) = \min\{\ \nu_{l'}\ :\ l' \geq l\ \}.$$

Then $d_{ORD}(l)$ is called the *order bound* or the *Feng-Rao designed minimum distance* of C_l. See [10, Definition 4.12].

Let c be the *conductor* of $H(Q)$, that is to say the largest element $m \in H(Q)$ such that $m-1 \notin H(Q)$. Then $c = g = 0$ or $g+1 \leq c \leq 2g$, see [10, Proposition 5.7] or Remark 3.3.

Theorem 2.5. *The minimum distance of C_l is at least $d_{ORD}(l)$. Furthermore $d_{ORD}(l) \geq d_G(l) = l+1-g$ and equality holds if $l > 2c-g-2$.*

Proof. See [5, 11] and [10, Theorem 5.24]. □

Remark 2.6. If $\rho_l < n$, then $\dim(E_l) = l$, by [10, Theorem 5.18]. So the redundancy of C_l is at most l, and equality holds if $\rho_l < n$. So for large values of l the parameters of the code C_l can be better than expected, since the parity checks $\mathbf{h}_1, \ldots, \mathbf{h}_l$ might be dependent. In the following we will see that for small values of l we can get an improvement on the redundancy by deleting certain parity checks while the bound on the minimum distance remains the same.

Definition 2.7. Let d be a positive integer. Define

$$\tilde{C}(d) = \{\ \mathbf{c} \in \mathbb{F}_q^n\ :\ \mathbf{c} \cdot \mathbf{h}_i = 0 \text{ for all } i \text{ such that } \nu_{i-1} < d\ \}.$$

Proposition 2.8. *The minimum distance of $\tilde{C}(d)$ is at least d.*

Proof. See [6] and [10, Proposition 4.23]. □

Definition 2.9. Let d be a positive integer. Then

$$r_d = \#\{\ i\ :\ \nu_{i-1} < d\ \}.$$

Remark 2.10. The code $\tilde{C}(d)$ has the *super code property*, that is to say: if $d = d_{ORD}(l)$, then $C_l \subseteq \tilde{C}(d)$. In other words: if $d = d_{ORD}(l)$, then the lower bound on the minimum distance of C_l and $\tilde{C}(d)$ is d for both codes, but $\tilde{C}(d)$ might be larger, and therefore better. That is why these codes are called *improved geometric Goppa codes* in [6]. From an algebraic geometric point of view these codes are defined with the help of incomplete linear systems.

Remark 2.11. The number r_d is the number of parity checks that define $\tilde{C}(d)$. So the redundancy of $\tilde{C}(d)$ is at most r_d. Hence the dimension of $\tilde{C}(d)$ is at least $n - r_d$. We will see in Remark 4.3 that the redundancy of $\tilde{C}(d)$ is exactly equal to r_d in the range of d where we can expect an improvement on the redundancy of $\tilde{C}(d)$ compared to C_l, if the number of rational places of the function field is large enough.

Example 2.12. Consider the Hermitian function field $\mathbb{F}_{16}(x,y)$ with defining equation $x^5 = y^4 + y$. See [17]. The genus is 6 and the number of rational places is 65. The Weierstrass semigroup H of the place at infinity is generated by 4 and 5. Hence

$$H = \{0,4,5,8,9,10\} \cup \{n \in \mathbb{N}_0 \ : \ n \geq 12\}.$$

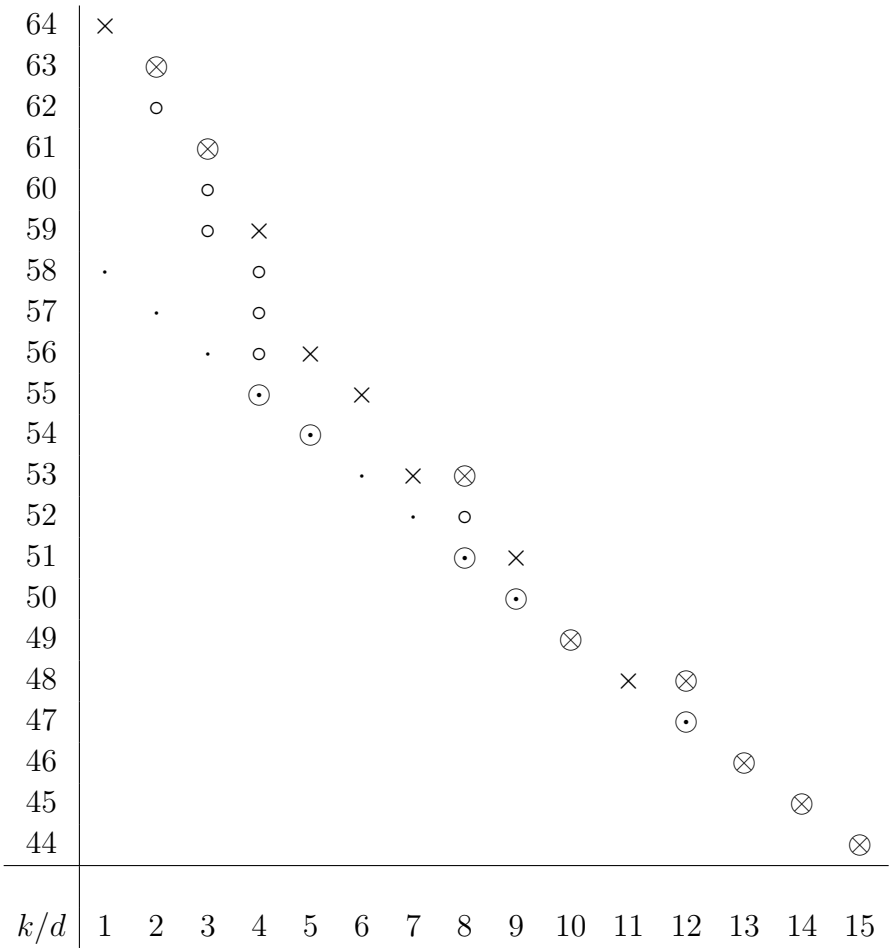
So the conductor is 12. The sequence $(\nu_i : i \in \mathbb{N}_0)$ is given by [10, Example 4.17].

$$1,2,2,3,4,3,4,6,6,4,5,8,9,8,9,10,12,12,13,14,15,\ldots$$

The sequence $(r_d : d \in \mathbb{N})$ is given by

$$0,1,3,5,8,9,11,11,13,15,16,16,18,19,20,21,22,\ldots$$

In the tabel below bounds are given on the the parameters of codes of length 64. The rows correspond to the dimension k. The columns correspond to the minimum distance d. The Goppa bound is given by the line $k + d = 64 + 1 - 6 = 59$ and the entries are denoted by $\cdot$. The order or Feng-Rao bound is given by $d = d_{ORD}(64 - k)$ and the entries are denoted by $\circ$. The symbol $\odot$ denotes that the order bound and the Goppa bound coincide. The redundancy of the code $\tilde{C}(d)$ is given by $k = 64 - r_d$ and the entries are denoted by $\times$. The symbol $\otimes$ denotes that the order bound and the redundancy of the improved code coincide. The three bounds coincide for $d \geq 13$.



Notice that for $d = 4, 5, 6$ and 9 the codes $\tilde{C}(d)$ give improvements of the order bound, see [6, Example 3.1]. In [9] the order bound of these codes is compared with subspace subcodes of Reed-Solomon codes of length 64.

An explicit formula for the redundancy of improved Hermitian codes is not known. In the following we give a class of improved geometric Goppa codes and determine an explicit formula for the redundancy.

Let $(\mathcal{F}_m : m \in \mathbb{N})$ be a *tower* of function fields over $\mathbb{F}_q$. So $\mathcal{F}_{m-1} \subset \mathcal{F}_m$ for all $m > 1$. Let a_m be the degree of $\mathcal{F}_m$ over $\mathcal{F}_{m-1}$. Let Q_m be a rational place of $\mathcal{F}_m$. Suppose that Q_m is totally ramified over Q_{m-1} for all $m > 1$. Let $H_m = H(Q_m)$ be the Weierstrass semigroup of Q_m. Let c_m be the conductor of H_m. Then

$$a_m H_{m-1} \cup \{\ n \in \mathbb{N}_0\ :\ n \geq c_m\ \} \subseteq H_m.$$

Definition 2.13. A sequence $(H_m : m \in \mathbb{N})$ of semigroups is called an *inductive tower* if there exist sequences $(a_m : m \in \mathbb{N})$ and $(b_m : m \in \mathbb{N})$ of positive integers such that

$H_1 = \mathbb{N}_0$ and

$$H_m = a_m H_{m-1} \cup \{\ n \in \mathbb{N}_0\ :\ n \geq a_m b_{m-1}\ \} \text{ and } a_m b_{m-1} \leq b_m \tag{2.1}$$

for all $m > 1$. By induction we define inductive semigroups. If $H = \mathbb{N}_0$, then H is inductive. If H_0 is inductive with conductor c_0 and there are positve integers a and b such that

$$H = aH_0 \cup \{\ n \in \mathbb{N}_0\ :\ n \geq ab\ \} \text{ and } b \geq c_0,$$

then H is inductive.

Remark 2.14. Let $(H_m : m \in \mathbb{N})$ be an inductive tower of semigroups. Let c_m be the conductor of H_m. Let g_m be the number of gaps of H_m. Then $c_m = a_m b_{m-1}$ and $g_m = (a_m - 1)b_{m-1} + g_{m-1}$ for $m > 1$, as we will see in Lemma 3.15.

Let H_0 be a semigroup with conductor c_0 and g_0 gaps. Let $H = aH_0 \cup \{\ n \in \mathbb{N}_0\ :\ n \geq ab\ \}$. If $b \geq c_0$, then $c = ab$ is the conductor of H and $g = (a-1)b + g_0$ is the number of gaps of H, by Lemma 3.15.

Theorem 2.15. *Let d be a positive integer. Let $\tilde{C}(d)$ be an improved geometric Goppa code of a function field with an inductive Weierstrass semigroup. Then the redundancy of $\tilde{C}(d)$ is at most r_d and*

$$r_d = \rho_{\lceil \frac{d}{2} \rceil} + \lfloor \tfrac{d}{2} \rfloor.$$

Proof. See next section. □

Example 2.16. Let $H = \{0, g+1, g+2, g+3, \ldots\}$. Then H is inductive. See Example 3.14. The Weierstrass semigroup of a general point of a general curve of genus g is of this type.

Example 2.17. Let $\mathcal{F}$ be a hyperelliptic funtion fields of genus g. Let Q be a rational hyperelliptic point, that is to say $L(2Q)$ has dimension 2. Then

$$H(Q) = 2\mathbb{N}_0 \cup \{\ n \in \mathbb{N}_0\ :\ n \geq 2g\ \}.$$

and the conductor of $H(Q)$ is $2g$. So $H(Q)$ is inductive. See Example 3.14. In Example 3.17 this example will be generalized.

The number of rational places of a hyperelliptic function field over the finite field $\mathbb{F}_q$ is at most $2q + 2$. Hence the length of an improved hyperelliptic code is at most $2q + 1$.

Example 2.18. Consider the Klein quartic with homogenuous equation

$$x^3y + y^3z + z^3x = 0.$$

The Weierstrass semigroup of the point $Q = (1 : 0 : 0)$ at infinity is $H(Q) = \{0, 3, 5, 6, 7 \ldots\}$. So $H(Q) = 3\mathbb{N}_0 \cup \{n \in \mathbb{N}_0 | n \geq 5\}$. But $H(Q)$ is not inductive, since the conductor is not divisible by 3.

In [2] the Weierstrass semigroup H of points of the curves with homogenuous equation

$$x^m y + y^m z + z^m x = 0$$

are computed:

$$H = \mathbb{N}_0 \setminus \{\ i + j(m-1) \mid 0 \leq j \leq i-1 \leq m-2\ \}.$$

We leave it to the reader to verify that $H = aH_0 \cup \{n \in \mathbb{N}_0 | n \geq c\}$ for some semigroup H_0 and positive integers a and c if and only if $m \leq 3$.

Example 2.19. The tower $(\mathcal{T}_m : m \in \mathbb{N})$ of function fields over $\mathbb{F}_q$ with $q = r^2$ is given in [8] as follows. Let $\mathcal{T}_1 = \mathbb{F}_q(x_1)$. Let $\mathcal{T}_m$ be obtained from $\mathcal{T}_{m-1}$ by adjoining a new element x_m that satisfies the equation:

$$x_m^r + x_m = \frac{x_{m-1}^r}{x_{m-1}^{r-1} + 1}\,.$$

Let Q_m be the rational place on the function field $\mathcal{T}_m$ that is the unique pole of x_1.

Let H_m be the Weierstrass semigroup of Q_m. Then Q_m is totally ramified over Q_{m-1} for all $m > 1$. In [16] it was shown that $H_1 = \mathbb{N}_0$ and

$$H_m = r \cdot H_{m-1} \cup \{n \in \mathbb{N}_0 \ :\ n \geq c_m\}\,,$$

where

$$c_m = \begin{cases} r^m - r^{\frac{m+1}{2}} & \text{if } \ m \text{ is odd,} \\ r^m - r^{\frac{m}{2}} & \text{if } \ m \text{ is even.} \end{cases}$$

So the tower is inductive.

3. Numerical sets and semigroups

The sets we have in mind in this section are certain Weierstrass semigroups at rational places of function fields, however we will consider a more general setting.

Definition 3.1. A non-empty subset H of $\mathbb{N}_0$ is called a *numerical set* if its complement is finite. The number $g = g(H) := \#(\mathbb{N}_0 \setminus H)$ is called the *genus* of H. The largest element $c = c(H) \in H$ such that $c - 1 \notin H$ is called the *conductor* of H. The elements of H, say $\rho_1 = \rho_1(H) < \rho_2 = \rho_2(H) < \cdots$, are called the *non-gaps* of H. The elements of $G = G(H) := \mathbb{N}_0 \setminus H$, say $\ell_1 = \ell_1(H) < \cdots < \ell_g = \ell_g(H)$, are called the *gaps* of H.

A *numerical semigroup* is a numerical set which is a subsemigroup of $(\mathbb{N}_0, +)$.

For $a, b \in \mathbb{N}_0$, we set $[a, b] := \{x \in \mathbb{N}_0 : a \leq x \leq b\}$.

Remark 3.2. Let H be a numerical set of genus g and $C \in \mathbb{N}$ such that $C \geq c(H)$. Then,

(1) $\rho_{l+1}(H) = g + l$ for $l \geq C - g$. This follows from $G(H) \subseteq [0, c(H)] \subseteq [0, C]$.
(2) H has at least g non-gaps in $[1, 2g]$.

Remark 3.3. Let H be a numerical semigroup of genus g. Then,

(1) $\rho_1 = 0$, and $\rho_2 = 1$ iff $g = 0$.
(2) we have that $c = c(H) \leq 2g$, i.e. $\rho_{g+1} = 2g, \rho_{g+2} = 2g+1, \ldots$. In fact, suppose that $c \geq 2g+1$. Let $n_1, \ldots, n_g$ be non-gaps of H in $[1, 2g]$ (cf. Remark 3.2 (2)). Then H would have $g+1$ gaps, namely $c-1, c-1-n_g, \ldots, c-1-n_1$, a contradiction.
(3) If $\rho_2 = 2$, then $\rho_i = 2(i-1)$, $i = 2, \ldots, g+1$. In particular, $c(H) = 2g$.
(4) If $\rho_2 \geq 3$, then $\rho_i \geq 2i-1$, $i = 2, \ldots, g-1$, and $\rho_g \geq 2g-2$ (see e.g. [14, Thm. 1.1]).
(5) H is called *symmetric* iff $c(H) = 2g$. It follows, from the definition of $c(H)$, that H is symmetric iff $\ell_g = 2g-1$. Consequently, H is symmetric iff for each $n \in \mathbb{Z}$ holds

$$n \ \in \ H \ \Leftrightarrow \ \ell_g - n \notin \ H.$$

Let $H = (\rho_l : l \in \mathbb{N})$ be a numerical set. As in Definition 2.3 and Definition 2.9, we consider

$$\nu_l = \nu_l(H) := \#\{(i,j) \in \mathbb{N}^2 : \rho_i + \rho_j = \rho_{l+1}\}\,, \qquad l \in \mathbb{N}_0\,,$$

and

$$r_d = r_d(H) := \#\{i \in \mathbb{N} : \nu_{i-1} \leq d-1\}\,, \qquad d \in \mathbb{N}_0\,.$$

Associate to these numbers we have

$$s_d = s_d(H) := \#\{i \in \mathbb{N} : \nu_{i-1} = d-1\}\,, \qquad d \in \mathbb{N}_0\,.$$

We have that $r_0 = s_0 = 0$, $\nu_0 \leq 1$, and $\nu_0 = 1$ iff $\rho_1 = 0$. Moreover

$$r_d = r_{d-1} + s_d \qquad \text{for } d \in \mathbb{N}\,. \tag{3.1}$$

Lemma 3.4. *Let $H = (\rho_l : l \in \mathbb{N})$ be a numerical set of genus g. For $l \in \mathbb{N}$ set*

$$\mu_l = \mu_l(H) := \#\{i \in [1, \rho_{l+1} - 1] : i,\ \rho_{l+1} - i \in G(H)\}\,.$$

(1) *Then $\nu_l = 2l + 1 - \rho_{l+1} + \mu_l$.*
(2) *Let $C \in \mathbb{N}$ such that $C \geq c(H)$. Then*

$$\mu_l = \begin{cases} \rho_{l+1} - 2l + 1 + \mu_l^0 & \text{if } \rho_1 = 0 \text{ and } 1 \leq l \leq C-g-1, \\ \rho_{l+1} - 2l - 1 + \mu_l^0 & \text{if } \rho_1 > 0 \text{ and } 1 \leq l \leq C-g-1, \\ 2g + 2j - \rho_{l+1} - 3 + \mu_l^j & \text{if } l \in [C-g+\rho_{j-1}, C-g+\rho_j - 1]; \\ & j = 1, \ldots, C-g, \\ 2C - \rho_{l+1} - 1 & \text{if } \rho_{C-g} + C - g \leq l \leq 2C-g-1, \\ 0 & \text{if } l \geq 2C-g, \end{cases}$$

where $\rho_0 := 0$,

$$\mu_l^0 = \mu_l^0(H, C) := \#\{i \in [1, \rho_{l+1} - 1] : i, \rho_{l+1} - i \in H\}\,, \tag{3.2}$$

and

$$\mu_l^j = \mu_l^j(H, C) := \#\{\rho_{l+1} - \rho_{C-g}, \ldots, \rho_{l+1} - \rho_j\} \cap H \qquad j = 1, \ldots, C - g\,. \tag{3.3}$$

Proof. (1) We have that

$$\{(i, j) \in \mathbb{N}^2 : \rho_i + \rho_j = \rho_{l+1}\} = \{(a, b) \in \mathbb{N}_0^2 : a + b = \rho_{l+1}\} \setminus (\mathcal{A} \cup \mathcal{B})\,,$$

where

$$\mathcal{A} := \{(a, b) \in \mathbb{N}_0^2 : a + b = \rho_{l+1},\ a \in G(H)\}$$

and

$$\mathcal{B} := \{(i, j) \in \mathbb{N}_0^2 : i + j = \rho_{l+1},\ j \in G(H)\}.$$

By symmetry $\#\mathcal{A} = \#\mathcal{B}$ and this number is equal to $\rho_{l+1} - l$. Then $\nu_l = (\rho_{l+1} + 1) - 2(\rho_{l+1} - l) + \#(\mathcal{A} \cap \mathcal{B})$. Since

$$(i, j) \in \mathcal{A} \cap \mathcal{B} \ \Leftrightarrow\ 0 < i < \rho_{l+1},\ i,\ \rho_{l+1} - i\ \in G(H)\,,$$

the proof follows.

(2) Let $i \in [1, \rho_{l+1} - 1]$ be such that $i, \rho_{l+1} - i \in G(H)$. Since $G(H) \subseteq [0, c(H) - 1] \subseteq [0, C - 1]$ we have that

$$\max(1, \rho_{l+1} - C + 1)\ \leq\ i \leq\ \min(C - 1, \rho_{l+1} - 1).$$

In particular, $\mu_l = 0$ provided that $\rho_{l+1} \geq 2C - 1$ so we obtain Lemma 3.4(2) for $l \geq 2C - g$. Let $\rho_{l+1} \leq 2C - 2$. We consider two cases according as $\rho_{l+1} \leq C - 1$ ($\Leftrightarrow 0 \leq l \leq C - g - 1$; cf. Remark 3.2 (1)) or $\rho_{l+1} \geq C$ ($\Leftrightarrow l \geq C - g$; cf. loc. cit.).

Case 1: $\rho_{l+1} \in\ [1, C - 1]$: Here we have

$$\begin{aligned}\mu_l &= \rho_{l+1} - 1 - \#\{i \in [1, \rho_{l+1} - 1] : i \in H \text{ or } \rho_{l+1} - i \in H\} \\ &= \rho_{l+1} - 1 - 2\#([1, \rho_{l+1} - 1] \cap H) + \mu_l^0\,.\end{aligned}$$

Now, since

$$\#\ [1, \rho_{l+1} - 1] \cap H = \begin{cases} l - 1 & \text{if } \rho_1 = 0\,, \\ l & \text{if } \rho_1 > 0\,, \end{cases}$$

we obtain Lemma 3.4(2) for $l \in [1, C - g - 1]$.

Case 2: $\rho_{l+1} \in [C, 2C - 2]$: Here we have

$$\mu_l = 2C - \rho_{l+1} - 1 - \#\{i \in [\rho_{l+1} - C + 1, C - 1] : i \in H \text{ or } \rho_{l+1} - i \in H\}\,.$$

Since $C = \rho_{C-g+1}$ (Remark 2.2(1)), there exists $j \in \{1, \ldots, C-g+1\}$ such that $\rho_{l+1} \in [\rho_{j-1} + C, \rho_j + C - 1]$ (we set $\rho_0 := 0$). Moreover, if $i \in H$ then

$$i \in [\rho_{l+1} - C + 1, C - 1] \qquad \Leftrightarrow \qquad i \in \{\rho_j, \ldots, \rho_{C-g}\}. \tag{3.4}$$

Consequently

$$\mu_l = 2C - \rho_{l+1} - 1 - 2(C - g - j + 1) + \#\{\rho_{l+1} - \rho_{C-g}, \ldots, \rho_{l+1} - \rho_j\} \cap H$$

and we obtain Lemma 3.4(2) for $C - g \leq l \leq 2C - g - 1$.. □

Proposition 3.5. *Let $H = (\rho_l : l \in \mathbb{N})$ be a numerical set of genus g and $C \in \mathbb{N}$ such that $C \geq c(H)$. Then*

$$\nu_l = \begin{cases} 1 \text{ (resp. } 0) & \text{if } \rho_1 = 0 \text{ (resp. } \rho_1 \geq 1); \ l = 0, \\ \mu_l^0 + 2 \text{ (resp. } \mu_l^0) & \text{if } \rho_1 = 0 \text{ (resp. } \rho_1 \geq 1); \ 1 \leq l \leq C - g - 1, \\ \mu_l^j + 2j - 2 & \text{if } l \in [C - g + \rho_{j-1}, C - g + \rho_j - 1]; \\ & j = 1, \ldots, C - g, \\ 2C - 2g & \text{if } l \in [C - g + \rho_{C-g}, 2C - g - 1], \\ l - g + 1 & \text{if } l \geq 2C - g. \end{cases}$$

Proof. We have that $r_0 = s_0 = 0$, $\nu_0 \leq 1$, and $\nu_0 = 1$ iff $\rho_1 = 0$ as remarked before, so we can assume $l \geq 1$, i.e. $\rho_{l+1} \geq 1$. The proof of the proposition follows from Remark 3.2 (1) and Lemma 3.4. □

Example 3.6. We compute the numbers ν_l for the semigroup H generated by two consecutive integers q and $q+1$, as is the case for the Weierstrass semigroup of a rational point of the Hermitian function field. We have $c(H) = 2g(H)$, $g := g(H) = q(q-1)/2$, and then, by Proposition 3.5, it is enough to consider $l \leq g + \rho_g - 1 = 3g - 3$.

(1) For $0 \leq l \leq g - 1$, let $l = i(i+1)/2 + j$ where $i = 0, \ldots, q-2$ and $j = 0, \ldots, i$. Then $\rho_{l+1} = iq + j = (i-j)q + j(q+1)$ and from [10, Lemma 5.7] or Proposition 3.5 we have that

$$\nu_l = (i - j + 1)(j + 1).$$

(2) Let $l \in \cup_{j=2}^{g} [g + \rho_{j-1}, g + \rho_j - 1]$, $l = g + \rho_{j-1} + m$, $m \in \{0, \ldots, \rho_j - \rho_{j-1} - 1\}$. Then from Proposition 3.5 we have that

$$\nu_l = \rho_j - (m^2 - m(\rho_j - \rho_{j-1} - 1)).$$

Remark 3.7. Let H and C be as in Proposition 3.5. Then $\mu_l^0 \leq l - 1$ (resp. $\mu_l^0 \leq l$) if $\rho_1 = 0$ (resp. $\rho_1 > 0$), and $\mu_l^j \leq C - g - j + 1$ for $j = 1, \ldots, C - g$. Then from Proposition 3.5 we have that

(1) $\nu_l \leq 2C - 2g$ iff $l \leq 2C - g - 1$;
(2) $\nu_l \leq 2C - 2g - 1$ iff $l \leq C - g + \rho_{C-g} - 1$.

Part (2) of the following corollary is Theorem 3.9 of [12].

Corollary 3.8. *Let H and C be as in Proposition 3.5. Then*

(1) $s_d = 1$ *if* $d \geq 2C - 2g + 2$;
(2) $r_d = d + g - 1$ *if* $d \geq 2C - 2g + 1$;
(3) $r_{2C-2g} = \rho_{C-g} + C - g$;
(4) $s_{2C-2g+1} = \rho_{C-g+1} - \rho_{C-g}$.

Proof. (1) It follows by Remark 3.2 (1) and Proposition 3.5.

(2) By Remark 3.7(1), $r_{2C-2g+1} = (2C - 2g + 1) + g - 1$ and then the proof follows from Eq. (3.1) and item (1).

(3) It follows from Remark 3.7(2).

(4) It follows from Eq. (3.1). □

Then if H and C are as above, Corollary 3.8 and Remark 3.2 (1) imply

$$r_d = \rho_{\lceil \frac{d}{2} \rceil} + \lfloor \tfrac{d}{2} \rfloor \,, \tag{3.5}$$

provided that $d \geq 2C - 2g$, or equivalently

$$s_d = \begin{cases} 1 & \text{if } d \text{ is even,} \\ \rho_{\frac{d+1}{2}} - \rho_{\frac{d-1}{2}} & \text{if } d \text{ is odd,} \end{cases} \tag{3.6}$$

provided that $d \geq 2C - 2g + 1$.

Question 3.9. Which H do satisfy (3.5) for each $d \in [0, 2c(H) - 2g(H) - 1]$, or equivalently (3.6) for each $d \in [1, 2c(H) - 2g(H)]$?

Next we are going to study Condition (3.6). For $C \geq c(H)$, we set

- $I^{(0)} = I^{(0)}(H, C) := [0, C - g - 1]$;
- $I^{(j)} = I^{(j)}(H, C) := [C - g + \rho_{j-1}, C - g + \rho_j - 1]$ for $j = 1, \ldots, C - g$;
- $S^j_d(H, C) := \{i \in \mathbb{N} : i - 1 \in I^{(j)},\ \nu_{i-1} = d - 1\}$, $d \in \mathbb{N}$, $j = 0, 1, \ldots, C - g$;
- $s^j_d := \# S^j_d(H, C)$.

Remark 3.10. Let $j = 1, \ldots, C - g$.

(1) By Proposition 3.5, $s^j_d = \#\{i \in \mathbb{N} : i - 1 \in I^{(j)},\ \mu^j_{i-1} = d - 2j + 1\}$. Since $0 \leq \mu^j_{i-1} \leq C - g - j + 1$ we then have that $s^j_d > 0$ implies $2j - 1 \leq d \leq C - g + j$. Therefore

$$\sum_{d=2j-1}^{C-g+j} s^j_d = \rho_j - \rho_{j-1} \,.$$

(2) $s^j_{C-g+j} \in \{0, 1\}$. In fact, suppose that $s^j_{C-g+j} > 0$. Then, by relation (3.4), there exists $i \in \mathbb{N}$ such that $\{\rho_i - \rho_{C-g}, \ldots, \rho_i - \rho_j\} = \{\rho_j, \ldots, \rho_{C-g}\}$; hence ρ_i is uniquely determinated by the conditions

$$(*) \qquad \rho_i = \rho_j + \rho_{C-g} = \rho_{j+l} + \rho_{C-g-l} \quad l = 0, \ldots C - g - j \,.$$

Notice that Remark 3.2 (1) implies $i-1=\rho_j+\rho_{C-g}-g$, and then

$$(**) \qquad C-\rho_{C-g}=\rho_{C-g+1}-\rho_{C-g}\leq \rho_j-\rho_{j-1}.$$

Conversely, conditions $(*)$ and $(**)$ imply $s^j_{C-g+j}=1$

Corollary 3.11. *Let H and C be as in Proposition 3.5.*

(1) *For $\bar{l}=0,\ldots,C-g-1$ we have*

$$s_{2\bar{l}+1}=\rho_{\bar{l}+1}-\rho_{\bar{l}}-\sum_{d=2\bar{l}+2}^{C-g+\bar{l}+1}s^{\bar{l}+1}_d+s^0_{2\bar{l}+1}+\sum_{j=\max(1,2\bar{l}+1-(C-g))}^{\bar{l}}s^j_{2\bar{l}+1}\ ,$$

$$s_{2\bar{l}+2}=s^0_{2\bar{l}+2}+\sum_{j=\max(1,2\bar{l}+2-(C-g))}^{\bar{l}+1}s^j_{2\bar{l}+2}\,.$$

(2) $s^0_d=0$ *provided that* $d\geq C-g+2$.

Proof. See also Proposition 3.6 of [4].
(1) For $d\leq 2C-2g$, by Proposition 3.5, $s_d=\sum_{j=0}^{C-g}s^j_d$. Now the results follows from Remark 3.10(1).

(2) It follows from the fact that $\nu_l\leq C-g$ whenever $l\in I^{(0)}$. □

Corollary 3.12. *Let H and C be as in Proposition 3.5. Then $s_{2C-2g}\in[0,1]$ and $s_{2C-2g-1}\in[\rho_{C-g}-\rho_{C-g-1}-1,\rho_{C-g}-\rho_{C-g-1}+1]$. Moreover,*

(1) *If $C-g\geq 2$, then* $s_{2C-2g}=1\Leftrightarrow \rho_{C-g+1}-\rho_{C-g}\leq\rho_{C-g}-\rho_{C-g-1}$.
(2) *If $C-g\geq 3$, then*

$$\begin{aligned}
s_{2C-2g-1}=\rho_{C-g}-\rho_{C-g-1}+1 \Leftrightarrow\ & \rho_{C-g+1}-\rho_{C-g}>\rho_{C-g}-\rho_{C-g-1}, \quad \textit{and}\\
& \rho_{C-g+1}-\rho_{C-g}\leq\rho_{C-g-1}-\rho_{C-g-2};\\
s_{2C-2g-1}=\rho_{C-g}-\rho_{C-g-1}\Leftrightarrow\ & \rho_{C-g+1}-\rho_{C-g}\leq\rho_{C-g}-\rho_{C-g-1}, \quad \textit{and}\\
& \rho_{C-g+1}-\rho_{C-g}\leq\rho_{C-g-1}-\rho_{C-g-2}; \quad \textit{or}\\
\rho_{C-g+1}-\rho_{C-g}>\rho_{C-g}-\rho_{C-g-1} \quad \textit{and}\ & \rho_{C-g+1}-\rho_{C-g}>\rho_{C-g-1}-\rho_{C-g-2};\\
s_{2C-2g-1}=\rho_{C-g}-\rho_{C-g-1}-1\Leftrightarrow\ & \rho_{C-g+1}-\rho_{C-g}\leq\rho_{C-g}-\rho_{C-g-1}, \quad \textit{and}\\
& \rho_{C-g+1}-\rho_{C-g}>\rho_{C-g-1}-\rho_{C-g-2}.
\end{aligned}$$

Proof. The case $\bar{l}=C-g-1$ in Corollary 3.11 gives $s_{2C-2g}=s^{C-g}_{2C-2g}$ and $s_{2C-2g-1}=\rho_{C-g}-\rho_{C-g-1}-s^{C-g}_{2C-2g}+s^{C-g-1}_{2C-2g-1}$. Now the result follows from Remark 3.10. □

Recall that a symmetric numerical semigroup H satisfies: (i) $c=c(H)=2g=2g(H)$, (ii) $\rho_{g+1}=2g$, $\rho_g=2g-2$, $\rho_{g-1}=2g-3$ and $\rho_{g-2}\geq 2g-5$ provided that $\rho_2\geq 3$ (see Remark 3.2(4)(5)).

Corollary 3.13. *Let H be a symmetric numerical semigroup of genus g and conductor c $(= 2g)$. If $\rho_2 \geq 3$, then*

(1) $s_{2c-2g} = 0$;
(2) $s_{2c-2g-1} \in [\rho_{c-g} - \rho_{c-g-1}, \rho_{c-g} - \rho_{c-g-1} + 1]$. *Moreover,*
   (a) $s_{2c-2g-1} = \rho_{c-g} - \rho_{c-h-1} \Leftrightarrow \rho_{c-g-2} = 2g - 4$;
   (b) $s_{2c-2g-1} = \rho_{c-g} - \rho_{c-h-1} + 1 \Leftrightarrow \rho_{c-g-2} = 2g - 5$.

In particular, H does not satisfy condition (3.6) and is not inductive.

Proof. It follows from Corollary 3.12, with $C = c(H)$, and the remarks above concerning symmetric numerical semigroups. □

Example 3.14. The following numerical semigroups satisfy (3.6) for each $d \in \mathbb{N}$:

(1) $H = \{0, g+1, g+2, \ldots\}$.
(2) H hyperellitpic, i.e. $\rho_2(H) = 2$.

In fact, in the first case $\rho_i(H) = g + i - 1$ for $i \geq 2$ so that $g(H) = g$, and $c(H) = g + 1$ (resp. 0) if $g \neq 0$ (resp. $g = 0$). Then from Proposition 3.5 we have

$$\nu_l = \begin{cases} 1 & \text{if } l = 0, \\ 2 & \text{if } 1 \leq l \leq g+1, \\ l - g + 1 & \text{if } l \geq g+2, \end{cases}$$

provided that $g \neq 0$; otherwise $\nu_l = l + 1$ for each $l \in \mathbb{N}_0$. So it is clear that H satisfies (3.6).

Let now $\rho_2 = 2$. We have seen in Remark 3.3(3) that $\rho_i = 2(i-1)$, $i = 2, \ldots, g+1$ and that $\rho_i = i + g - 1$. It follows then that

$$\nu_l = \begin{cases} l + 1 & \text{if } 0 \leq l \leq g - 1, \\ 2\bar{l} \text{ (resp. } g + \bar{l}) & \text{if } l = g + 2\bar{l} - 1 \text{ (resp. } l = g + 2\bar{l} - 2); \\ & g \leq l \leq 3g - 1, \bar{l} \in \{1, \ldots, g\}, \\ l - g + 1 & \text{if } l \geq 3g. \end{cases}$$

From these formulae it is easy to see that H fulfils (3.6).

From now on we study numerical sets of type

$$\tilde{H} := aH \cup \{x \in \mathbb{N} : x \geq \tilde{c}\},$$

where $a, \tilde{c} \in \mathbb{N} \setminus \{1\}$, and $H = (\rho_l : l \in \mathbb{N})$ is a numerical set. Clearly we have that

- $\tilde{H}$ is a semigroup if H does;
- $c(\tilde{H}) \leq \tilde{c}$.

Now we relate the genus and the conductor of $\tilde{H}$ with those of H. We set $\rho_i := \rho_i(H)$ and $\tilde{\rho}_i := \rho_i(\tilde{H})$. We can assume $\tilde{c} > a\rho_1$ (otherwise $\tilde{H} = \{\tilde{c}, \tilde{c}+1, \ldots\}$). Thus there exists $I \in \mathbb{N}$ such that $a\rho_I < \tilde{c} \leq a\rho_{I+1}$, i.e.

$$\tilde{H} = \{a\rho_1, \ldots, a\rho_I\} \cup \{\tilde{c}, \tilde{c}+1 \ldots\}. \tag{3.7}$$

We can easily prove the

Lemma 3.15. *With the above notations and assumption we have:*

(1) *If $\tilde{c} - 1 > a\rho_I$, then $c(\tilde{H}) = \tilde{c}$.*
(2) *If $\tilde{c} - 1 = a\rho_I$, then $c(\tilde{H}) = a\rho_I = \tilde{c} - 1$.*
(3) *$\tilde{g} := g(\tilde{H}) = \tilde{c} - I$.*

If in addition we suppose that

(I) *$\tilde{c} = ab$ with $b \geq c := c(H)$, say $b = \rho_{l+1} = g(H) + l$ (cf. Remark 3.2(1)),*

then $I = l = b - g(H)$ so that

4 *$c(\tilde{H}) = \tilde{c}$.*
5 *$\tilde{g} = g(\tilde{H}) = (a-1)b + g$, where $g = g(H)$.*

Proposition 3.16. *With the above notations and assumptions, if H satisfies condition* (3.6) *for each $d \in \mathbb{N}$, then $\tilde{H}$ does.*

Proof. We have to show that $\tilde{H}$ satisfies (3.6) for each $d \in [1, 2\tilde{c} - 2\tilde{g}]$. We are going to apply Proposition 3.5 and its corollaries to $\tilde{H}$ and $C = \tilde{c}$, and to H and $C = b$. Notice that $\tilde{c} - \tilde{g} = b - g$ by the above lemma and by condition (I), and recall that $\tilde{H}$ satisfies (3.7) with $I = \tilde{c} - \tilde{g}$ and $\tilde{\rho}_i = a\rho_i$ for each $i = 1, \ldots, \tilde{c} - \tilde{g}$.

For $j = 0, 1, \ldots, \tilde{c} - \tilde{g} = b - g$, we set (see notations after Question 3.9, (3.2) and (3.3)):

- $S_d^j := S_d^j(H, b)$ and $s_d^j := \#S_d^j$;
- $\mu_i^j := \mu_i^j(H, b)$;
- $\tilde{S}_d^j := S_d^j(\tilde{H}, \tilde{c})$ and $\tilde{s}_j := \#S_d^j$;
- $\tilde{\mu}_i^j := \mu_i^j(\tilde{H}, \tilde{c})$.

Claim. For each j and d as above, $\tilde{s}_d^j = s_d^j$.

Proof. (*Claim*) Let $j \geq 1$; from Proposition 3.5, Remark 3.2(1) and (3.3) we have that

$$i \in S_d^j \Leftrightarrow \rho_i \in [b + \rho_{j-1}, b + \rho_j - 1] \quad \text{and}$$
$$\#\{\rho_i - \rho_{b-g}, \ldots, \rho_i - \rho_j\} \cap H = \mu_{i-1}^j = d - 2j + 1\,.$$

Since $\{\rho_i - \rho_{b-g}, \ldots, \rho_i - \rho_j\} \cap H \subseteq \{\rho_j, \ldots, \rho_{b-g}\}$ (see (3.4)) we conclude that for each ρ_i above, there exist exactly μ_{i-1}^j pairs $(\alpha, \beta) \in \{j, \ldots, b-g\}^2$ such that $\rho_\alpha + \rho_\beta = \rho_i$. Let $I \in \mathbb{N}$ uniquely defined by $a\rho_i = \tilde{\rho}_I$. Next we show that $I \in \tilde{S}_d^j$. This follows

because $\mu_{i-1}^j = \tilde{\mu}_{I-1}^j$ and $\tilde{\rho}_I \in [\tilde{c} + \tilde{\rho}_{j-1}, \tilde{c} + \tilde{\rho}_j - 1]$. We conclude that the map $i \mapsto I$ ($a\rho_i = \tilde{\rho}_I$) provides a bijection between S_d^j and $\tilde{S}_d^j$.

The case $j = 0$ is proved in a similar way. □

Now Proposition 3.16 follows from the claim, (3.7), and Corollary 3.11. □

Now we can prove Theorem 2.15.

Proof. (*Theorem 2.15*) By Example 3.14(1) $H_1 = \mathbb{N}_0$ satisfies (3.5) and then we apply induction by means of Proposition 3.16. □

Example 3.17. Let g be a non-negative integer. A function field K over $\mathbb{F}_q$ is called *g-hyperelliptic* if it is a degree two field extension of a function field L over $\mathbb{F}_q$ of genus g. Let P be a (totally) ramified place of K over Q of L, and suppose that it is $\mathbb{F}_q$-rational (in general notice that P has degree one or two by the Fundamental Equality on places). In [18] it has been studied the type of the Weierstrass semigroup at P. In fact, the even elements of $H(P)$ are

$$2\rho_1, 2\rho_2, \ldots, 2\rho_{g+1} = 4g, 4g+2, 4g+4, \ldots ,$$

where $\rho_1, \rho_2, \ldots, \rho_{g+1}$ are the first $g+1$ Weierstrass non-gaps of the place Q of L, while the odd elements of $H(P)$ are

$$s_g < \ldots < s_1 < 2\tilde{g} + 1 < 2\tilde{g} + 3 < \ldots ,$$

where $\tilde{g}$ is the genus of K. Therefore semigroups of type (3.7) appear as Weierstrass semigroups of places P as above provided that

$$s_g = 2\tilde{g} - 2g + 1 .$$

If in addition, $H(Q)$ is inductive, then $H(P)$ is inductive. If in particular, $\rho_i = g + i - 1$ for $i \geq 2$, then $H(P)$ is inductive and satisfies (3.6) for each d as follows from Example 3.14(1) and Proposition 3.16.

4. Asymptotically good codes

We have seen that in every stage of the tower of Example 2.19 we get improvements of the Goppa bound. In this section we will see that we do not get asymptotic improvements.

Remark 4.1. Algebraic geometry codes satisfy Goppa's bound $k + d \geq n + 1 - g$, where k is the dimension, d the minimum distance and n the length of the code, and g the genus of the function field. The number of rational places is an upperbound for n.

The Tsfasman-Vlăduţ-Zink (TVZ) bound [19, 20] says that there are asymptotically good sequences of algebraic geometry codes over $\mathbb{F}_q$ such that the limit R of the information rate and the limit of the relative minimum distance δ satisfy the inequality

$$R + \delta \geq 1 - \frac{1}{\sqrt{q} - 1},$$

for all R such that $0 \leq R \leq 1$, if q is a square.

If moreover $q \geq 49$, then this bound is better than the Gilbert-Varshamov (GV) bound for intermediate values of the information rate.

In [15] an improvement of the TVZ bound was obtained for high rates but it was still below the Gilbert-Varshamov bound.

We are interested in the asymptotic behaviour of the parameters of the codes $\tilde{C}(d)$ coming from a tower of function fields $(\mathcal{F}_m : m \in \mathbb{N})$ with known semigroups, since they are candidates for an improvement of the TVZ bound.

Example 4.2. Consider the tower of function fields $(\mathcal{T}_m : m \in \mathbb{N})$ of Example 2.19. The number N_m of $\mathbb{F}_q$-rational points of $\mathcal{T}_m$ is equal to

$$N_m = (r^2 - r)r^{m-1} + \begin{cases} r^{\frac{m+1}{2}} + r^{\frac{m-1}{2}} & \text{if } m \text{ is odd,} \\ 2r^{\frac{m}{2}} & \text{if } m \text{ is even.} \end{cases}$$

The genus g_m of the function field $\mathcal{T}_m$ is equal to

$$g_m = \begin{cases} (r^{\frac{m+1}{2}} - 1)(r^{\frac{m-1}{2}} - 1) & \text{if } m \text{ is odd,} \\ (r^{\frac{m}{2}} - 1)^2 & \text{if } m \text{ is even.} \end{cases}$$

Hence this sequence of function fields attains the Drinfeld-Vlăduţ (DV) bound [19, 20]. So the sequence of function fields is asymptotically optimal, but this does not mean that every function field $\mathcal{T}_m$ is optimal. For instance $\mathcal{T}_2$ is a function field over $\mathbb{F}_{16}$ of genus 9 with 56 rational places. The Hermitian function field over $\mathbb{F}_{16}$ has genus 6 and 65 rational places.

Remark 4.3. Assume that twice the conductor c of the Weierstrass semigroup is smaller than N, the number of rational places. This assumption is for instance satisfied for towers over $\mathbb{F}_q$, $q > 9$ attaining the DV bound, since $c \leq 2g$ and $g \leq N/(\sqrt{q} - 1)$.

Let $l_0 = 2c - g$ and $d_0 = 2(c - g) + 1$. Then

$$d_{ORD}(l_0) = d_G(l_0) = l_0 + 1 - g = d_0$$

and

$$d_{ORD}(l) = d_G(l) = l + 1 - g \quad \text{for all} \quad l \geq l_0$$

by Theorem 2.5. Furthermore $r_d = d + g - 1$ for all $d \geq d_0$ by Corollary 3.8. Now

$$\rho_{l_0} = l_0 + g - 1 = 2c - 1 < N - 1 = n,$$

by assumption. So C_l has redundancy l for all $l \leq l_0$, by Remark 2.6.

In other words: in the range $d < d_0$ where we can expect an improvement of the redundancy of the improved geometric Goppa code $\tilde{C}(d)$, the number r_d is the exact value of this redundancy. The difference $e = c - g$ is a measure for the improvement.

We restrict ourselves to a tower $(\mathcal{F}_m : m \in \mathbb{N})$ of function fields with an inductive tower $(H_m : m \in \mathbb{N})$ of Weierstrass semigroups.

Let N_m be the number of $\mathbb{F}_q$-rational places of $\mathcal{F}_m$. Let a_m be the degree of the extension of $\mathcal{F}_m$ over $\mathcal{F}_{m-1}$. Suppose that $a_m > 1$ for all m. We may assume that $N_m \geq \prod_{i=2}^{m} a_i$, since otherwise the expected redundancy r_d of $\tilde{C}(d)$ is larger than the possible length $N_m - 1$ of the code, since

$$r_d \geq r_3 = \rho_2 + 1 = \prod_{i=2}^{m} a_i + 1 \quad \text{for all} \quad d > 2,$$

by Theorem 2.15.

The limit

$$\epsilon = \lim_{m \to \infty} (c_m - g_m)/N_m$$

is an asymptotic measure for an improvement of the TVZ bound, by Remark 4.3. The next proposition shows that we can not expect an asymptotic improvement of the code parameters for such codes.

Proposition 4.4. *Let $(\mathcal{F}_m : m \in \mathbb{N})$ be a tower of function fields with an inductive tower $(H_m : m \in \mathbb{N})$ of Weierstrass semigroups. Suppose that $N_m \geq \prod_{i=2}^{m} a_i$ and that the limit*

$$\lim_{m \to \infty} \frac{c_m - g_m}{N_m}$$

exists and is equal to $\epsilon > 0$. Then the tower is not asymptotically good, that is to say

$$\lim_{m \to \infty} \frac{N_m}{g_m} = 0.$$

Proof. If $\epsilon > 0$, then there exists an m_0 such that $b_{m-1} \geq \epsilon N_m/2 + g_{m-1}$ for all $m \geq m_0$, since $b_{m-1} - g_{m-1} = c_m - g_m$. Let $\delta = \min\{\epsilon/2, b_{m_0}\}$. Then $\delta > 0$. We show by induction that

$$g_m \geq \delta(m - m_0) \prod_{i=m_0+1}^{m} a_i$$

for all $m > m_0$. The inequality is true for $m = m_0 + 1$, since

$$g_{m_0+1} = a_{m_0+1} b_{m_0} + g_{m_0} \geq a_{m_0+1} b_{m_0} \geq \delta a_{m_0+1}.$$

Suppose that the inequality is true for $m > m_0$. Then

$$\begin{aligned} g_{m+1} &= (a_{m+1}-1)b_m + g_m \\ &\geq (a_{m+1}-1)(\delta N_{m+1} + g_m) + g_m \\ &\geq \delta N_{m+1} + a_{m+1} g_m \\ &\geq \delta \textstyle\prod_{i=2}^{m+1} a_i + \delta(m-m_0) \prod_{i=m_0+1}^{m+1} a_i \\ &\geq \delta(m+1-m_0) \textstyle\prod_{i=m_0+1}^{m+1} a_i. \end{aligned}$$

This proves the claim about the lower bound for g_m. But for the number of rational points N_m we have that $N_m \leq N_{m_0} \prod_{i=m_0+1}^{m} a_i$, since $\prod_{i=m_0+1}^{m} a_i$ is the degree of the extension of $\mathcal{F}_m$ over $\mathcal{F}_{m_0}$. So

$$g_m \geq \delta(m-m_0) \prod_{i=m_0+1}^{m} a_i \geq \frac{\delta(m-m_0)}{N_{m_0}} N_m.$$

Hence

$$\lim_{m\to\infty} \frac{N_m}{g_m} \leq \lim_{m\to\infty} \frac{N_{m_0}}{\delta(m-m_0)} = 0.$$

□

References

[1] R.-O. Buchweitz, "Über Deformationen monomialer Kurvensingularitäten und Weierstrasspunkte auf Riemannschen Flächen," Ph.D. Thesis, Hannover 1976.

[2] P. Carbonne, T. Henocq and J.A. Thiong-Ly, "Feng and Rao designed minimum distance and non symmetric semigroups for special curves," preprint April 1994.

[3] V.G. Drinfeld and S.G. Vlăduţ, "Number of points of an algebraic curve," *Func. Anal.,* vol. 17, pp. 53-54, 1983.

[4] J.I. Farran, "Weierstrass semigroups and AG codes," to appear in *Proc. Int. Conf. Coding Theory, Cryptography and Related Areas,* Guanojuato, Mexico, April 20-24, 1998.

[5] G.-L. Feng and T.R.N. Rao, "A simple approach for construction of algebraic-geometric codes from affine plane curves," *IEEE Trans. Inform. Theory*, vol. IT-40, pp. 1003-1012, July 1994.

[6] G.-L. Feng and T.R.N. Rao, "Improved geometric Goppa codes," Part I: Basic Theory, *IEEE Trans. Inform. Theory*, vol. IT-41, pp. 1678-1693, Nov. 1995 .

[7] A. Garcia and H. Stichtenoth, "A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound," *Invent. Math.,* vol. 121, pp. 211-222, 1995.

[8] A. Garcia and H. Stichtenoth, "On the asymptotic behaviour of some towers of function fields over finite fields," *J. of Number Theory,* vol. 61, pp. 248-273, 1996.

[9] M. Hattori, R.J. McEliece and G. Solomon, "Subspace subcodes of Reed-Solomon codes," *IEEE Trans. Inform. Theory*, vol. IT-44, pp. 1861-1880, Sept. 1998.

[10] T. Høholdt, J.H. van Lint and R. Pellikaan, "Algebraic geometry codes," in *Handbook of Coding Theory*, (V.S. Pless, W.C. Huffman and R.A. Brualdi Eds.), vol 1, pp. 871-961, Elsevier, Amsterdam 1998.

[11] C. Kirfel and R. Pellikaan, "The minimum distance of codes in an array coming from telescopic semigroups," *IEEE Trans. Inform. Theory,* vol. 41, pp.1720-1732, Nov. 1995.

[12] R. Matsumoto, "Linear codes on nonsingular curves are better than those on singular curves," *IEICE Trans. Fundamentals,* vol. E82-A, no. 4, pp. 665-670, April 1999.

[13] R. Matsumoto, "Miura's generalization of one-point AC codes is equivalent to Høholdt, van Lint and Pellikaan's generalization," to appear in *IEICE Trans. Fundamentals,* vol. E82-A, no. 10, October 1999.
[14] G. Oliveira, "Weierstrass semigroups and the canonical ideal of non-trigonal curves", *Manuscripta Math.* vol. 71, pp. 431-450, (1991).
[15] R. Pellikaan, "On the gonality of curves, abundant codes and decoding," in Coding Theory Algebraic Geometry, Luminy 1991, (H. Stichtenoth and M.A. Tsfasman eds.), *Springer Lect. Notes,* vol. 1518, pp. 132-144, 1992.
[16] R. Pellikaan, H. Stichtenoth and F. Torres, "Weierstrass semigroups of an asymptotically good tower of function fields," *Finite Fields and their Applications,* vol. 4, pp. 381-392, 1998.
[17] H. Stichtenoth, *Algebraic function fields and codes*, Universitext, Springer-Verlag, Berlin 1993.
[18] F. Torres, "Weierstrass points and double coverings of curves. With application: symmetric numerical semigroups which cannot be realized as Weierstrass semigroups," *Manuscripta Math.,* vol. 83, pp. 39-58, 1994.
[19] M.A. Tsfasman and S.G. Vlăduţ, *Algebraic-geometric codes*, Mathematics and its Applications vol. 58, Kluwer Acad. Publ., Dordrecht 1991.
[20] M.A. Tsfasman, S.G. Vlăduţ and T. Zink, "Modular curves, Shimura curves and Goppa codes, better than Varshamov-Gilbert bound," *Math. Nachrichten*, vol. 109, pp. 21-28, 1982.

Department of Mathematics and Computing Science, Eindhoven University of Technology, 5600 MB Eindhoven, The Netherlands

E-mail address: ruudp@win.tue.nl

IMECC-UNICAMP, Cx. P. 6065, 13083-970, Campinas-SP, Brazil

E-mail address: ftorres@ime.unicamp.br