DTU Library

Bounding the number of points on a curve using a generalization of Weierstrass semigroups

Beelen, Peter; Ruano, Diego

Published in:
Proceedings of WCC

Publication date:
2011

Bounding the number of points on a curve using a generalization of Weierstrass semigroups

Peter Beelen[1] and Diego Ruano[2⋆]

[1] DTU-Mathematics, Technical University of Denmark,
Matematiktorvet, Building 303, 2800 Kgs. Lyngby, Denmark
P.Beelen@mat.dtu.dk
[2] Department of Mathematical Sciences, Aalborg University,
Fr. Bajersvej 7G, 9220 Aalborg Øst, Denmark.
diego@math.aau.dk

Abstract. In [5] an upper bound for the number of points on an algebraic curve defined over a finite field was derived. In this article we generalize their result by considering Weierstrass groups of several points simultaneously.

1 Introduction

Let $\mathbb{F}_q$ be the finite field with q elements and $\mathcal{F}/\mathbb{F}_q$ be a function field [12]. We denote by $N(\mathcal{F})$ the number of rational places of $\mathcal{F}$ and by $g(\mathcal{F})$ its genus. For any rational place P of $\mathcal{F}$, we may consider $v_P : \mathcal{F} \to \mathbb{Z} \cup \{\infty\}$ the valuation at P and the associated Riemann–Roch spaces $L(mP) = \{f \in \mathcal{F} \mid v_P(f)+m \geq 0\}$, for $m \in \mathbb{Z}$. Furthermore, we have the Weierstrass semigroup $H(P) = \{-v_P(f) \mid f \in R\} \subset \mathbb{N}_0$, where $R = \cup_{m \geq 0} L(mP) \backslash \{0\}$. The Geil–Matsumoto bound estimates the number of rational places using the Weierstrass semigroup [5, Theorem 1],

$$N(\mathcal{F}) \leq \# \left(H(P) \setminus (qH^*(P) + H(P))\right) + 1,$$

where $qH^*(P) + H(P) = \{q\lambda + \lambda' \mid \lambda, \lambda' \in H(P), \lambda \neq 0\}$.

We will consider the Weierstrass semigroup defined by several rational places [3], in order to extend the Geil–Matsumoto bound in section 2. In section 3, we estimate the size of certain subsets of the set of rational places. This estimation can lead to a sharper estimation of the total number of rational places. The motivation of this work is to estimate the minimum distance of toric codes [7]. This is work in progress.

2 A generalization of the Geil–Matsumoto bound

In this section we will present our main result: a generalization of the Geil–Matsumoto bound. The main ingredient of this generalization is to consider the

⋆ Partially supported by Spanish MEC MTM2007-64704

Weierstrass semigroup of an n-tuple $P_1, \ldots, P_n$ of rational places of the function field. In this section, we will denote by $\mathcal{Q}$ the set of $N(\mathcal{F})-n$ remaining rational places, but we would like to warn the reader that in the next section, $\mathcal{Q}$ will in general denote a subset of these $N(\mathcal{F})-n$ places. For an n-tuple $\mathbf{i} = (i_1, \ldots, i_n) \in \mathbb{Z}^n$ we write $\deg(\mathbf{i}) = \sum_{j=1}^n i_j$ and $L(\mathbf{i}) = L(\sum_{j=1}^n i_j P_j)$. Further we will denote with $\mathbf{e}_j$ the n-tuple all of whose coordinates are 0, except the j-th one, which is assumed to be 1. Then one has for example that $L(\lambda \mathbf{e}_j) = L(\lambda P_j)$.

Definition 1. *Given* $\mathbf{i} \in \mathbb{Z}^n$, *we define*

$$H_{\mathbf{i}}(P_j) = \{-v_{P_j}(f) \quad | \quad f \in \cup_{k \in \mathbb{Z}} L(\mathbf{i} + k\mathbf{e}_j) \backslash \{0\}\}$$

Remark 1.
1. Denoting by $\mathbf{0}$ the n-tuple consisting of zeroes only, we have $H_{\mathbf{0}}(P_j) = H(P_j)$.
2. Note that the set $H_{\mathbf{i}}(P_j)$ does not depend on the j-th coordinate of $\mathbf{i}$.
3. We remark that $L(\mathbf{i} + k\mathbf{e}_j) = \{0\}$, for $k < -\deg(\mathbf{i})$, so it also holds that

$$H_{\mathbf{i}}(P_j) = \{-v_{P_j}(g) \quad | \quad f \in \cup_{k \geq -\deg(\mathbf{i})} L(\mathbf{i} + k\mathbf{e}_j) \backslash \{0\}\}.$$

4. Sets such as $H_{\mathbf{i}}(P_j)$ were also introduced in [2], where they were used to compute lower bound on the minimum distances of certain algebraic geometry codes. There it is also explained how to compute these sets.

With this notation in place, we define the following functions:

Definition 2. *Let* $\mathbf{i} \in \mathbb{Z}^n$ *and let* j *be an integer between* 1 *and* n. *If either* $L(\mathbf{i}) = L(\mathbf{i} + \mathbf{e}_j)$ *or if there exists* $\lambda \in H(P_j) \backslash \{0\}$ *and* $\mu \in H_{\mathbf{i}}(P_j)$ *such that* $\mu + q\lambda = \mathbf{i}_j + 1$, *we call the pair* $(\mathbf{i}, \mathbf{i} + \mathbf{e}_j)$ *negligible. Further we define*

$$\delta(\mathbf{i}, \mathbf{i} + \mathbf{e}_j) = \begin{cases} 0 & \textit{if the pair } (\mathbf{i}, \mathbf{i} + \mathbf{e}_j) \textit{ is negligible,} \\ 1 & \textit{otherwise.} \end{cases}$$

Lemma 1. *Let* $(\mathbf{i}, \mathbf{i} + \mathbf{e}_j)$ *be a negligible pair such that* $L(\mathbf{i}) \subsetneq L(\mathbf{i} + \mathbf{e}_j)$, *say* $\mu + q\lambda = \mathbf{i}_j + 1$ *for* $\lambda \in H(P_j) \backslash \{0\}$ *and* $\mu \in H_{\mathbf{i}}(P_j)$. *Then there exist* $f \in L(\lambda \mathbf{e}_j)$ *and* $g \in L(\mathbf{i})$ *such that* $f^q g \in L(\mathbf{i} + \mathbf{e}_j) \backslash L(\mathbf{i})$.

Proof. Since $\lambda \in H(P_j)$, there exists a function $f \in L(\mathbf{e}_j)$ whose pole divisor equals $(f)_\infty = \lambda P_j$. Similarly there exists a function $g \in L(\mathbf{i})$ such that $(g) \geq -\sum_{j=0}^n i_j P_j$ and $v_{P_j}(g) = \mu$. This implies that $v_{P_j}(f^q g) = q\lambda + \mu = \mathbf{i}_j + 1$ and $(f^q g) \geq -q\lambda P_j - \sum_{j=0}^n i_j P_j$. Together these imply that $f^q g \in L(\mathbf{i} + \mathbf{e}_j) \backslash L(\mathbf{i})$ as desired. □

A pair $(\mathbf{i}, \mathbf{i} + \mathbf{e}_j)$ is negligible if $\deg(\mathbf{i})$ is large enough. More precisely, one has:

Proposition 1. *Let* $\mathbf{i} \in \mathbb{Z}^n$ *and let* j *be an integer between* 1 *and* n. *If* $\deg(\mathbf{i}) \geq (q+2)(g(\mathcal{F})+1) - 3$, *then the pair* $(\mathbf{i}, \mathbf{i} + \mathbf{e}_j)$ *is negligible.*

Proof. Suppose that $\deg(\mathbf{i}) \geq (q+2)(g(\mathcal{F})+1)-3$. Since then in particular $\deg(\mathbf{i}) \geq 2g(\mathcal{F})-1$, it follows from the theorem of Riemann–Roch that $L(\mathbf{i}) \subsetneq L(\mathbf{i}+\mathbf{e}_j)$. Since the semigroup $H(P_j) = \{0, \lambda, \dots\}$ has exactly $g(\mathcal{F})$ gaps, there exists $\lambda \in H(P_j)\backslash\{0\}$ with $\lambda \leq g(\mathcal{F})+1$. This implies that $\deg(\mathbf{i}+(1-q\lambda)\mathbf{e}_j) \geq 2g(\mathcal{F})$, so applying the theorem of Riemann–Roch again, we see that there exists a function $g \in L(\mathbf{i}+(1-q\lambda)\mathbf{e}_j)$ such that $v_{P_j}(g) = \mathbf{i}_j + 1 - q\lambda$. By Definition 1, we see that $\mathbf{i}_j + 1 - q\lambda \in H_{\mathbf{i}}(P_j)$. By Definition 2 the proposition now follows, since $(\mathbf{i}_j + 1 - q\lambda) + q\lambda = \mathbf{i}_j + 1$. □

Actually we showed the following more precise result:

Corollary 1. *Let λ_j denote the smallest nonzero element of $H(P_j)$. Then the pair $(\mathbf{i}, \mathbf{i}+\mathbf{e}_j)$ is negligible if $\deg(\mathbf{i}) \geq q\lambda_j + 2g(\mathcal{F}) - 1$.*

Now we come to the main theorem.

Theorem 1. *Define $M = (q+2)(g(\mathcal{F})+1)-3$ and let $\mathbf{i}^{(-1)}, \dots, \mathbf{i}^{(M)}$ be a sequence of n-tuples such that:*

1. $\deg(\mathbf{i}^{(-1)}) = -1$,
2. *for any k there exists a j such that $\mathbf{i}^{(k)} - \mathbf{i}^{(k-1)} = \mathbf{e}_j$.*

Then $N(\mathcal{F}) \leq n + \sum_{k=0}^{M} \delta(\mathbf{i}^{(k-1)}, \mathbf{i}^{(k)})$.

Proof. Note that by the properties of the divisor sequence, we have $\deg(\mathbf{i}^{(k)}) = k$ for any $-1 \leq k \leq M$. For any divisor G with support disjoint from $\mathcal{Q}$, we introduce the following notation:

$$\mathrm{Ev}_{\mathcal{Q}} : L(G) \to \mathbb{F}_q^{N(\mathcal{F})-n}$$

$$f \mapsto (f(Q))_{Q\in\mathcal{Q}}$$

and $C_{\mathcal{Q}}(G) = \mathrm{Ev}_{\mathcal{Q}}(L(G))$. For an n-tuple $\mathbf{i}$, we define

$$C_{\mathcal{Q}}(\mathbf{i}) = \mathrm{Ev}_{\mathcal{Q}}(L(\mathbf{i})).$$

We will begin the proof of the theorem by showing the following three claims:

1. For any divisor G of degree $\deg(G) \geq N(\mathcal{F}) - n + 2g(\mathcal{F}) - 1$, we have $C_{\mathcal{Q}}(G) = \mathbb{F}_q^{N(\mathcal{F})-n}$.
2. For any $k \geq 0$ we have $\dim(C_{\mathcal{Q}}(\mathbf{i}^{(k)})) \leq \dim(C_{\mathcal{Q}}(\mathbf{i}^{(k-1)})) + \delta(\mathbf{i}^{(k-1)}, \mathbf{i}^{(k)})$.
3. $\dim(C_{\mathcal{Q}}(\mathbf{i}^{(-1)})) = 0$.

The first claim follows from a standard argument: the kernel of the evaluation map $\mathrm{Ev}_{\mathcal{Q}} : L(G) \to \mathbb{F}_q^{N(\mathcal{F})-n}$ is given by $L(G - \sum_{Q\in\mathcal{Q}} Q)$. Therefore we get $\dim(C_{\mathcal{Q}}(G)) = \dim(L(G)) - \dim(L(G - \sum_{Q\in\mathcal{Q}} Q))$. Using the assumption $\deg(G) \geq N(\mathcal{F}) - n + 2g(\mathcal{F}) - 1$ and the theorem of Riemann–Roch, this expression simplifies to $N(\mathcal{F}) - n$.

The second claim is trivial if $\delta(\mathbf{i}^{(k-1)}, \mathbf{i}^{(k)}) = 1$, so we may assume that $\delta(\mathbf{i}^{(k-1)}, \mathbf{i}^{(k)}) = 0$. Since by assumption there exists j such that $\mathbf{i}^{(k)} = \mathbf{i}^{(k-1)} + \mathbf{e}_j$, we may apply Lemma 1 to conclude that there exist $f \in L(\lambda \mathbf{e}_j)$ for some $\lambda > 0$ and $g \in L(\mathbf{i}^{(k-1)})$ such that $f^q g \in L(\mathbf{i}^{(k)}) \backslash L(\mathbf{i}^{(k-1)})$. On the level of codes this means that the code $C_{\mathcal{Q}}(\mathbf{i}^{(k)})$ is generated as a vector space by the vectors of $C_{\mathcal{Q}}(\mathbf{i}^{(k-1)})$ and the vector $\mathrm{Ev}_{\mathcal{Q}}(f^q g)$. However, since the codes are defined over $\mathbb{F}_q$, we have $\mathrm{Ev}_{\mathcal{Q}}(f^q g) = \mathrm{Ev}_{\mathcal{Q}}(fg)$. On the other hand, since $\lambda > 0$, we see that $fg \in L(\mathbf{i}^{(k-1)})$ and therefore that $\mathrm{Ev}_{\mathcal{Q}}(fg) \in C_{\mathcal{Q}}(\mathbf{i}^{(k-1)})$. The second claim now follows.

The third claim is clear, since $L(G) = \{0\}$ for any divisor of negative degree.

From the last two parts of the claim we find inductively that

$$\dim(C_{\mathcal{Q}}(\mathbf{i}^{(M)})) \leq \sum_{k=0}^{M} \delta(\mathbf{i}^{(k-1)}, \mathbf{i}^{(k)}).$$

On the other hand, combining a similar reasoning and Proposition 1, we find that

$$\dim(C_{\mathcal{Q}}(\mathbf{i}^{(M)})) = \dim(C_{\mathcal{Q}}(\mathbf{i}^{(M)} + l\mathbf{e}_j))$$

for any j and any natural number l. From this and the first part of the claim we can conclude that

$$\dim(C_{\mathcal{Q}}(\mathbf{i}^{(M)})) = N(\mathcal{F}) - n.$$

The theorem now follows. $\square$

The above proof is inspired by the proof of the Geil–Matsumoto bound [5]. If $n = 1$, the above theorem reduces to their result. If $n = 1$, the only choice for the sequence $\mathbf{i}^{(-1)}, \ldots, \mathbf{i}^{(M)}$ is $-1, 0, \ldots, M$, but for $n > 1$, there are many possibilities. Therefore, we have a weighted oriented graph given by the lattice with vertices $\{-1, \ldots, M\}^n$ and edges $(\mathbf{i}, \mathbf{i} + \mathbf{e}_j)$, with weights $w(\mathbf{i}, \mathbf{i} + \mathbf{e}_j) = \delta(\mathbf{i}, \mathbf{i} + \mathbf{e}_j)$, for $\mathbf{i} \in \{-1, \ldots, M\}^n$ and $j = 1, \ldots, n$ such that $i_j \neq M$. In practice, we consider the bound from Corollary 1 instead of M and we may not consider the whole lattice, we can start with a one-dimensional lattice and increase its size progressively. We just find an optimal sequence $\mathbf{i}^{(-1)}, \ldots, \mathbf{i}^{(M)}$, by finding a path from a vertex with degree -1 to a vertex with degree M with minimum weight (using Dijkstra's algorithm).

We will now give some examples showing that this sometimes can be used to obtain better bounds on the number of rational places of a function field.

Example 1. Consider the function field $\mathcal{F}_1/\mathbb{F}_8 = \mathbb{F}_8(x, y)/\mathbb{F}_8$ of the Klein quartic defined by the equation $x^3 y + y^3 + x = 0$. One has that $N(\mathcal{F}) = 24$ and $g(\mathcal{F}_1) = 3$. There are three rational places occurring as poles and/or zeroes of the functions x and y. We will denote these by P_1, P_2 and P_3. More precisely one has, $(x) = 3P_1 - P_2 - 2P_3$ and $(y) = P_1 + 2P_2 - 3P_3$ ([8, Example 2.34]). From this one can show that $H = H(P_1) = H(P_2) = H(P_3) = \langle 3, 5, 7 \rangle$ and

$$L(i_1 P_1 + i_2 P_2 + i_3 P_3) = \langle x^\alpha y^\beta \mid 3\alpha + \beta \geq -i_1, -\alpha + 2\beta \geq -i_2, -2\alpha - 3\beta \geq -i_3 \rangle. \quad (1)$$

From the Geil–Matsumoto bound, we have $N(\mathcal{F}_1) \leq 1 + 24 = 25$, since $H \setminus (qH^* + H) = \{0, 3, 5, 6, \dots, 23, 25, 26, 28\}$. Actually, one can prove that every rational place of the Klein quartic has the same Weierstrass semigroup.

We now compute the bound from Theorem 1, where we will consider $n = 2$, and P_1, P_2 as above. It is enough to consider a sequence of n-tuples $(\mathbf{i}^{(-1)}, \dots, \mathbf{i}^{(29)})$, since $(\mathbf{i}, \mathbf{i} + \mathbf{e}_j)$ is negligible if $\deg(\mathbf{i}) \geq 8 \cdot 3 + 2 \cdot 3 - 1 = 29$ (Corollary 1). As before we represent the divisor P_1, resp. P_2 by $\mathbf{e}_1$, resp. $\mathbf{e}_2$ and write $\mathbf{i}^k = (i_1^{(k)}, i_2^{(k)}) = i_1^{(k)}\mathbf{e}_1 + i_2^{(k)}\mathbf{e}_2$.

We computed a oriented graph as above, given by the $\{-1, \dots 29\} \times \{0, \dots 4\}$ lattice, with weights given by $\delta(\mathbf{i}, \mathbf{i} + \mathbf{e}_j)$ and got a path with minimum weight given by

$$\begin{cases} \mathbf{i}^{(k)} = (k, 0), & \text{for } k = -1, \dots, 23, \\ \mathbf{i}^{(23+k)} = (24, k-1), & \text{for } k = 1, \dots, 3, \\ \mathbf{i}^{(26+k)} = (25, k+1), & \text{for } k = 1, \dots, 3, \end{cases}$$

then, $\{k \geq 0 \mid \delta(\mathbf{i}^{(k-1)}, \mathbf{i}^{(k)}) = 1\} = \{0, 3, 5, 6, \dots, 23, 25\}$ and therefore $N(\mathcal{F}) \leq 2 + 22 = 24$.

The Geil–Matsumoto bound is an improvement to Lewittes' bound [10],

$$N(\mathcal{F}) \leq q\lambda_1 + 1,$$

where λ_1 denotes the smallest non-zero element of H. Let us present a case where the Geil–Matsumoto bound gives the same result as Lewittes' bound. Let $\mathcal{F}/\mathbb{F}_q$ be a function field, assume that $q \in H = H(P)$, we claim that Geil–Matumoto bound gives the same result as Lewittes bound. We introduce the Apéry set of a numerical semigroup [1, 11], which is our main tool for this result. For $e \in H$, the Apéry set of H relative to e is defined to be $\mathrm{Ap}(H, e) = \{\lambda \in H | H - e \notin H\}$. One has that $\mathrm{Ap}(H, e)$ is $\{w_0 = 0, w_1, \dots, w_{e-1}\}$, where w_i is the smallest element of H congruent with i modulo e, for $i = 0, \dots, e-1$. Moreover, for $\lambda \in H$ there exist a unique i and k, with $i \in \{0, \dots, e-1\}$ and $k \in \mathbb{N}_0$, such that $\lambda = w_i + ke$, which is called Apéry's notation. Thus we have the disjoint union

$$H = \bigcup_{i=0}^{e-1} \{w_i + e\mathbb{N}_0\},$$

in particular $\{e, w_1, \dots, w_{e-1}\}$ generates H.

Proposition 2. *Let $q \in H$ and λ_1 the smallest non-zero element of H, then*

$$H \setminus (qH^* + H) = H \setminus (q\lambda_1 + H),$$

and therefore the bounds in [5, 10] give the same result if $q \in H$.

Proof. Let $\mathrm{Ap}(H, q) = \{w_0 = 0, w_1, \dots, w_{q-1}\}$ be the Apéry set of H relative to $e = q \in H$. We consider H generated by $\{q, w_1, \dots, w_{q-1}\}$, hence

$$H \setminus (qH^* + H) = H \setminus \left((\bigcup_{i=1}^{q-1} (qw_i + H)) \cup (qq + H) \right)$$

We consider Apéry's notation for qq and qw_i: $qq = w_0 + qq$ and $qw_i = w_0 + w_i q$, for $i = 0, \ldots, q-1$. Thus,

$$H \setminus (qH^* + H) = H \setminus (\lambda q + H),$$

where $\lambda = \min\{q, w_1, \ldots, w_{q-1}\}$, since qq, $qw_i \in \{w_0 + q\mathbb{N}_0\}$, for $i = 0, \ldots, q-1$. Furthermore, the smallest non-zero element λ_1 of H either is equal to q or belongs to $\mathrm{Ap}(H, q)$ – as in this case $\lambda_1 - q \notin H$. Hence, $\lambda = \lambda_1$ is the smallest non-zero element of H. Therefore, we have

$$\#\,(H \setminus (qH^* + H)) + 1 = \#\,(H \setminus (q\lambda_1 + H)) + 1 = q\lambda_1 + 1,$$

and the result holds. □

The Weierstrass semigroup of Example 1 contains $q = 8$, the number of elements of the base field. Therefore, both bounds in [5, 10] give the same result. Namely, we have $e = q = 8$ and $w_0 = 0, w_1 = 9, w_2 = 10, w_3 = 3, w_4 = 12, w_5 = 5, w_6 = 6, w_7 = 7$.

3 A second generalization of the Geil–Matsumoto bound

In this section we will generalize the previous results by estimating the size of certain subsets of the set of rational places. Contrary to the previous section, we will therefore in this section by $\mathcal{Q}$ denote some subset of the set of all rational places not containing any of the places $P_1, \ldots, P_n$. The results from the previous section can be refined in this setup. One of the reasons we now look at subsets is that we want to apply Geil–Matsumoto like bounds to curves lying on toric varieties [4] and explore the resulting consequences for some toric codes [7]. For convenience we define $T = \mathbb{F}_q \setminus \{0\}$.

Definition 3. *Let $\mathbf{i} \in \mathbb{Z}^n$ and let j be an integer between 1 and n. We call the pair $(\mathbf{i}, \mathbf{i} + \mathbf{e}_j)$ T-negligible if either $L(\mathbf{i}) = L(\mathbf{i} + \mathbf{e}_j)$ or if*

1. *there exists $\lambda \in H(P_j)\setminus\{0\}$ and $\mu \in H_{\mathbf{i}}(P_j)$ such that $\mu + (q-1)\lambda = \mathbf{i}_j + 1$ and*
2. *for this λ there exists $f \in L(\lambda P_j)\setminus L((\lambda - 1)P_j)$ such that $f(Q) \in T$ for all $Q \in \mathcal{Q}$.*

Further we define

$$\delta_T(\mathbf{i}, \mathbf{i} + \mathbf{e}_j) = \begin{cases} 0 & \text{if the pair } (\mathbf{i}, \mathbf{i} + \mathbf{e}_j) \text{ is } T\text{-negligible,} \\ 1 & \text{otherwise.} \end{cases}$$

Note that depending on the choice of $\mathcal{Q}$, the function δ_T may change. Strictly speaking we should therefore include $\mathcal{Q}$ in the notation for this function, but for the sake of simplicity, we will not do this.

Lemma 2. *Let* $(\mathbf{i}, \mathbf{i}+\mathbf{e}_j)$ *be a* T*-negligible pair such that* $L(\mathbf{i}) \subsetneq L(\mathbf{i}+\mathbf{e}_j)$*, say* $\mu + (q-1)\lambda = \mathbf{i}_j + 1$ *for* $\lambda \in H(P_j)\backslash\{0\}$ *and* $\mu \in H_{\mathbf{i}}(P_j)$*. Then there exist* $f \in L(\lambda \mathbf{e}_j)$ *and* $g \in L(\mathbf{i})$ *such that* $f^{q-1}g \in L(\mathbf{i}+\mathbf{e}_j)\backslash L(\mathbf{i})$ *and such that moreover* $f(Q) \in T$ *for all* $Q \in \mathcal{Q}$*.*

Proof. Since $\lambda \in H(P_j)$, there exists a function $f \in L(\mathbf{e}_j)$ whose pole divisor equals $(f)_\infty = \lambda P_j$. By definition 3 we can choose f such that $f(Q) \in T$ for all $Q \in \mathcal{Q}$. Similarly there exists a function $g \in L(\mathbf{i})$ such that $(g) \geq -\sum_{j=0}^{n} i_j P_j$ and $v_{P_j}(g) = \mu$. This implies that $v_{P_j}(f^{q-1}g) = (q-1)\lambda + \mu = \mathbf{i}_j + 1$ and $(f^{q-1}g) \geq -(q-1)\lambda P_j - \sum_{j=0}^{n} i_j P_j$. Together these imply that $f^{q-1}g \in L(\mathbf{i}+\mathbf{e}_j)\backslash L(\mathbf{i})$ as desired. □

A pair $(\mathbf{i}, \mathbf{i}+\mathbf{e}_j)$ is negligible if $\deg(\mathbf{i})$ is large enough. More precisely, one has:

Proposition 3. *Let* $\mathbf{i} \in \mathbb{Z}^n$ *and let* j *be an integer between* 1 *and* n*. Define* $\Lambda = \#\mathcal{Q} + 2g(\mathcal{F}) - 1$ *and* $M_T = (q-1)(\Lambda+1) + 2g(\mathcal{F}) - 1$*. Then any pair* $(\mathbf{i}, \mathbf{i}+\mathbf{e}_j)$ *satisfying* $\deg(\mathbf{i}) \geq M_T$ *is* T*-negligible.*

Proof. Suppose that $\deg(\mathbf{i}) \geq M_T$. Since then in particular $\deg(\mathbf{i}) \geq 2g(\mathcal{F})-1$, it follows from the theorem of Riemann–Roch that $L(\mathbf{i}) \subsetneq L(\mathbf{i}+\mathbf{e}_j)$. Also note that $\deg(\mathbf{i}+(1-(q-1)(\Lambda+1))\mathbf{e}_j) \geq 2g(\mathcal{F})$, so applying the theorem of Riemann–Roch again, we see that there exists a function $g \in L(\mathbf{i}+(1-(q-1)(\Lambda+1))\mathbf{e}_j)$ such that $v_{P_j}(g) = \mathbf{i}_j+1-(q-1)(\Lambda+1)$. By Definition 1, we see that $\mathbf{i}_j+1-(q-1)(\Lambda+1) \in H_{\mathbf{i}}(P_j)$.

Since the largest gap of the semigroup $H(P_j)$ is at most $2g(\mathcal{F})-1$, the number $\Lambda+1$ is not a gap of $H(P_j)$. This means that there exists a function $f \in L((\Lambda+1)P_j)$ such that $v_{P_j}(f) = \Lambda+1$. We cannot conclude yet from Definition 3 that the pair $(\mathbf{i}, \mathbf{i}+\mathbf{e}_j)$ is T-negligible, since f could have a zero among the places in $\mathcal{Q}$. However, from the proof of Theorem 1 and the definition of Λ we see that for any j the evaluation map $\mathrm{Ev}_{\mathcal{Q}} : L(\Lambda P_j) \to \mathbb{F}_q^{\#\mathcal{Q}}$ is surjective. Therefore, we can always choose f such that $f(Q) \in T$ for all $Q \in \mathcal{Q}$. □

The M_T given in this proposition can be very large. Under some additional conditions, we can obtain better results.

Proposition 4. *Let* $\mathbf{i} \in \mathbb{Z}^n$ *and let* j *be an integer between* 1 *and* n*. Suppose that for any* $\lambda \in H(P_j)$ *there exists* $f \in L(\lambda P_j)\backslash L((\lambda-1)P_j)$ *such that* $f(Q) \in T$ *for all* $Q \in \mathcal{Q}$*. If* $\deg(\mathbf{i}) \geq (q+1)(g(\mathcal{F})+1) - 3$*, then the pair* $(\mathbf{i}, \mathbf{i}+\mathbf{e}_j)$ *is* T*-negligible.*

Proof. Suppose that $\deg(\mathbf{i}) \geq (q+1)(g(\mathcal{F})+1) - 3$. Since then in particular $\deg(\mathbf{i}) \geq 2g(\mathcal{F}) - 1$, it follows from the theorem of Riemann–Roch that $L(\mathbf{i}) \subsetneq L(\mathbf{i}+\mathbf{e}_j)$. As in the proof of Proposition 1 we can conclude that there exists $\lambda \in H(P_j)\backslash\{0\}$ with $\lambda \leq g(\mathcal{F})+1$. This implies that $\deg(\mathbf{i}+(1-(q-1)\lambda)\mathbf{e}_j) \geq 2g(\mathcal{F})$, so applying the theorem of Riemann–Roch again, we see that there exists a function $g \in L(\mathbf{i}+(1-(q-1)\lambda)\mathbf{e}_j)$ such that $v_{P_j}(g) = \mathbf{i}_j + 1 - (q-1)\lambda$. By Definition 1, we see that $\mathbf{i}_j+1-(q-1)\lambda \in H_{\mathbf{i}}(P_j)$. Furthermore by assumption, there exists $f \in L(\lambda P_j)\backslash L((\lambda - 1)P_j)$ such that $f(Q) \in T$ for all $Q \in \mathcal{Q}$. Therefore, by Definition 3, the proposition follows. □

As in the previous section, we can refine the above statement:

Corollary 2. *Let λ_j denote the smallest nonzero element of $H(P_j)$. Suppose that for any $\lambda \in H(P_j)$ there exists $f \in L(\lambda P_j)\backslash L((\lambda-1)P_j)$ such that $f(Q) \in T$ for all $Q \in \mathcal{Q}$. Then the pair $(\mathbf{i}, \mathbf{i} + \mathbf{e}_j)$ is T-negligible if $\deg(\mathbf{i}) \geq (q-1)\lambda_j + 2g(\mathcal{F}) - 1$.*

Now we come to the refinement of Theorem 1.

Theorem 2. *Define $\Lambda = \#\mathcal{Q} + 2g(\mathcal{F}) - 1$ and $M_T = (q-1)(\Lambda+1) + 2g(\mathcal{F}) - 1$. Let $\mathbf{i}^{(-1)}, \ldots, \mathbf{i}^{(M_T)}$ be a sequence of n-tuples such that:*

1. $\deg(\mathbf{i}^{(-1)}) = -1$,
2. *for any k there exists a j such that $\mathbf{i}^{(k)} - \mathbf{i}^{(k-1)} = \mathbf{e}_j$.*

Then $\#\mathcal{Q} \leq \sum_{k=0}^{M_T} \delta_T(\mathbf{i}^{(k-1)}, \mathbf{i}^{(k)})$.

Proof. The proof is similar to that of Theorem 1. All the reasoning is similar apart from the proof of the following claim: For any $k \geq 0$ we have $\dim(C_{\mathcal{Q}}(\mathbf{i}^{(k)})) \leq \dim(C_{\mathcal{Q}}(\mathbf{i}^{(k-1)})) + \delta_T(\mathbf{i}^{(k-1)}, \mathbf{i}^{(k)})$.

This is clear if $\delta_T(\mathbf{i}^{(k-1)}, \mathbf{i}^{(k)}) = 1$, so we may assume that $\delta_T(\mathbf{i}^{(k-1)}, \mathbf{i}^{(k)}) = 0$. We may apply Lemma 2 to conclude that there exist $f \in L(\lambda \mathbf{e}_j)$ for some $\lambda > 0$ and $g \in L(\mathbf{i}^{(k-1)})$ such that $f^{q-1}g \in L(\mathbf{i}^{(k)})\backslash L(\mathbf{i}^{(k-1)})$. Moreover, we may assume that $f(Q) \in T$ for all $Q \in \mathcal{Q}$. Since $\alpha^{q-1} = 1$ for all $\alpha \in T$, this implies $f(Q)^{q-1} = 1$ for all $Q \in \mathcal{Q}$. On the level of codes we have, as in Theorem 1, that the code $C_{\mathcal{Q}}(\mathbf{i}^{(k)})$ is generated as a vector space by the vectors of $C_{\mathcal{Q}}(\mathbf{i}^{(k-1)})$ and the vector $\mathrm{Ev}_{\mathcal{Q}}(f^{q-1}g)$. However, we have $\mathrm{Ev}_{\mathcal{Q}}(f^{q-1}g) = \mathrm{Ev}_{\mathcal{Q}}(g) \in C_{\mathcal{Q}}(\mathbf{i}^{(k-1)})$. The claim now follows and the proof of the theorem can be concluded as that of Theorem 1. □

In case $n = 1$ and the hypotheses from Proposition 4 are satisfied, we obtain the following result:

Corollary 3. *Suppose that for any $\lambda \in H(P)$ there exists $f \in L(\lambda P)\backslash L((\lambda - 1)P)$ such that $f(Q) \in T$ for all $Q \in \mathcal{Q}$. Then*

$$\#\mathcal{Q} \leq \#H(P)\backslash((q-1)H^*(P) + H(P)).$$

Proof. Since $n = 1$, the only sequence we can choose is $-1, 0, 1, \ldots$. However, under the stated assumptions, a pair $(k-1, k)$ is T-negligible if and only if $k \in (q-1)H^*(P) + H(P)$. □

We will now give some examples.

Example 2. This example is a continuation of Example 1. In particular we will use the same notation as in that example. We choose $P = P_1$ and $\mathcal{Q}$ to be the set of all rational places Q satisfying $x(Q) \in T$ and $y(Q) \in T$. Using the divisors for x and y in Example 1, we see that the only rational places not in $\mathcal{Q}$ are P_1, P_2 and P_3.

Using Equation (1), we see that the conditions in Corollary 3 are satisfied for our choice of $\mathcal{Q}$. Therefore we find that

$$\#\mathcal{Q} \leq \#H(P_1)\backslash(7H^*(P_1) + H(P_1)) = \#\{0, 3, 5, \ldots, 20, 22, 23, 25\} = 21.$$

Also counting the rational points P_1, P_2 and P_3 we find that $N(\mathcal{F}_1) \leq 24$. In this instance Corollary 3 gives a better bound than the bound by Geil–Matsumoto.

Example 3. In this example we consider the function field $\mathcal{F}_2/\mathbb{F}_{32} = \mathbb{F}_{32}(x, y)/\mathbb{F}_{32}$ defined by the equation $x^9 + x^2y^5 + y^2 = 0$ [6, 9]. This is a function field with 158 rational places and genus 15. The function y has a unique zero, which we denote by P_1 and it holds that $v_{P_1}(x) = 2$ and $v_{P_1}(y) = 9$. The function x has a unique pole, which we will denote by P_2 and it holds that $v_{P_2}(x) = -5$ and $v_{P_2}(y) = -7$. Apart from P_1, the function x has exactly one other zero, which we denote by P_3 and it holds that $v_{P_3}(x) = 3$ and $v_{P_3}(y) = -2$. All in all, we see that

$$(x) = 2P_1 - 5P_2 + 3P_3$$

and

$$(y) = 9P_1 - 7P_2 - 2P_3.$$

With these divisors in hand it is possible to compute the semigroups for P_1, P_2 and P_3:

$$H(P_1) = \{0, 7, 9, 14, 16, 18, 19, 20, 21, 23, 25, \ldots\},$$

$$H(P_2) = \{0, 5, 10, 12, 15, 17, 18, 20, 22, 23, 24, 25, 27, \ldots\}$$

and

$$H(P_3) = \{0, 8, 11, 13, 14, 16, 19, 21, 22, 24, \ldots\}.$$

Moreover it holds that

$$L(i_1P_1 + i_2P_2 + i_3P_3) = \langle x^\alpha y^\beta \mid 2\alpha + 9\beta \geq -i_1, -5\alpha - 7\beta \geq -i_2, 3\alpha - 2\beta \geq -i_3 \rangle. \tag{2}$$

One can also show that all rational places different from P_1, P_2 and P_3 have the same semigroup $\{0, 16, \ldots\}$. The Geil–Matsumoto bound using the point P_2 yields $N(\mathcal{F}_2) \leq 161$.

We will apply Corollary 3 for $P = P_2$. As in the previous example, we choose $\mathcal{Q}$ to be the set of all rational places Q satisfying $x(Q) \in T$ and $y(Q) \in T$. The only rational places not contained in $\mathcal{Q}$ are P_1, P_2 and P_3. Equation (2) implies that we can apply Corollary 3 for any of the places P_1, P_2 and P_3. Using P_2 we find that

$$\#\mathcal{Q} \leq H(P_2)\backslash(31H^*(P_2) + H(P_2)) = 155.$$

Also counting the places P_1, P_2 and P_3, we find that $N(\mathcal{F}_2) \leq 158$, which is sharp.

References

1. Apéry, R.: Sur les branches superlinéaires des courbes algébriques. C. R. Acad. Sci. Paris 222, 1198–1200 (1946)
2. Beelen, P.: The order bound for general algebraic geometric codes. Finite Fields Appl. 13(3), 665–680 (2007)
3. Beelen, P., Tutaş, N.: A generalization of the Weierstrass semigroup. J. Pure Appl. Algebra 207(2), 243–260 (2006)
4. Fulton, W.: Introduction to toric varieties, Annals of Mathematics Studies, vol. 131
5. Geil, O., Matsumoto, R.: Bounding the number of $\mathbb{F}_q$-rational places in algebraic function fields using Weierstrass semigroups. J. Pure Appl. Algebra 213(6), 1152–1156 (2009)
6. Haché, G., Le Brigand, D.: Effective construction of algebraic geometry codes. IEEE Trans. Inform. Theory 41(6, part 1), 1615–1628 (1995), special issue on algebraic geometry codes
7. Hansen, J.P.: Toric surfaces and error-correcting codes. In: Coding theory, cryptography and related areas (Guanajuato, 1998), pp. 132–142. Springer, Berlin (2000)
8. Høholdt, T., van Lint, J.H., Pellikaan, R.: Algebraic geometry codes. Pless, V. S. (ed.) et al., Handbook of coding theory. Vol. 1. Part 1: Algebraic coding. Vol. 2. Part 2: Connections, Part 3: Applications. Amsterdam: Elsevier. 871-961 (1998). (1998)
9. Justesen, J., Larsen, K.J., Jensen, H.E., Havemose, A., Høholdt, T.: Construction and decoding of a class of algebraic geometry codes. IEEE Trans. Inform. Theory 35(4), 811–821 (1989)
10. Lewittes, J.: Places of degree one in function fields over finite fields. J. Pure Appl. Algebra 69(2), 177–183 (1990)
11. Rosales, J.C., García-Sánchez, P.A.: Numerical semigroups, Developments in Mathematics, vol. 20. Springer, New York (2009)
12. Stichtenoth, H.: Algebraic function fields and codes. Universitext, Springer-Verlag, Berlin (1993)