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

Peter Beelen† Diego Ruano‡

Abstract

In this article we use techniques from coding theory to derive upper bounds for the number of rational places of the function field of an algebraic curve defined over a finite field. The used techniques yield upper bounds if the (generalized) Weierstrass semigroup [3] for an n-tuple of places is known, even if the exact defining equation of the curve is not known. As shown in examples, this sometimes enables one to get an upper bound for the number of rational places for families of function fields. Our results extend results in [6].

1 Introduction

Let $\mathbb{F}_q$ be the finite field with q elements and $\mathcal{F}/\mathbb{F}_q$ be a function field [10] of an algebraic curve $\mathcal{C}$ defined over $\mathbb{F}_q$. We denote by $N(\mathcal{F})$ the number of rational places of $\mathcal{F}$ and by $g(\mathcal{F})$ its genus. Even when the defining equation of $\mathcal{C}$ is known explicitly, it can be useful to have a priori upper bounds for $N(\mathcal{F})$. If only partial information is available about the curve $\mathcal{C}$, it is often still possible to give an upper bound on the number of rational places of $\mathcal{F}$. One such upper bound is the well-known Hasse–Weil upper bound, stating that $N(\mathcal{F}) \leq q + 1 + 2g(\mathcal{F})\sqrt{q}$. To use this upper bound, one only needs to know (an upper bound for) the genus of $\mathcal{F}$. In [6, Theorem 1] another type of an a priori upper bound is given, which assumes the knowledge of the Weierstrass semigroup $H(P_1)$ of a rational place P_1 of $\mathcal{F}$:

$$N(\mathcal{F}) \leq \#\left(H(P_1) \setminus (qH^*(P_1) + H(P_1))\right) + 1,$$

*Published in Designs, Codes and Cryptography, Volume 66, Issue 1-3, pages 221-230 (2013). This work was supported in part by the Danish FNU grant 272-07-0266, the Danish National Research Foundation and the National Science Foundation of China (Grant No.11061130539) for the Danish-Chinese Center for Applications of Algebraic Geometry in Coding Theory and Cryptography and by the Spanish grant MTM2007-64704.

†DTU-Mathematics, Technical University of Denmark, Matematiktorvet, Building 303, 2800 Kgs. Lyngby, Denmark P.Beelen@mat.dtu.dk

‡Department of Mathematical Sciences, Aalborg University, Fr. Bajersvej 7G, 9220 Aalborg Øst, Denmark. diego@math.aau.dk

where $qH^*(P_1)+H(P_1) = \{q\lambda+\lambda' \mid \lambda, \lambda' \in H(P_1), \lambda \neq 0\}$. One may rightly ask how often the situation arises in which one does not know the exact equation of $\mathcal{C}$, but one does know a Weierstrass semigroup. However, we will show in examples that having only some information on the defining equation sometimes is enough to compute the bound in [6] as well as our generalized bounds (see Example 11). In order to extend the Geil–Matsumoto bound, we will in Section 2 consider the Weierstrass semigroup defined by several rational places [3]. In section 3, we estimate the size of certain subsets of the set of rational places. This second estimation can lead to a sharper estimate of the total number of rational places. As done in [6], one may change viewpoint and use the bounds obtained in this article to obtain information about the kind of (generalized) semigroups that may occur when one assumes that the function field has many rational places. This is also the point of view taken in Example 11, where it is shown that a certain family of function fields of genus 6 cannot improve upon known records from [11].

The main techniques to prove our results come from coding theory. More precisely, we consider AG-codes constructed by evaluating functions from a Riemann-Roch space $L(G)$ (for suitable divisors G) in rational places of $\mathcal{F}$. The length of the resulting code is given by the number of rational places used in this construction. Usually, the rational places are fixed and one is interested in determining the minimum distance of the code. In this article, modifying an idea from [6], we estimate the dimension of the code. Since the dimension of a code cannot exceed its length, this gives information about the number of rational places the function field $\mathcal{F}$ can have.

2 A generalization of the Geil–Matsumoto bound

In this section we will present a first generalization of the Geil–Matsumoto bound [6]. Let $P_1, \ldots, P_n$ be n rational places of a given function field $\mathcal{F}$ and denote by $\mathcal{Q}$ the set of $N(\mathcal{F}) - n$ remaining rational places. Note though 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 2

1. *We have $H_{\mathbf{0}}(P_j) = H(P_j)$, where $\mathbf{0}$ denotes the n-tuple consisting of zeroes only.*
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*

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

4. *Sets such as $H_{\mathbf{i}}(P_j)$ were also mentioned in [2], where they were used to compute lower bounds on the minimum distances of certain algebraic geometry codes. In [2] it is also explained how to compute these sets. They are closely related to the generalized Weierstrass semigroups introduced in [3].*

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

Definition 3 *Let $\mathbf{i} \in \mathbb{Z}^n$ and let j be an integer between 1 and n. If $L(\mathbf{i}) = L(\mathbf{i}+\mathbf{e}_j)$ 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*

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

Lemma 4 *Let $(\mathbf{i}, \mathbf{i}+\mathbf{e}_j)$ be a negligible pair such that $L(\mathbf{i}) \subsetneq L(\mathbf{i}+\mathbf{e}_j)$, and write $\mu + q\lambda = \mathbf{i}_j + 1$ 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 $(g) \geq -\sum_{k=0}^{n} i_k P_k$ and $-v_{P_k}(g) = \mu$. This implies that $-v_{P_j}(f^q g) = q\lambda + \mu = \mathbf{i}_j + 1$ and also that $(f^q g) \geq -P_j - \sum_{k=0}^{n} i_k P_k$. 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 5 *Let $\mathbf{i} \in \mathbb{Z}^n$ and let j be an integer between 1 and n and assume that $\deg(\mathbf{i}) \geq (q+2)(g(\mathcal{F})+1) - 3$. 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 this implies in particular that $\deg(\mathbf{i}) \geq 2g(\mathcal{F}) - 1$, the theorem of Riemann–Roch implies 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 an integer $\lambda \in H(P_j)\backslash\{0\}$ with $\lambda \leq g(\mathcal{F}) + 1$. Therefore $\deg(\mathbf{i} + (1-q\lambda)\mathbf{e}_j) \geq 2g(\mathcal{F})$, 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 3 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 6 *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 7 *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:

$$\begin{aligned} \mathrm{Ev}_{\mathcal{Q}} : L(G) &\rightarrow \mathbb{F}_q^{N(\mathcal{F})-n} \\ f &\mapsto (f(Q))_{Q \in \mathcal{Q}} \end{aligned}$$

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 $\deg(G) \geq N(\mathcal{F}) - n + 2g(\mathcal{F}) - 1$, it holds that $C_{\mathcal{Q}}(G) = \mathbb{F}_q^{N(\mathcal{F})-n}$.
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 4 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 5, 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 claim we can conclude that

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

The theorem now follows. ■

The above proof is inspired by the proof of the Geil–Matsumoto bound [6]. 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 $-1, 0, \ldots, M$. For $n > 1$, there are more possibilities. In fact, we obtain 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 6 instead of the bound M in Theorem 7. We do not need to consider the whole lattice, but can start with a one-dimensional lattice and increase its size progressively. Then 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 [5], which computes a path with lowest weight between a particular vertex of a graph and every other vertex of that graph).

Example 8 *In this example we consider the function field of the Klein quartic over $\mathbb{F}_8$ which has genus three. It can be described as $\mathcal{F}_1/\mathbb{F}_8 = \mathbb{F}_8(x, y)/\mathbb{F}_8$, where $x^3y + y^3 + x = 0$. Of course it is well-known how many rational places this function field has (namely 24) and it should be noted that the only purpose of this example is to illustrate the theory.*

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 we choose them such that the following identities of divisors hold:

$$(x) = 3P_1 - P_2 - 2P_3 \text{ and } (y) = P_1 + 2P_2 - 3P_3.$$

From this, one can show that $H = H(P_1) = H(P_2) = H(P_3) = \langle 3, 5, 7\rangle$ and

$$L(i_1P_1 + i_2P_2 + i_3P_3) = \langle x^\alpha y^\beta \mid 3\alpha + \beta \geq -i_1, -\alpha + 2\beta \geq -i_2, -2\alpha - 3\beta \geq -i_3\rangle. \tag{1}$$

Actually, one can prove that all rational places of the Klein quartic have the same Weierstrass semigroup. The Geil–Matsumoto bound gives $N(\mathcal{F}_1) \leq 1 + 24 = 25$ in this case, since $H \setminus (8H^* + H) = \{0, 3, 5, 6, \ldots, 23, 25, 26, 28\}$.

We now compute the bound from Theorem 7, where we will consider $n = 2$, and P_1, P_2 as above. It is enough to consider a sequence of n-tuples $(\mathbf{i}^{(-1)}, \ldots, \mathbf{i}^{(29)})$, since $(\mathbf{i}, \mathbf{i} + \mathbf{e}_j)$ is negligible if $\deg(\mathbf{i}) \geq 8 \cdot 3 + 2 \cdot 3 - 1 = 29$ (Corollary 6). 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 $\{-1, \ldots 29\} \times \{0, \ldots 4\}$ lattice, with weights given by $\delta(\mathbf{i}, \mathbf{i} + \mathbf{e}_j)$ and got a path with minimum weight given by

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

Then $\{k \geq 0 \mid \delta(\mathbf{i}^{(k-1)}, \mathbf{i}^{(k)}) = 1\} = \{0, 3, 5, 6, \ldots, 23, 25\}$*, which implies that* $N(\mathcal{F}) \leq 2 + 22 = 24$*.*

The Geil–Matsumoto bound is an improvement to the gonality bound, sometimes called Lewittes' bound [8],

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

where λ_1 denotes the smallest non-zero element of H. In the above example these bounds give rise to the same upper bound for $N(\mathcal{F})$. The following proposition explains this phenomenon. We introduce the Apéry set of a numerical semigroup [1, 9], which is the main tool for this result. For $e \in H$, the Apéry set of H relative to e is defined to be $\mathrm{Ap}(H, e) = \{\lambda \in H | \lambda - e \notin H\}$. One has that $\mathrm{Ap}(H, e)$ is $\{w_0 = 0, w_1, \ldots, w_{e-1}\}$, where w_i is the smallest element of H congruent with i modulo e, for $i = 0, \ldots, e-1$. Moreover, for $\lambda \in H$ there exist a unique i and k, with $i \in \{0, \ldots, e-1\}$ and $k \in \mathbb{N}_0$, such that $\lambda = w_i + ke$. Thus we have the disjoint union

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

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

Proposition 9 *Let* $e \in H$ *and* λ_1 *the smallest non-zero element of* H*, then*

$$\#(H \setminus (eH^* + H)) = e\lambda_1.$$

In particular the bounds in [6, 8] give the same result if $q \in H$*.*

Proof. Let $\mathrm{Ap}(H, e) = \{w_0 = 0, w_1, \ldots, w_{e-1}\}$ be the Apéry set of H relative to $e \in H$. For any $\lambda \in H$ we have

$$e\lambda + H = \bigcup_{i=0}^{e-1} (e\lambda + w_i + e\mathbb{N}_0) = \bigcup_{i=0}^{e-1} (w_i + e\mathbb{N}_{\geq \lambda}),$$

where $\mathbb{N}_{\geq \lambda}$ denotes the set of natural numbers greater than or equal to λ. This implies that for $\lambda < \mu \in H$ we have $e\lambda + H \supset e\mu + H$ and thus

$$eH^* + H = e\lambda_1 + H,$$

with λ_1 the smallest element of H^*. The proposition now follows, since the equality $\#(H \setminus (e\lambda_1 + H)) = e\lambda_1$ is a well-known result for semigroups, see [7, Chapter 10, Lemma 5.15].

■

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

Remark 10 *The converse statement, namely that (in the notation of Proposition 9) $\#(H \setminus (eH^* + H)) = e\lambda_1$ implies that $e \in H$, is not necessarily true. Consider for example the semigroup $\{0, 2, 4, 5, 6, \dots\}$ generated by 2 and 5 and suppose that $e = 3$.*

On the other hand, for semigroups H generated by m and $m + 1$, with m a natural number, this converse does hold: Suppose that $\#(H \setminus (eH^* + H)) = em$, then $e(m + 1) \in em + H$ (by [7, Chapter 10, Lemma 5.15]), which would imply that $e = e(m + 1) - em \in H$. It is also studied in [4] when the bounds in [6, 8] coincide.

We conclude this section with an example that shows that the above techniques also can be used when only partial information is given about the defining equation of the function field.

Example 11 *In this example we consider the function field $\mathcal{F}_2/\mathbb{F}_8 = \mathbb{F}_8(x, y)/\mathbb{F}_8$, where x and y are related by an equation of the form*

$$\alpha y^4 + \beta y + x^5 + \sum_{(i,j)\in\Delta} a_{i,j} x^i y^j = 0, \tag{2}$$

where α and β are nonzero elements in $\mathbb{F}_8$ and $a_{i,j}$ are arbitrary elements in $\mathbb{F}_8$. Moreover $\Delta = \{(i, j) \in \mathbb{Z}^2 \mid 4i + 5j < 20,\ i \geq 0,\ 5j + i > 5\}$. Another way of stating the structure of the defining equation is that its Newton polygon is a triangle with vertices $(0, 0)$, $(5, 0)$ and $(0, 4)$. We will assume that the genus of $\mathcal{F}_2$ equals 6, which amounts to saying if we interpret Equation (2) as a defining equation of a curve, then this curve does not have any singularities.

Like for the Klein quartic in the previous example, we can derive information about the divisors for x and y from the defining equation. In fact, denoting by P_1 the common zero of x and y and by P_2 the unique pole of x (and y), we have

$$(x) \geq P_1 - 4P_2 \text{ and } (y) = 5(P_1 - P_2).$$

Using the assumption that $g(\mathcal{F}_2) = 6$, one can show that this implies

$$L(i_1P_1 + i_2P_2) = \langle x^\alpha y^\beta \mid \alpha + 5\beta \geq -i_1, -4\alpha - 5\beta \geq -i_2, i_1 \geq 0\rangle. \tag{3}$$

In particular, we see that the semigroup of P_2 (and in fact also P_1) is generated by 4 and 5. Since $8 \in H(P_1)$, we see that the bound from [6] gives 33 for this example. Any function field of genus 6 defined over $\mathbb{F}_8$ can have at most 34 points (i.e. $N_8(6) \leq 34$), while it is also known that $N_8(6) \geq 33$ [11]. Based on this, one may hope that for a clever choice of the coefficients α, β and the $a_{i,j}$

one can find a function field defined by an equation of the form as in (2) with 33 *rational places. However, it turns out that using Theorem 7 with*

$$\begin{cases} \mathbf{i}^{(k)} = (k, 0), & \text{for } k = -1, \ldots, 34, \\ \mathbf{i}^{(34+k)} = (34, k), & \text{for } k = 1, \ldots, 3, \\ \mathbf{i}^{(37+k)} = (34 + k, 3), & \text{for } k = 1, \ldots, 3, \\ \mathbf{i}^{(40+k)} = (37, 3 + k), & \text{for } k = 1, \ldots, 3. \end{cases}$$

that $N(\mathcal{F}_2) \leq 2 + 29 = 31$. *Note that we do not have to describe more values of* $\mathbf{i}^{(k)}$ *by Corollary 6.*

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. Further we define $T = \mathbb{F}_q \backslash \{0\}$ for convenience.

Definition 12 *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* $\lambda \in H(P_j) \backslash \{0\}$ *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* $f \in L(\lambda P_j) \backslash L((\lambda - 1)P_j)$ *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 13 *Let* $(\mathbf{i}, \mathbf{i} + \mathbf{e}_j)$ *be a* T*-negligible pair such that* $L(\mathbf{i}) \subsetneq L(\mathbf{i} + \mathbf{e}_j)$ *and write* $\mu + (q-1)\lambda = \mathbf{i}_j + 1$ *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 12 we can choose a function 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 $(g) \geq -\sum_{k=0}^{n} i_k P_k$ 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 also that $(f^{q-1}g) \geq -(q-1)\lambda P_j - \sum_{j=0}^{n} i_j P_j$. 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 14 *Let $\mathbf{i} \in \mathbb{Z}^n$ and let j be an integer between 1 and n. Define $\Lambda = \#\mathcal{Q} + 2g(\mathcal{F})$ and $M_T = (q-1)\Lambda + 2g(\mathcal{F}) - 1$. 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 $\deg(\mathbf{i}+(1-(q-1)\Lambda)\mathbf{e}_j) \geq 2g(\mathcal{F})$, 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 $\mathbf{i}_j+1-(q-1)\Lambda \in H_{\mathbf{i}}(P_j)$.

Since the largest gap of the semigroup $H(P_j)$ is at most $2g(\mathcal{F})-1$, the number Λ is not a gap of $H(P_j)$. This means that there exists a function $f \in L(\Lambda P_j)$ such that $-v_{P_j}(f) = \Lambda$. We cannot conclude yet from Definition 12 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 7 and the definition of Λ we see that for any j the evaluation map $\mathrm{Ev}_{\mathcal{Q}} : L((\Lambda-1)P_j) \to \mathbb{F}_q^{\#\mathcal{Q}}$ is surjective. Therefore, we can always choose $f \in L(\Lambda P_j)\backslash L((\Lambda-1)P_j)$ 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 15 *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 $\deg(\mathbf{i}) \geq 2g(\mathcal{F})-1$, 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 5 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 12, the proposition follows. ■

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

Corollary 16 *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 7.

Theorem 17 *Define* $\Lambda = \#\mathcal{Q} + 2g(\mathcal{F})$ *and* $M_T = (q-1)\Lambda + 2g(\mathcal{F}) - 1$. *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 7. 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 13 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 7, 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 7. ■

In case $n = 1$ and the hypotheses from Proposition 15 are satisfied, we obtain the following result:

Corollary 18 *Suppose that for any* $\lambda \in H(P_1)$ *there exists* $f \in L(\lambda P_1) \backslash L((\lambda - 1)P_1)$ *such that* $f(Q) \in T$ *for all* $Q \in \mathcal{Q}$. *Then*

$$\#\mathcal{Q} \leq \#H(P_1) \backslash ((q-1)H^*(P_1) + H(P_1)).$$

Proof. Since $n = 1$, the only sequence we can choose is $-1, 0, 1, 2, \ldots$. However, under the stated assumptions, a pair $(k-1, k)$ is T-negligible if and only if $k \in (q-1)H^*(P_1) + H(P_1)$. ■

We will now give some examples.

Example 19 *This example is a continuation of Example 8. 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 8, 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 18 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* $N(\mathcal{F}_1) \leq 24$. *Since* $N(\mathcal{F}_1) = 24$, *Corollary 18 gives a tight bound in this case.*

Example 20 *This example is a continuation of Example 11. There we have seen that* $N(\mathcal{F}_2) \leq 31$. *This can also been seen using Corollary 18. From Equation (2), we see that there are at most* 4 *rational places* P *of* $\mathcal{F}_2$ *with* $x(P) = 0$ *or* $y(P) = 0$ *and a unique pole of* x *and* y. *On the other hand applying Corollary 18 to the semigroup* $H(P_2) = \langle 4, 5 \rangle$, *we get that* $\#\mathcal{Q} \leq 26$. *Therefore* $N(\mathcal{F}_2) \leq 4 + 1 + 26 = 31$.

References

[1] Roger Apéry. Sur les branches superlinéaires des courbes algébriques. *C. R. Acad. Sci. Paris*, 222:1198–1200, 1946.

[2] Peter Beelen. The order bound for general algebraic geometric codes. *Finite Fields Appl.*, 13(3):665–680, 2007.

[3] Peter Beelen and Nesrin Tutaş. A generalization of the Weierstrass semigroup. *J. Pure Appl. Algebra*, 207(2):243–260, 2006.

[4] Maria Bras-Amorós and Albert Vico-Oton. On the Geil-Matsumoto bound and the length of AG codes. *Des. Codes Cryptogr.*, Accepted.

[5] E. W. Dijkstra. A note on two problems in connexion with graphs. *Numer. Math.*, 1:269–271, 1959.

[6] Olav Geil and Ryutaroh Matsumoto. 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.

[7] Tom Høholdt, Jacobus H. van Lint, and Ruud Pellikaan. Algebraic geometry of codes. In *Handbook of coding theory, Vol. I, II*, pages 871–961. North-Holland, Amsterdam, 1998.

[8] Joseph Lewittes. Places of degree one in function fields over finite fields. *J. Pure Appl. Algebra*, 69(2):177–183, 1990.

[9] J. C. Rosales and P. A. García-Sánchez. *Numerical semigroups*, volume 20 of *Developments in Mathematics*. Springer, New York, 2009.

[10] Henning Stichtenoth. *Algebraic function fields and codes*. Universitext. Springer-Verlag, Berlin, 1993.

[11] Gerard van der Geer, Everett Howe, Kristin Lauter, and Christophe Ritzenthaler. manYPoints – Table of Curves with Many Points. Online available at `http://www.manypoints.org`, 2011.