Journal of Pure and Applied Algebra 213 (2009) 1152–1156

Contents lists available at ScienceDirect

Journal of Pure and Applied Algebra

journal homepage: www.elsevier.com/locate/jpaa

Bounding the number of $\mathbb{F}_q$-rational places in algebraic function fields using Weierstrass semigroups

Olav Geil [a,*], Ryutaroh Matsumoto [b]

[a] Department of Mathematical Sciences, Aalborg University, 9220, Denmark

[b] Department of Communications and Integrated Systems, Tokyo Institute of Technology, 152-8550, Japan

ARTICLE INFO

Article history:
Received 12 December 2007
Received in revised form 25 September 2008
Available online 19 December 2008
Communicated by J. Walker

MSC:
Primary: 14G15
11G20
14H05
14H25

ABSTRACT

We present a new bound on the number of $\mathbb{F}_q$-rational places in an algebraic function field. It uses information about the generators of the Weierstrass semigroup related to a rational place. As we demonstrate, the bound has implications to the theory of towers of function fields.

1. Introduction

Throughout this paper by a function field we will always mean an algebraic function field of one variable. Given a function field $\mathbb{F}/\mathbb{F}_q$, we denote by $N(\mathbb{F})$ the number of rational places and we denote by $g(\mathbb{F})$ the genus. We will always assume that $\mathbb{F}_q$ is the full constant field of $\mathbb{F}$. For applications in coding theory it is desirable to have $N(\mathbb{F})/g(\mathbb{F})$ as high as possible as this allows for the construction of codes with good parameters. The above observation has led to extensive research on the problem of deciding, given a constant field $\mathbb{F}_q$ and a number g, what is the highest number $N_q(g)$ such that a function field $\mathbb{F}/\mathbb{F}_q$ exists with $N(\mathbb{F}) = N_q(g)$ and $g(\mathbb{F}) = g$.

Recall that, for any rational place the number of gaps in the corresponding Weierstrass semigroup Λ equals the genus g of the corresponding function field. This suggests that in some cases a Weierstrass semigroup Λ for a rational place might hold more information about the number of rational places of the function field than does the genus alone. This theme was firstly explored by Lewittes in [4], though the bound by Stöhr and Voloch ([9, pp. 14–15]) induces a bound in terms of a Weierstrass semigroup under certain conditions. The smallest non-zero element in a numerical semigroup Λ is called the multiplicity of Λ and we denote it by λ_1. Lewittes showed that if λ_1 is the multiplicity of a Weierstrass semigroup corresponding to a rational place of $\mathbb{F}/\mathbb{F}_q$ then $N(\mathbb{F}) \leq q\lambda_1 + 1$ holds. In the present paper we derive an improved upper bound on $N(\mathbb{F})$ as we take into account not only the multiplicity but also all the other elements in a generating set of Λ.

2. The bounds

In the following Λ is always a numerical semigroup with finitely many gaps and $\{\lambda_1, \ldots, \lambda_m\}$ is a generating set for Λ with $0 < \lambda_1 < \cdots < \lambda_m$.

* Corresponding author.
E-mail addresses: olav@math.aau.dk (O. Geil), ryutaroh@rmatsumoto.org (R. Matsumoto).
URLs: http://www.math.aau.dk/~olav/publications.html (O. Geil), http://www.rmatsumoto.org/research.html (R. Matsumoto).

0022-4049/$ – see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.jpaa.2008.11.013

Definition 1. Let Λ be fixed. If there exist function fields over $\mathbb{F}_q$ having a rational place whose Weierstrass semigroup is equal to Λ then we define

$$N_q(\Lambda) = \max\{N(\mathbb{F}) \mid \mathbb{F} \text{ is a function field over } \mathbb{F}_q \text{ having a rational place which Weierstrass semigroup equals } \Lambda\}.$$

If such function fields do not exist, we define $N_q(\Lambda) = 0$.

Theorem 1.

$$N_q(\Lambda) \leq \#\left(\Lambda \setminus \bigcup_{i=1}^{m} (q\lambda_i + \Lambda)\right) + 1 \tag{1}$$

which implies

$$N_q(\Lambda) \leq \#(\Lambda \setminus (q\lambda_1 + \Lambda)) + 1 = q\lambda_1 + 1. \tag{2}$$

Here, $\gamma + \Lambda$ means $\{\gamma + \lambda \mid \lambda \in \Lambda\}$.

Proof. Let $\mathbb{F}/\mathbb{F}_q$ be a function field. Let its rational places be $\mathcal{P}_1, \ldots, \mathcal{P}_{N-1}, \mathcal{P}$ and assume that the Weierstrass semigroup corresponding to $\mathcal{P}$ is Λ. Define $\mathcal{L} = \cup_{s=0}^{\infty} \mathcal{L}(s\mathcal{P})$ and let $\mathcal{L}_t = \mathcal{L}(t\mathcal{P})$ for $t \in \mathbb{N}_0 \cup \{-1\}$. In particular $\mathcal{L}_{-1} = \{0\}$. It is well known that

$$\mathcal{L}_t = \mathcal{L}_{t-1} \quad \text{if } t \in \mathbb{N}_0 \setminus \Lambda \quad \text{and} \quad \dim(\mathcal{L}_t) = \dim(\mathcal{L}_{t-1}) + 1 \quad \text{if } t \in \Lambda. \tag{3}$$

Here dim denotes the dimension as a vector space over $\mathbb{F}_q$. Let $\varphi : \mathcal{L} \to \mathbb{F}_q^{N-1}$ be the map $\varphi(f) = (f(\mathcal{P}_1), \ldots, f(\mathcal{P}_{N-1}))$ and define $E_t = \varphi(\mathcal{L}_t)$ for $t \in \mathbb{N}_0 \cup \{-1\}$. From Eq. (3) we observe that $\dim(E_{-1}) = 0$ and that $\dim(E_t) = \dim(E_{t-1})$ for all $t \in \mathbb{N}_0 \setminus \Lambda$. For $t \in \Lambda$ we can either have $\dim(E_t) = \dim(E_{t-1})$ or $\dim(E_t) = \dim(E_{t-1}) + 1$. The map φ is surjective meaning that for t large enough $\dim(E_t) = N - 1$. Hence, if we can give an upper bound on the number of $t \in \Lambda$ for which $\dim(E_t) = \dim(E_t - 1) + 1$ holds then this upper bound will also be an upper bound on the number $N - 1$. To prove Eq. (1) we therefore only need to show that $\dim(E_t) = \dim(E_{t-1}) + 1$ cannot happen when $t \in q\lambda_i + \Lambda$ for some i. For this purpose let for $i = 1, \ldots, m$, $x_i \in \mathcal{L}$ be an element with $-v_{\mathcal{P}}(x_i) = \lambda_i$. Here $v_{\mathcal{P}}$ is the valuation corresponding to $\mathcal{P}$. Given $t = q\lambda_i + \lambda$ with $\lambda \in \Lambda$ choose $f \in \mathcal{L}_\lambda \setminus \mathcal{L}_{\lambda-1}$. We have $x_i^q f \in \mathcal{L}_t \setminus \mathcal{L}_{t-1}$ and $x_i f \in \mathcal{L}_{t-1}$. Clearly, $\varphi(x_i^q f) = \varphi(x_i f)$ and the proof of Eq. (1) is complete. The left part of Eq. (2) is an immediate consequence of Eq. (1) and the right part corresponds to [3, Lemma 5.15]. □

The Serre bound implies that if Λ is of genus g then

$$N_q(\Lambda) \leq g\lfloor 2\sqrt{q} \rfloor + q + 1 \tag{4}$$

holds. We observe that Lewittes' bound (2) is better than the bound (4) if and only if $(\lambda_1 - 1)/g < \lfloor 2\sqrt{q} \rfloor/q$ holds. As a consequence the bound (2) is always better than the bound (4) when $q \leq 4$.

Example 1. In Table 1 we consider a collection of 3 semigroups. We apply the bounds to a number of fields of characteristics 2 and 3. Restricting to characteristics 2 and 3 allows us to get information on the number $N_q(g)$ from van der Geer and van der Vlugt's table in [2]. An entry x/y in the row named "bounds" indicates that Lewittes' bound produces x and that the new bound produces y. An interval in the row named $N_q(g)$ means that $N_q(g)$ is known to be in this interval. By $\langle \lambda_1, \ldots, \lambda_n \rangle$ we mean the semigroup generated by $\lambda_1, \ldots, \lambda_n$. Table 1 illustrates that the new bound can be quite an improvement to Lewittes' bound and that it can be much smaller than $N_q(g)$ also when Lewittes' bound is not. We get the most significant results for small q.

Example 2. From [2] we have $N_2(8) = 11$, $N_3(8) \in \{17, 18\}$ and $N_4(8) \in \{21, 22, 23, 24\}$. If one applies the bounds (1) and (2) to the 67 different semigroups of genus 8 (these semigroups can be found at [5]) one gets the following picture. Lewittes' bound tells us that in a function field over $\mathbb{F}_2$ of genus 8 and with $N_2(8) = 11$ rational places 13 semigroups are not allowed as Weierstrass semigroups of a rational place. The new bound gives us that 33 semigroups are not allowed. Assuming that $N_3(8) = 18$ and $N_4(8) = 24$ Lewittes' bound excludes in both cases 26 semigroups whereas the new bound excludes in both cases 31 semigroups.

The following Proposition gives us some information on how good or bad the bound in Eq. (1) can possibly be.

Proposition 1. *We have*

$$q\lambda_1 + 1 - g \leq \#\left(\Lambda \setminus \left(\bigcup_{i=1}^{m} (q\lambda_i + \Lambda)\right)\right) + 1 \leq \min\{q\lambda_1 + 1, q^m + 1\}.$$

Table 1
Semigroups from Example 1.

$\Lambda = \langle 8, 9, 20\rangle \quad g = 20$						
q	2	3	4	8	9	16
Bounds	17/9	25/16	33/25	65/65	73/73	129/129
$N_q(g)$	19–21	30–34	40–45	76–83	70–91	127–139
$\Lambda = \langle 13, 14, 20\rangle \quad g = 42$						
q	2	3	4	8	9	16
Bounds	27/9	40/17	53/33	105/95	118/102	209/195
$N_q(g)$	33–35	52–59	75–80	129–147	122–161	209–254
$\Lambda = \langle 10, 11, 20, 22\rangle \quad g = 45$						
q	2	3	4	8	9	16
Bounds	21/5	31/10	41/17	81/65	91/82	161/141
$N_q(g)$	33–37	54–62	80–84	144–156	136–170	242–268

Proof. To see the first inequality observe that there are at least $q\lambda_1 - g$ elements in Λ that are smaller than $q\lambda_1$, and these elements must belong to $\Lambda \setminus \cup_{i=1}^{m}(q\lambda_i + \Lambda)$. Regarding the last inequality the upper bound $\lambda_1 q + 1$ comes from Theorem 1. To see the upper bound $q^m + 1$ we note that all $\lambda \in \Lambda$ can be written as $a_1\lambda_1 + \cdots + a_m\lambda_m$ for some $a_1, \ldots, a_m \in \mathbb{N}_0$. If $\lambda \in \Lambda \setminus (\cup_{i=1}^{m}(q\lambda_i + \Lambda))$ then necessarily $a_1, \ldots, a_m < q$ must hold. □

We now present some corollaries to Theorem 1.

Corollary 1. *Define* $t = \#\{\lambda \in \Lambda \mid \lambda \in [\lambda_1 + 1, \lambda_1 + \lceil \lambda_1/q \rceil - 1]\}$. *We have* $N_q(\Lambda) \leq q\lambda_1 - t + 1$.

Proof. For $\lambda \in \Lambda$ with $\lambda \in [\lambda_1 + 1, \lambda_1 + \lceil \lambda_1/q \rceil - 1]$ we have $q\lambda \neq q\lambda_1 + \eta$ for any $\eta \in \Lambda$ as there are no non-zero $\eta \in \Lambda$ with $\eta < \lambda_1$. This implies $q\lambda \in (\cup_{i=1}^{m}(q\lambda_i + \Lambda)) \setminus (q\lambda_1 + \Lambda)$. Therefore the number on the right side of Eq. (1) is at least t smaller than the number on the right side of Eq. (2). □

Example 3. Consider the case $\lambda_1 = g + 1$. That is, the case $\Lambda = \{0, g + 1, g + 2, \ldots\}$. The number t from Corollary 1 becomes equal to $\lceil (g + 1)/q \rceil - 1$. Hence

$$N_q(\Lambda) \leq q(g + 1) + 2 - \lceil (g + 1)/q \rceil \tag{5}$$

holds. Given $\lambda > \lambda_1$ we have $q\lambda \notin q\lambda_1 + \Lambda$ if and only if $\lambda \in [\lambda_1 + 1, \lambda_1 + \lceil \lambda_1/q \rceil - 1]$ and $q\lambda + \eta \in q\lambda_1 + \Lambda$ holds for all $\eta \in \Lambda \setminus \{0\}$. Hence, for the particular semigroup in the present example, we have

$$\#\left(\Lambda \setminus \left(\bigcup_{i=1}^{m}(\lambda_i + \Lambda)\right)\right) + 1 = q\lambda_1 - t + 1 = q(g + 1) + 2 - \lceil (g + 1)/q \rceil.$$

Remark 1. The conductor of a semigroup $\Lambda \subseteq \mathbb{N}_0$ with finitely many gaps is the smallest number c such that there are no gaps greater or equal to c. The conductor is known to be smaller or equal to $2g$ ([3, Proposition 5.7]). If $q\lambda_1 + c \leq q\lambda_2$ then it is clear that the number on the right side of Eq. (1) is the same as the number on the right side of Eq. (2). In particular the numbers are the same if $q\lambda_1 + 2g \leq q\lambda_2$.

3. Bounds on $N_q(g)$

From Lewittes' bound (2) we immediately get $N_q(g) \leq q(g + 1) + 1$ as the multiplicity of a semigroup with g gaps can be at most $g + 1$. This fact is not stressed in [4] as the paper contains slightly better bounds on $N_q(g)$ namely $N_q(g) \leq qg + 2$ ([4, Theorem 1, part (a)]) and $N_2(g) \leq 2g - 2$ ([4, Eq. (19)]). We now investigate the implication of the new result in Eq. (1) for establishing bounds on $N_q(g)$. We get the following proposition.

Proposition 2.

$$N_q(g) \leq \left(q - \frac{1}{q}\right) g + q + 2 - \frac{1}{q}. \tag{6}$$

Proof. The proof uses Corollary 1. An estimate of the number t in Corollary 1 can be given in terms of λ_1 and g alone. We have

$$t \geq \lceil \lambda_1/q \rceil - 1 - (g - (\lambda_1 - 1)) \geq \frac{\lambda_1}{q} + \lambda_1 - g - 2$$

as there are $g-(\lambda_1-1)$ gaps greater than λ_1. Hence,

$$N_q(g) \leq \max\left\{q\lambda_1 - \left(\frac{\lambda_1}{q}+\lambda_1-g-2\right)+1 \mid 2\leq\lambda_1\leq g+1\right\}. \quad \square$$

Observe, that the bound (6) was obtained by showing that the semigroup considered in Example 3 is the worst case. Proposition 2 implies

$$N_2(g) \leq 1\frac{1}{2}g+3\frac{1}{2}, \qquad N_3(g)\leq 2\frac{2}{3}g+4\frac{2}{3}, \qquad N_4(g)\leq 3\frac{3}{4}g+5\frac{3}{4} \tag{7}$$

which is much better than Serre's upper bound. It should be mentioned that the bounds in Eqs. (7) compete with Ihara's bound only for small values of g.

4. Towers of function fields

Recall, that a sequence of function fields $(F^{(1)}/\mathbb{F}_q, F^{(2)}/\mathbb{F}_q, \cdots)$ is called a tower if $F^{(i)}\subseteq F^{(i+1)}$ holds for all $i\geq 1$. Given a tower of function fields we write $N^{(i)}=N(F^{(i)})$, $g^{(i)}=g(F^{(i)})$ and we say that the tower is asymptotically good if $g^{(i)}\to\infty$ for $i\to\infty$ and $\liminf_{i\to\infty}(N^{(i)}/g^{(i)})=\kappa$ holds for some $\kappa>0$. Eq. (8) in the following corollary is a consequence of Lewittes' bound (2). Eq. (9) seems a well-known fact but it also immediately follows from the last part of Proposition 1.

Corollary 2. *Assume a tower of function fields is given with $g^{(i)}\to\infty$ for $i\to\infty$ and $\liminf_{i\to\infty}(\frac{N^{(i)}}{g^{(i)}})=\kappa>0$. Let $(\mathcal{P}^{(1)},\mathcal{P}^{(2)},\ldots)$ be any sequence such that $\mathcal{P}^{(i)}$ is a rational place of $F^{(i)}$ for $i=1,2,\ldots$. Let $\lambda_1^{(i)}$ be the multiplicity of the Weierstrass semigroup $\Lambda^{(i)}$ related to $\mathcal{P}^{(i)}$ and let m_i be the number of generators in some description of $\Lambda^{(i)}$. We have*

$$\liminf_{i\to\infty}(\lambda_1^{(i)}/g^{(i)})\geq\kappa/q, \tag{8}$$

$$m_i\to\infty \quad \text{for } i\to\infty. \tag{9}$$

Example 4. In [1] Garcia and Stichtenoth introduced a tower of function fields over $\mathbb{F}_{q^2}$ which satisfies $g^{(i)}\to\infty$ for $i\to\infty$ and $\lim_{i\to\infty}(N^{(i)}/g^{(i)})=q-1$. This tower was further studied in [8] where Pellikaan, Stichtenoth and Torres found the generators of a sequence of Weierstrass semigroups related to it. Using the results in [8] one finds that $\lim_{i\to\infty}(\lambda_1^{(i)}/g^{(i)})=1/q$ holds. For comparison Eq. (8) reads $\liminf_{i\to\infty}(\lambda_1^{(i)}/g^{(i)})\geq(1-(1/q))/q$.

For the construction of one-point geometric Goppa codes with efficient decoding algorithms [3], we need a basis $\{f_1,f_2,\ldots\}$ of $\mathcal{L}(i\mathcal{P})$ such that $v_{\mathcal{P}}(f_i)>v_{\mathcal{P}}(f_{i+1})$ and have to compute $f_i(\mathcal{P}_j)$, which are generally difficult even when a set of defining equations is explicitly provided. Miura [6] and Pellikaan [7] independently and simultaneously proposed a standard form of defining equations for affine algebraic curves which renders that the subsequent finding of the required f_i's and the computing of $f_i(\mathcal{P}_j)$ is straightforward. The number of equations in that standard form becomes the minimum if and only if the Weierstrass semigroup Λ of $\mathcal{P}$ is telescopic [10]. Therefore, it is desirable to find asymptotically good towers of function fields with telescopic Weierstrass semigroups. We will show that we cannot find such a tower.

Definition 2. Let $(a_1,\ldots,a_k)$ be a sequence of positive integers. Define $d_i=\gcd(a_1,\ldots,a_i)$, $i=1,\ldots,k$. If $d_k=1$ and $a_i/d_i\in\langle a_1/d_{i-1},\ldots,a_{i-1}/d_{i-1}\rangle$ for $i=2,\ldots,k$, then the sequence $(a_1,\ldots,a_k)$ is called telescopic. A semigroup is called telescopic if it is generated by a telescopic sequence.

We will need the following result corresponding to [3, Lem. 5.34].

Lemma 1. *If $(a_1,\ldots,a_k)$ is telescopic then for any $\lambda\in\langle a_1,\ldots,a_k\rangle$ there exist (uniquely determined) non-negative integers $x_1,\ldots,x_k$ such that $0\leq x_j<d_{j-1}/d_j$ for $2\leq j\leq k$ and $\lambda=\sum_{j=1}^{k}x_ja_j$.*

Proposition 3. *Let $(F^{(1)}/\mathbb{F}_q, F^{(2)}/\mathbb{F}_q,\ldots)$ be a tower of function fields such that for infinitely many i the following holds: $F^{(i)}$ possesses a rational place $\mathcal{P}^{(i)}$ having a telescopic Weierstrass semigroup $\Lambda^{(i)}$. Then the tower is asymptotically bad.*

Proof. Let $(\lambda_1^{(i)},\ldots,\lambda_{m_i}^{(i)})$ be a telescopic sequence generating $\Lambda^{(i)}$ with m_i being the smallest possible. By [6, pp. 1420–1421], $\{\lambda_1^{(i)},\ldots,\lambda_{m_i}^{(i)}\}$ is a minimum generating set for $\Lambda^{(i)}$. Write $d_j^{(i)}=\gcd(\lambda_1^{(i)},\ldots,\lambda_j^{(i)})$ for $1\leq j\leq m_i$. Clearly, $d_j^{(i)}\mid d_{j-1}^{(i)}$ for $j\geq 2$ and by minimality of m_i, Lemma 1 implies $d_{j-1}^{(i)}\geq 2d_j^{(i)}$. The genus $g^{(i)}$ is given by the following expression (see [3, Pro. 5.35])

$$g^{(i)}=\left(1+\sum_{j=2}^{m_i}\left(\frac{d_{j-1}}{d_j}-1\right)\lambda_j^{(i)}\right)\Big/2,$$

and therefore $g^{(i)}\geq\frac{m_i-1}{2}\lambda_1^{(i)}$ holds. From Eq. (8) we see that the only hope for the tower to be asymptotically good is that the sequence of m_i's is bounded above. Eq. (9) tells us the opposite. $\square$

Acknowledgments

The authors would like to thank Peter Beelen, Tom Høholdt, Massimiliano Sala, Ruud Pellikaan and Masaaki Homma for pleasant discussions.

References

[1] A. Garcia, H. Stichtenoth, On the asymptotic behaviour of some towers of function fields over finite fields, J. Number Theory 61 (1996) 248–273.
[2] G. van der Geer, M. van der Vlugt, Tables of curves with many points, (November 17, 2007) http://www.science.uva.nl/~geer/tables-mathcomp18.pdf.
[3] T. Høholdt, J. van Lint, R. Pellikaan, Algebraic Geometry Codes, in: V.S. Pless, W.C. Huffman (Eds.), Handbook of Coding Theory, vol. 1, Elsevier, Amsterdam, 1998, pp. 871–961. (Chapter 10).
[4] J. Lewittes, Places of degree one in function fields over finite fields, J. Pure Appl. Algebra 69 (1990) 177–183.
[5] Nivaldo Medeiros, homepage http://w3.impa.br/nivaldo/algebra/semigroups/ (September 26, 2008).
[6] S. Miura, Linear codes on affine algebraic curves, Trans. IEICE J81-A (1998) 1398–1421 (in Japanese).
[7] R. Pellikaan, On the existence of order functions, J. Statist. Plann. Inference 94 (2001) 287–301.
[8] R. Pellikaan, H. Stichtenoth, F. Torres, Weierstrass semigroups in an asymptotically good tower of function fields, Finite Fields Appl. 4 (1998) 381–392.
[9] K.O. Stöhr, J.F. Voloch, Weierstrass points and curves over finite fields, Proc. London Math. Soc. (3) 52 (1986) 1–19.
[10] J. Suzuki, Miura conjecture on affine curves, Osaka J. Math 44 (2007) 187–196.