Constructing sequences with high nonlinear complexity using the Weierstrass semigroup of a pair of distinct points of a Hermitian curve

Geil, Hans Olav; Ozbudak, Ferruh; Ruano Benito, Diego

Published in:
Semigroup Forum

DOI (link to publication from Publisher):
10.1007/s00233-018-9976-8

Publication date:
2019

Document Version
Accepted author manuscript, peer reviewed version

Constructing Sequences with High Nonlinear Complexity Using the Weierstrass Semigroup of a Pair of Distinct Points of a Hermitian Curve*

Olav Geil†, Ferruh Özbudak‡, Diego Ruano§

Abstract

Using the Weierstrass semigroup of a pair of distinct points of a Hermitian curve over a finite field, we construct sequences with improved high nonlinear complexity. In particular we improve the bound obtained in [15, Theorem 3] considerably and the bound in [15, Theorem 4] for some parameters.

1 Introduction

Goppa introduced a very general and useful method for constructing linear codes with very good designed parameters [7, 8]. These linear codes are called *Goppa codes* or *algebraic geometry codes*. The method uses a divisor G which corresponds to a generator matrix of the linear codes in the end. One of the main tools used in the designed parameters of the linear code is the Riemann-Roch theorem applied on G. Later Garcia, Kim and Lax [5] improved the bound on the designed minimum distance of the linear code if the support of G consists of one point P using the Weierstrass semigroup of P. Similarly Matthews [9] improved the bound on the minimum distance of the linear code if the support of G consists of two distinct points P_1 and P_2 using the Weierstrass semigorup of the pair (P_1, P_2). Nowadays there are a lot of works devoted to further results on Weierstrass semigroups at several points on curves and their applications to coding theory (see, for example, [1], [2], [3],[18]).

*Published in Semigroup Forum, accepted for publication.
This work was supported by The Danish Council for Independent Research (Grant No. DFF–4002-00367), by the Spanish MINECO/FEDER (Grant No. MTM2015-65764-C3-2-P, MTM2015-69138-REDT and RYC-2016-20208 (AEI/FSE/UE)) and by METU Coordinatorship of Scientific Research Projects via grant for projects BAP-01-01-2016-008 and BAP-07-05-2017-007.

†Department of Mathematical Sciences, Aalborg University, Denmark, olav@math.aau.dk

‡Department of Mathematical Sciences, Aalborg University, Denmark and Institute of Applied Mathematics and the Department of Mathematics, Middle East Technical University, Turkey, ozbudak@metu.edu.tr

§IMUVA (Mathematics Research Institute), University of Valladolid, Spain and Department of Mathematical Sciences, Aalborg University, Denmark, diego.ruano@uva.es

In fact the ideas of Goopa are very general. There has been many approaches using similar methods in various problems in coding theory and cryptography (see, for example, [13], [14] and the references therein). In many of these applications Hermitian curves over finite fields are used because of their excellent arithmetic and geometric properties.

Sequences over finite fields from the complexity-theoretic standpoint have many applications in cryptography and pseudorandom number generation. We refer to [4, 10, 11, 16] for some classical results and a recent survey. There are many results on linear complexity of sequences over finite fields. Recently there have been interesting results in the nonlinear complexity of sequences (see, for example, [12, 15]). They use the notion of $k-$th order nonlinear complexity as defined below.

Let $\mathbb{F}_q$ and $\mathbb{F}_{q^2}$ denote the finite fields with q and q^2 elements.

Definition 1.1. Let $\mathbf{s} = (s_1, s_2, \ldots, s_n)$ be a sequence of length $n \geq 1$ over the finite field $\mathbb{F}_q$ and let $k \in \mathbb{N}$. If $s_i = 0$ for all $1 \leq i \leq n$, then we define the *$k-th$ order nonlinear complexity* $N^k(\mathbf{s})$ to be 0. Otherwise let $N^k(\mathbf{s})$ be the smallest $m \in \mathbb{N}$ for which there exists a polynomial $f \in \mathbb{F}_q[x_1, \ldots, x_m]$ of degree at most k in each variable such that

$$s_{i+m} = f(s_i, s_{i+1}, \ldots, s_{i+m-1}) \text{ for } 1 \leq i \leq n - m.$$

In [15], among other results, they give a construction of sequences with high nonlinear complexity using a Hermitian curve. As we use the Hermitian curve over $\mathbb{F}_{q^2}$, it suits better to consider sequences over $\mathbb{F}_{q^2}$ (cf. Definition 1.1) in this paper. In [15] they construct a long sequence of length $(q-1)(q^2-1)$ over $\mathbb{F}_{q^2}$ with high nonlinear complexity. Their main tools are an explicit automorphism of the Hermitian curve and the Riemann-Roch theorem. The main ideas are again similar to Goppa's ideas in general.

In this paper we improve their results using the structure of Weierstrass pairs of distinct points of a Hermitian curve. In particular our main results improve the bounds in [15, Theorem 3] for all parameters considerably. Moreover we also improve bounds in [15, Theorem 4] for some parameters. This is very analogous to the situation of improving the designed parameters of the linear codes using Weierstrass semigroups in Goppa construction.

We use the language of algebraic function fields, which is essentially equivalent to the language of algebraic curves, and we refer to [17] for the notation and background. For the sake of simplicity we use the term *rational place* instead of *place of degree one* from now on throughout the paper.

Let H denote the Hermitian function field

$$H = \mathbb{F}_{q^2}(x, y) \text{ with } y^q + y = x^{q+1}.$$

Recall that $\mathbb{F}_{q^2}$ is the full constant field of H. Moreover H has $q^3 + 1$ distinct rational places and its genus is $\dfrac{q(q-1)}{2}$.

The rest of this paper is organized as follows. We give the construction and state our main results in Section 2. We prove our results in Section 3. We compare our new bounds and the bounds of [15] in Section 4.

2 Construction and the Main Result

Let $\theta \in \mathbb{F}_{q^2}^\star$ be a generator of the multiplicative group of $\mathbb{F}_{q^2}^\star$. Let $\phi : H \to H$ be the automorphism of H fixing $\mathbb{F}_{q^2}$ defined as

$$\begin{array}{rlll} \phi: & H & \to H & \\ & x & \mapsto \theta x & \\ & y & \mapsto \theta^{q+1} y. & \end{array} \tag{1}$$

Note that $\phi^{(q^2-1)} = \iota$, where ι is the identity automorphism of H. Let P_∞ be the rational place of H corresponding to the common pole of x and y. It is clear that ϕ fixes P_∞. The action of ϕ on the rational places of H is well-known [6]. In particular, there exist distinct rational places $Q, P_1, P_2, \ldots, P_{q-1}$ different from P_∞ such that their orbits under ϕ are distinct and having length equal to $q^2 - 1$. The following is a partial list of distinct orbits of the rational places of H under ϕ:

- P_∞
- $Q, \phi(Q), \ldots, \phi^{(q^2-2)}(Q)$
- $P_1, \phi(P_1), \ldots, \phi^{(q^2-2)}(P_1)$

$\vdots$

- $P_{q-1}, \phi(P_{q-1}), \ldots, \phi^{(q^2-2)}(P_{q-1})$.

The union of these orbits form $1 + q(q^2-1) = q^3 - q + 1$ distinct rational places. We do not use the remaining of q rational places in this paper. We fix the notation of these rational places throughout the paper.

The following proposition is crucial for our construction. We need to use certain facts from the theory of Weierstrass pairs of rational places of the Hermitian function field H in its proof. We give a proof in Section 3 below.

Proposition 2.1. *Under notation and assumptions as above there exists $h \in H$ such that its pole divisor satisfies*

$$(h)_\infty = (q-1)P_\infty + (q-1)Q.$$

We also fix h and use it in our construction below.

Remark 2.2. The main difference of our construction with the corresponding construction of [15] is as follows. Using only the Riemann-Roch Theorem in [15], they obtain existence of $f \in H$ such that its pole divisor satisfies

$$(f)_\infty = (2g-1)P_\infty + Q,$$

where g is the genus $\dfrac{q(q-1)}{2}$ of H. It turns out that using h as in Proposition 2.1 instead of f gives a construction with much higher nonlinear complexity lower bound. Note that existence of h as in Proposition 2.1 does not follow from the Riemann-Roch theorem directly and it requires more knowledge of subtle geometric structures of the Hermitian function field H.

Remark 2.3. The full knowledge of the Weierstrass semigroup of a pair of distinct rational places of the Hermitian function field allows us to choose the best tuple (a, b) of positive integers such that there exists a pole divisor $(h)_\infty = aP_\infty + bQ$ giving the best designed lower bound on $N^{(k)}(\mathbf{s_n})$ for the constructed sequence $\mathbf{s_n}$ in Theorem 2.4 below.

We are ready to present our construction.

Construction 1. *Under notation and construction as above let* $M = (q-1)(q^2-1)$ *and* $\mathbf{s} = (s_1, \ldots, s_M)$ *be a sequence of length* M *with terms in* $\mathbb{F}_{q^2}$ *defined as*

$$\begin{array}{llll}
s_1 = h(P_1), & s_2 = h(\phi(P_1)), & \cdots, & s_{q^2-1} = h\left(\phi^{(q^2-2)}(P_1)\right), \\
s_{q^2} = h(P_2), & s_{q^2+1} = h(\phi(P_2)), & \cdots, & s_{2(q^2-1)} = h\left(\phi^{(q^2-2)}(P_2)\right), \\
s_{2q^2-1} = h(P_3), & s_{2q^2} = h(\phi(P_3)), & \cdots, & s_{3(q^2-1)} = h\left(\phi^{(q^2-2)}(P_3)\right), \\
\quad \vdots & \quad \vdots & & \quad \vdots \\
s_{(q-2)(q^2-1)+1} & s_{(q-2)(q^2-1)+2} & & s_{(q-1)(q^2-1)} \\
\quad = h(P_{q-1}), & \quad = h(\phi(P_{q-1})), & \cdots, & \quad = h\left(\phi^{(q^2-2)}(P_{q-1})\right).
\end{array}$$

Namely for $0 \le i \le q-2$ *and* $1 \le i \le q^2-1$ *we have*

$$s_{iq+j} = h\left(\phi^{(j-1)}(P_{i+1})\right).$$

The following is our first result.

Theorem 2.4. *Under notation and assumptions as above, let* $1 \le n \le M = (q-1)(q^2-1)$ *be an integer and consider the initial sequence* $\mathbf{s_n} = (s_1, s_2, \ldots, s_n)$ *of the sequence* $\mathbf{s}$ *constructed in Construction 1 above. For any integer* $1 \le k \le q^2-1$*, we have*

$$N^{(k)}(\mathbf{s_n}) \ge \frac{\lfloor \frac{n}{q^2-1} \rfloor (q^2-1) - (q-1)}{\lfloor \frac{n}{q^2-1} \rfloor + 2k(q-1)} \tag{2}$$

for the $k-$*th order nonlinear complexity.*

Remark 2.5. Theorem 2.4 gives a much improved lower bound on $N^{(k)}(\mathbf{s_n})$ compared to the lower bound of [15, Theorem 3] for all parameters. Recall that in [15] they construct a sequence $\mathbf{t}$ using Hermitian function field of length $M = (q-1)(q^2-1)$ with terms in $\mathbb{F}_{q^2}$. For their initial sequence $\mathbf{t_n}$ with $1 \le n \le M$, the lower bound of [15, Theorem 3] is

$$N^{(k)}(\mathbf{t_n}) \ge \frac{\lfloor \frac{n}{q^2-1} \rfloor (q^2-1) - 1}{\lfloor \frac{n}{q^2-1} \rfloor + q(q-1)k}. \tag{3}$$

We compare (2) and (3) using some figures in Section 4 below.

The following is a direct corollary of Theorem 2.4 using the fact that $N^{(k)}(\mathbf{s_n})$ is an integer.

Corollary 2.6. *Under the notation and assumptions as in Theorem 2.4, for any integer* $1 \leq k \leq q^2 - 1$ *we have*

$$N^{(k)}(\mathbf{s_n}) \geq \left\lceil \frac{\lfloor \frac{n}{q^2-1} \rfloor (q^2-1) - (q-1)}{\lfloor \frac{n}{q^2-1} \rfloor + 2k(q-1)} \right\rceil . \tag{4}$$

Remark 2.7. Similarly the lower bound of [15, Theorem 3] has a direct improvement. Namely under notation and assumptions as in Remark 2 we have

$$N^{(k)}(\mathbf{s_n}) \geq \left\lceil \frac{\lfloor \frac{n}{q^2-1} \rfloor (q^2-1) - 1}{\lfloor \frac{n}{q^2-1} \rfloor + q(q-1)k} \right\rceil . \tag{5}$$

For comparison of (4) and (5) we also refer to Section 4 below.

The nonlinear complexity notion of Definition 1.1 is the main nonlinear complexity notion used, for example, in [15] and [12]. Moreover in [15] they also use a modified notion for nonlinear complexity, denoted as $L^k(\mathbf{s})$ instead of $N^k(\mathbf{s})$ (see [15, Remark 3]). The difference is that the condition "of degree at most k in each variable" in $N^k(\mathbf{s})$ is replaced with the condition "of total degree at most k" in $L^k(\mathbf{s})$. For the sake of clarity we formally give its definition here.

Definition 2.8. Let $\mathbf{s} = (s_1, s_2, \ldots, s_n)$ be a sequence of length $n \geq 1$ over the finite field $\mathbb{F}_q$ and let $k \in \mathbb{N}$. If $s_i = 0$ for all $1 \leq i \leq n$, then we define the $k-th$ *order nonlinear complexity* $L^k(\mathbf{s})$ to be 0. Otherwise let $L^k(\mathbf{s})$ be the smallest $m \in \mathbb{N}$ for which there exists a polynomial $f \in \mathbb{F}_q[x_1, \ldots, x_m]$ of total degree at most k such that

$$s_{i+m} = f(s_i, s_{i+1}, \ldots, s_{i+m-1}) \text{ for } 1 \leq i \leq n - m.$$

Note that our construction gives sequences over $\mathbb{F}_{q^2}$ and hence our statements in our results are over $\mathbb{F}_{q^2}$, although we formally present Definition 1.1 and Definition 2.8 over $\mathbb{F}_q$.

The following is our second result.

Theorem 2.9. *Under notation and assumptions as above, let* $1 \leq n \leq M = (q-1)(q^2-1)$ *be an integer and consider the initial sequence* $\mathbf{s_n} = (s_1, s_2, \ldots, s_n)$ *of the sequence* $\mathbf{s}$ *constructed in Construction 1 above. For any integer* $1 \leq k \leq q^2 - 1$*, we have*

$$L^{(k)}(\mathbf{s_n}) \geq \frac{\lfloor \frac{n}{q^2-1} \rfloor (q^2-1) - (k+1)(q-1)}{\lfloor \frac{n}{q^2-1} \rfloor + k(q-1)} \tag{6}$$

for the $k-th$ *order nonlinear complexity.*

Remark 2.10. It is trivial that $L^k(\mathbf{s}) \geq N^k(\mathbf{s})$ for all k. We remark that Theorem 2.9 gives a better bound than using the bound of Theorem 2.4 and the fact $L^k(\mathbf{s}) \geq N^k(\mathbf{s})$. This is the same phenomenon that happened in [15, Theorem 3 and Theorem 4], which also uses Hermitian function fields.

Remark 2.11. The lower bounds on $N^k(\mathbf{s})$ and $L^k(\mathbf{s})$ are important for all integers $1 \leq k \leq q^2 - 1$ as $\mathbf{s}$ is a sequence over $\mathbb{F}_{q^2}$. For example in [15, Remark 2] the authors explain the importance of the case $k = q^2 - 1$ corresponding the largest value of k for a sequence over $\mathbb{F}_{q^2}$.

Remark 2.12. Theorem 2.9 gives an improved lower bound on $L^k(\mathbf{s})$ compared to the bound of [15, Theorem 4] for relatively large k or small n. Under the notation of Remark 2.5 for the sequence $\mathbf{t}$ constructed in [15] using Hermitian function field, the lower bound of [15, Theorem 4] is

$$L^{(k)}(\mathbf{t_n}) \geq \frac{\lfloor \frac{n}{q^2-1} \rfloor (q^2-1) - (q^2-q-1)k - 1}{\lfloor \frac{n}{q^2-1} \rfloor + k}. \tag{7}$$

For example if k is near to $q^2 - 1$ (see Remark 2.11 above), then the bound of [15, Theorem 4] stated in (7) is negative and hence trivial. However our bound in Theorem 2.9 is always positive. We also compare (6) and (7) using some figures in Section 4 below.

Similarly to the situation above, the following is a direct corollary of Theorem 2.9 using the fact that $L^{(k)}(\mathbf{s_n})$ is an integer.

Corollary 2.13. *Under the notation and assumptions as in Theorem 2.9, for any integer* $1 \leq k \leq q^2 - 1$ *we have*

$$L^{(k)}(\mathbf{s_n}) \geq \left\lceil \frac{\lfloor \frac{n}{q^2-1} \rfloor (q^2-1) - (k+1)(q-1)}{\lfloor \frac{n}{q^2-1} \rfloor + k(q-1)} \right\rceil. \tag{8}$$

Remark 2.14. Again, the lower bound of [15, Theorem 3] has a direct improvement. Namely under notation and assumptions as in Remark 2.12 we have

$$L^{(k)}(\mathbf{s_n}) \geq \left\lceil \frac{\lfloor \frac{n}{q^2-1} \rfloor (q^2-1) - (q^2-q-1)k - 1}{\lfloor \frac{n}{q^2-1} \rfloor + k} \right\rceil. \tag{9}$$

For comparison of (8) and (9) we also refer to Section 4 below.

3 Proofs

In this section we present proofs of our results.

3.1 Proof of Proposition 2.1

Let P be a rational place of H. Let $W(P)$ denote its Weierstrass semigroup, which is defined as

$$W(P) = \{\alpha \in \mathbb{N}_0 : \text{ there exists } f \in H \text{ with } (f)_\infty = \alpha P\}.$$

The gap sequence $G(P)$ of P is defined as

$$G(P) = \mathbb{N}_0 \setminus W(P).$$

It is well-known that $G(P)$ (and hence $W(P)$) is the same for all rational places P of the Hermitian function field H (see, for example, [5]). Namely

$$\begin{aligned} G(P) &= \{1, 2, \ldots, q-2, q-1, \\ &\quad (q+1)+1, (q+1)+2, \ldots, (q+1)+(q-2), \\ &\quad 2(q+1)+1, 2(q+1)+2, \ldots, 2(q+1)+(q-3), \\ &\quad \vdots \\ &\quad (q-3)(q+1)+1, (q-3)(q+1)+2, \ldots, (q-3)(q+1)+2, \\ &\quad (q-3)(q+1)+1\}. \end{aligned}$$

Let Q_1 and Q_2 be two distinct rational places of H. Similarly the Weierstrass semigroup $W(Q_1, Q_2)$ of the pair (Q_1, Q_2) is defined as

$$W(Q_1, Q_2) = \{(\alpha_1, \alpha_2) \in \mathbb{N}_0^2 : \text{ there exists } f \in H \text{ with } (f)_\infty = \alpha_1 Q_1 + \alpha_2 Q_2\}.$$

It is important to note that $W(Q_1, Q_2)$ is also the same for all pairs (Q_1, Q_2) of distinct rational places Q_1, Q_2 of the Hermitian function field ([9]). Let α_1 be a gap number at Q_1. Let β_{α_1} be the nonnegative number defined as

$$\beta_{\alpha_1} = \min\{\alpha_2 : (\alpha_1, \alpha_2) \in W(Q_1, Q_2)\}.$$

Note that β_{α_1} is independent from the choice of distinct rational places Q_1, Q_2 as we use the Hermitian function field. It follows from [9, Theorem 3.4] that

$$\beta_{(t-j)(q+1)+j} = (q-t-1)(q+1)+j \text{ for integers } 1 \le j \le t \le q-1. \qquad (10)$$

Putting $Q_1 = P_\infty$, $Q_2 = Q$ and $t = j = (q-1)$ we obtain that

$$\beta_{(q-1)} = (q-1).$$

This means that there exists $h \in H$ such that

$$(h)_\infty = (q-1)P_\infty + (q-1)Q.$$

This completes the proof. □

3.2 Proof of Theorem 2.4

If $n < (q^2-1)$, then the lower bound in Theorem 2.4 is trivial. Hence we assume that $n \ge (q^2-1)$ without loss of generality.

Assume there exists $f(x_1, \ldots, x_m) \in \mathbb{F}_{q^2}[x_1, \ldots, x_m]$ such that the degree of f with respect to x_i is at most k for each $1 \le i \le m$, and also that

$$\begin{aligned} s_{m+1} &= f(s_1, s_2, \ldots, s_m), \\ s_{m+2} &= f(s_2, s_3, \ldots, s_{m+1}), \\ &\vdots \\ s_n &= f(s_{n-m}, s_{n-m+1}, \ldots, s_{n-1}), \end{aligned} \qquad (11)$$

where $n \geq m+1$ is an integer to be decided.

Let $1 \leq n_1 \leq n_2 \leq M$ be integers and consider the initial sequences $\mathbf{s_{n_1}}$ and $\mathbf{s_{n_2}}$ of the sequence $\mathbf{s}$ constructed in Construction 1. If $N^{(k)}(\mathbf{s_{n_2}}) = m$, then there exists $f(x_1, \ldots, x_m) \in \mathbb{F}_{q^2}[x_1, \ldots, x_m]$ satisfying (11) with $n = n_2$ and hence also with $n = n_1 \leq n_2$ automatically. This shows that

$$1 \leq n_1 \leq n_2 \leq M \Rightarrow N^{(k)}(\mathbf{s_{n_1}}) \leq N^{(k)}(\mathbf{s_{n_2}}).$$

Therefore it is enough to prove the theorem for $n = r(q^2-1)$ with $1 \leq r \leq (q-1)$. From now on we assume that $n = r(q^2-1)$ with $1 \leq r \leq (q-1)$.

Let $w \in H$ be the function

$$w = -\phi^{(-m)}(h) + f(h, \phi^{(-1)}(h), \ldots, \phi^{-(m-1)}(h)). \tag{12}$$

By definition of $\mathbf{s}$ in Construction 1, we have

$$s_{m+1} = f(s_1, s_2, \ldots, s_m) \Rightarrow h(\phi^{(m)}(P_1)) = f(h(P_1), h(\phi(P_1)), \ldots, h(\phi^{(m-1)}(P_1))).$$

Note that for any integer $i \geq 0$ and any rational place P of H, it holds that

$$h(\phi^{(i)}(P)) = \phi^{(-i)}(h(P)).$$

Therefore we get

$$\phi^{(-m)}(h)(P_1) = f(h(P_1), \phi^{(-1)}(h)(P_1), \ldots, \phi^{-(m-1)}(h)(P_1)).$$

By definition of w in (12), this is equivalent to

$$w(P_1) = 0.$$

Using also

$$s_{m+2} = f(s_2, s_3, \ldots, s_{m+1}), \cdots, s_{q^2-1} = f(s_{q^2-1-m}, s_{q^2-m}, \ldots, s_{q^2-2})$$

we obtain that

$$w(P_1) = w(\phi(P_1)) = \cdots = w(\phi^{(q^2-2-m)}(P_1)) = 0.$$

For $1 \leq i \leq r$ and $m+1 \leq j \leq q^2-1$, similarly using

$$s_{(i-1)(q^2-1)+j} = f(s_{(i-1)(q^2-1)+j-m}, s_{(i-1)(q^2-1)+j-m+1}, \ldots, s_{(i-1)(q^2-1)+j-1})$$

altogether we obtain that

$$\begin{array}{lll} w(P_1) = w(\phi(P_1)) & = \cdots & = w(\phi^{q^2-2-m}(P_1)) = 0, \\ w(P_2) = w(\phi(P_2)) & = \cdots & = w(\phi^{q^2-2-m}(P_2)) = 0, \\ \vdots \qquad\quad \vdots & & \vdots \\ w(P_r) = w(\phi(P_r)) & = \cdots & = w(\phi^{q^2-2-m}(P_r)) = 0. \end{array}$$

In particular for the zero divisor $(w)_0$ of w we have

$$\begin{aligned}(w)_0 \quad \geq \quad & (P_1 + \phi(P_1) + \cdots + \phi^{q^2-2-m}(P_1)) \\ & + (P_2 + \phi(P_2) + \cdots + \phi^{q^2-2-m}(P_2)) \\ & \qquad \vdots \\ & + (P_r + \phi(P_r) + \cdots + \phi^{q^2-2-m}(P_r))\end{aligned}$$

and hence

$$\deg(w)_0 \geq r(q^2 - 1 - m). \tag{13}$$

Recall that $f(x_1, x_2, \ldots, x_m)$ is a polynomial in $\mathbb{F}_{q^2}[x_1, x_2, \ldots, x_m]$ such that the degree of x_i in f is at most k for each $1 \leq i \leq m$. As the pole divisor of $f \in H$ is

$$(h)_\infty = (q-1)P_\infty + (q-1)Q,$$

for the pole divisor $(\phi^{(-i)}(h))_\infty$ of $\phi^{(-i)}(h) \in H$ we have

$$(\phi^{(-i)}(h))_\infty = (q-1)P_\infty + (q-1)\phi^{(i)}Q$$

for each $1 \leq i \leq m$. Therefore the pole divisor of $f(h, \phi^{-1}(h), \ldots, \phi^{-(m-1)}(h)) \in H$ satisfies that

$$\begin{aligned}&(f(h, \phi^{-1}(h), \ldots, \phi^{-(m-1)}(h)))_\infty \\ &\quad \leq km(q-1)P_\infty + k(q-1)Q + k(q-1)\phi(Q) + \cdots + k(q-1)\phi^{(m-1)}(Q).\end{aligned}$$

For the pole divisor of $\phi^{-m}(h)$, recall that we have

$$(\phi^{(-m)}(h))_\infty = (q-1)P_\infty + (q-1)\phi^{(m)}Q.$$

For the pole divisor of w, these arguments imply that

$$\begin{aligned}(w)_\infty \quad \leq \quad & km(q-1)P_\infty + k(q-1)(Q + \phi(Q) \\ & + \cdots + \phi^{(m-1)}(Q)) + (q-1)\phi^{(m)}(Q).\end{aligned}$$

In particular we have

$$\deg(w)_\infty \leq 2km(q-1) + (q-1). \tag{14}$$

Using the fact that $\deg(w)_0 = \deg(w)_\infty$ and combining (13), (14) we obtain that

$$r(q^2 - 1 - m) \leq \deg(w)_0 = \deg(w)_\infty \leq 2km(q-1) + (q-1).$$

This implies that

$$m \geq \frac{r(q^2-1) - (q-1)}{2k(q-1) + r}.$$

This completes the proof. □

3.3 Proof of Theorem 2.9

We use the same approach as in the proof of Theorem 2.4 but here we assume that $f(x_1, x_2, \ldots, x_m)$ is a polynomial in $\mathbb{F}_{q^2}[x_1, x_2, \ldots, x_m]$ of total degree at most k. Then the part of the proof after display (13) changes as follows:

Let $\ell(x_1, x_2, \ldots, x_m) = cx_1^{i_1}x_2 i_2 \cdots x_m^{i_m} \in \mathbb{F}_{q^2}[x_1, x_2, \ldots, x_m]$ be a term having a nonzero coefficient in $f(x_1, x_2, \ldots, x_m)$. We have $i_1 + i_2 + \cdots + i_m \le k$ and the pole divisor of $\ell(h, \phi^{-1}(h), \ldots, \phi^{-(m-1)}(h)) \in H$ satisfies that

$$\begin{aligned}&(\ell(h, \phi^{-1}(h), \ldots, \phi^{-(m-1)}(h)))_\infty \\ &\quad \le k(q-1)P_\infty + i_1(q-1)Q + i_2(q-1)\phi(Q) + \cdots + i_m(q-1)\phi^{(m-1)}(Q).\end{aligned}$$

Hence for the pole divisor of w we obtain

$$\begin{aligned}(w)_\infty \quad \le \quad & k(q-1)P_\infty + k(q-1)(Q + \phi(Q) \\ & + \cdots + \phi^{(m-1)}(Q)) + (q-1)\phi^{(m)}(Q).\end{aligned}$$

In particular we have

$$\deg(w)_\infty \le k(q-1) + (q-1)(km+1).$$

We again have the same lower bound on $\deg(w)_\infty = \deg(w)_0$ given in (13). We complete the proof as in the proof of Theorem 2.4. □

4 Comparison of the Bounds

In this section we compare Construction 1 in this paper with the construction corresponding to Theorem 3 and Theorem 4 in [15]. For an integer $1 \le r \le (q-1)$, Construction 1 gives a sequence $\mathbf{s}$ of length $(q-1)(q^2-1)$ with terms in $\mathbb{F}_{q^2}$ such that if $\lfloor \frac{n}{q^2-1} \rfloor = r$, then for the initial sequence $\mathbf{s_n}$ we have (see Theorem 2.4 above)

$$N^k(\mathbf{s_n}) \ge B_1(r) = \frac{r(q^2-1) - (q-1)}{r + 2k(q-1)}. \tag{15}$$

Similarly the construction corresponding to Theorem 3 in [15] gives a sequence $\mathbf{t}$ of length $(q-1)(q^2-1)$ with terms in $\mathbb{F}_{q^2}$ such that if $\lfloor \frac{n}{q^2-1} \rfloor = r$, then for the initial sequence $\mathbf{s_n}$ we have

$$N^k(\mathbf{t_n}) \ge B_2(r) = \frac{r(q^2-1) - 1}{r + q(q-1)k}. \tag{16}$$

In Figure 1 we compare $B_1(r)$ in (15) and $B_2(r)$ in (16) for $k = 5$. Moreover r runs through $1 \le r \le q-1$ with $q = 32$ in this figure. It is clear that Construction 1 gives large improvements in nonlinear complexity bounds compared to [15, Theorem 3]. Note that $\lceil B_1(r) \rceil$ is also much larger than $\lceil B_2(r) \rceil$

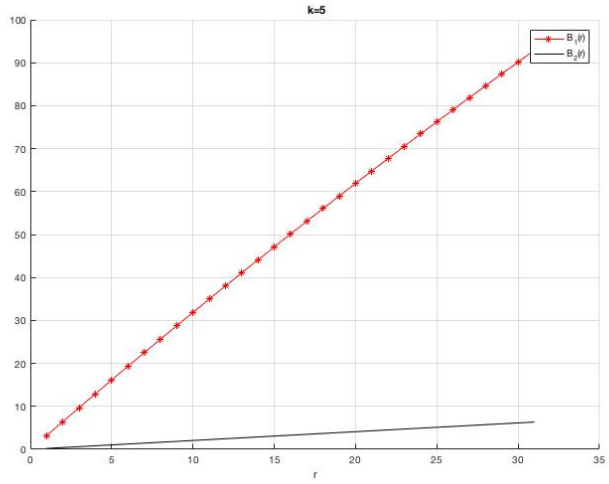

Figure 1:

as observed in Figure 1. Hence Corollary 2.6 is also much better than the direct improvement of [15, Theorem 3] given in Remark 2.7 above.

Similarly by Theorem 2.9 we have

$$L^k(\mathbf{s_n}) \geq C_1(r) = \frac{r(q^2-1)-(k+1)(q-1)}{r+k(q-1)}, \tag{17}$$

and Theorem 4 in [15] gives

$$L^k(\mathbf{t_n}) \geq C_2(r) = \frac{r(q^2-1)-(q^2-q-1)k-1}{r+k}. \tag{18}$$

In Figure 2 we compare $C_1(r)$ in (17) and $C_2(r)$ in (18) for $k = 20$. Again r runs through $1 \leq r \leq q-1$ with $q = 32$ in this figure. It is clear that Construction 1 gives improvements in nonlinear complexity bounds compared to [15, Theorem 4] for relatively large k or small n. Note that, again for relative large k or small n, $\lceil C_1(r) \rceil$ gives the same improvements compared to $\lceil C_2(r) \rceil$ as observed in Figure 2. Hence Corollary 2.13 is also an improvement of [15, Theorem 4] given in Remark 2.14 above.

acknowledgements

The authors are grateful to Department of Mathematical Sciences, Aalborg University for supporting a one month visiting professor position for the second listed author.

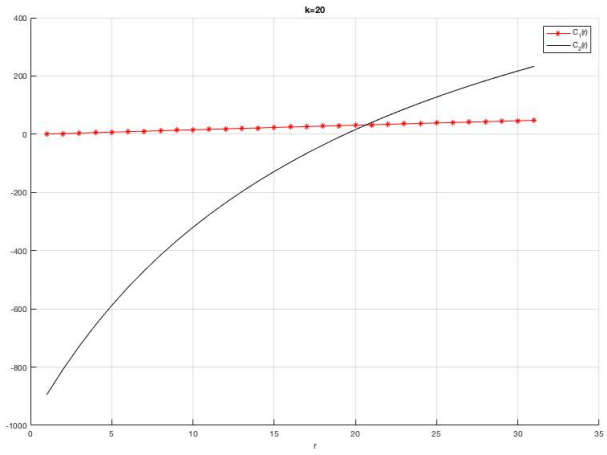

Figure 2:

References

[1] C. Carvallo and T. Kato, *On Weierstrass semigroups and sets: review of new results*, Geom. Dedicate, 239: 195–210, 2009.

[2] C. Carvallo and F. Torres, *On Goppa codes and Weierstrass points at several points*, Des. Codes. Cryptogr., 35: 211–225, 2005.

[3] C. Castellanos and G. Tizziotti, *On Weierstrass semigroup at m points on curves of the form* $f(y) = g(x)$, J. Pure Appl. Algebra, 222: 1803–1809, 2018.

[4] C. Ding, G. Xiao and W. Shan, "The stability theory of stream ciphers", *Lecture Notes in Computer Science, 561. Springer-Verlag, Berlin*, x+187 pp. ISBN: 3-540-54973-0, 1991.

[5] A. Garcia, S. J. Kim and R. F. Lax, *Consecutive Weierstrass gaps and minimum distance of Goppa codes*, J. Pure Appl. Algebra 84(2):199–207, 1993.

[6] A. Garcia, H. Stichtenoth and C.-P. Xing, *On subfields of the Hermitian function field*, Compositio Math. 120(2):137–170, 2000.

[7] V. D. Goppa, *Codes associated with divisors*, Prob. Pereda. Inf, 13: 33–39, 1977.

[8] V. D. Goppa, *Codes on algebraic curves*, Sov. Math. Dokl. 24:75–91. 1981.

[9] G. L. Matthews, *Weierstrass semigroups and codes from a quotient of the Hermitian curve*, Des. Codes Cryptogr. 37(3):473–492, 2005.

[10] W. Meidl and A. Winterhof "Linear complexity of sequences and multisequences", *In Handbook of Finite Fields, Chapman and Hall/CRC*, 1068 pp. ISBN: 9781439873786, 2013.

[11] H. Niederreiter, "Random number generation and quasi-Monte Carlo methods", *CBMS-NSF Regional Conference Series in Applied Mathematics, 63. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA*, vi+241 pp. ISBN: 0-89871-295-5, 1992.

[12] W. Meidl, and H. Niederreiter, *Multisequences with high joint nonlinear complexity*, Des. Codes Cryptogr., 81(2):337–346, 2016.

[13] H. Niederreiter and C. Xing, "Rational Points on Curves over Finite Fields", *Cambridge Univ. Press, Cambridge*, x+245 pp. ISBN: 0-521-66543-4, 2001.

[14] H. Niederreiter and C. Xing, "Algebraic geometry in coding theory and cryptography", *Cambridge Univ. Press, Princeton University Press, Princeton, NJ*, xii+260 pp. ISBN: 978-0-691-10288-7, 2009.

[15] H. Niederreiter and C. Xing, *Sequences with high nonlinear complexity*, IEEE Trans. Inform. Theory, 60(10):6696–6701, 2014.

[16] R. A. Rueppel, "Stream ciphers", *Contemporary cryptology, IEEE, New York*, 65–134, 1992.

[17] H. Stichtenoth, "Algebraic function fields and codes", *Second edition. Graduate Texts in Mathematics, 254. Springer-Verlag, Berlin*, xiv+355 pp. ISBN: 978-3-540-76877-7, 2009.

[18] S. Yang and C. Hu, *Pure Weierstrass gaps from a quotient of the Hermitian curve*, Finite Fields Appl. 50: 251–271. 2018.