On the constant $D(_q)$ defined by Homma

Beelen, Pieter Hendrik Turdus; Montanucci, Maria; Vicino, Lara

Published in:
Arithmetic, Geometry, Cryptography, and Coding Theory 2021

Publication date:
2022

Document Version
Peer reviewed version

On the constant $D(q)$ defined by Homma

Peter Beelen, Maria Montanucci, and Lara Vicino

Abstract. Let $\mathcal{X}$ be a projective, irreducible, nonsingular algebraic curve over the finite field $\mathbb{F}_q$ with q elements and let $|\mathcal{X}(\mathbb{F}_q)|$ and $g(\mathcal{X})$ be its number of rational points and genus respectively. The Ihara constant $A(q)$ has been intensively studied during the last decades, and it is defined as the limit superior of $|\mathcal{X}(\mathbb{F}_q)|/g(\mathcal{X})$ as the genus of $\mathcal{X}$ goes to infinity. In 2012 Homma defined an analogue $D(q)$ of $A(q)$, where the nonsingularity of $\mathcal{X}$ is dropped and $g(\mathcal{X})$ is replaced with the degree of $\mathcal{X}$. We will call $D(q)$ Homma's constant. In this paper, upper and lower bounds for the value of $D(q)$ are found.

1. Introduction

Let p be a prime and let $q = p^e$ be a prime power. Let $\mathcal{X}$ be a projective, nonsingular, geometrically irreducible curve of genus g. The interaction between the genus g of $\mathcal{X}$ and the number $|\mathcal{X}(\mathbb{F}_q)|$ of its rational points has been subject of intense studies during the last years. It is well known that the Weil bound

$$|\mathcal{X}(\mathbb{F}_q)| \leq q + 1 + 2g\sqrt{q}$$

is not sharp if g is large compared to q. Put

$$N_q(g) := \max |\mathcal{X}(\mathbb{F}_q)|, \tag{1.1}$$

where the maximum is taken over all curves $\mathcal{X}/\mathbb{F}_q$ with genus g. The *Ihara constant* is defined by

$$A(q) := \limsup_{g\to\infty} \frac{N_q(g)}{g}. \tag{1.2}$$

This is a measure of the asymptotic behaviour of the number of rational points on curves over $\mathbb{F}_q$ when the genus becomes large. Ihara's constant $A(q)$ has been intensively studied during the last decades. For any q, we have $A(q) \leq \sqrt{q} - 1$ (see [**4**]), and if q is a square we have (see [**13**, **21**]) $A(q) = \sqrt{q} - 1$.

For any q, using class field theory, Serre [**17**] showed that $A(q) > c\log(q)$ for some constant $c > 0$ independent of q. In particular $A(q) > 0$ for all q. For $q = p^{2m+1}$, with $m > 0$, the currently best-known lower bound is $A(q) \geq 2(1/(p^m - 1) + 1/(p^{m+1} - 1))^{-1}$, see [**2**]. The exact value of $A(q)$ is however unknown when q is not a square.

1991 *Mathematics Subject Classification.* Primary 14G15, 14H50; Secondary 11G20, 14H25.

Key words and phrases. Algebraic curve, rational point, finite field.

The first and second authors were supported by The Danish Council for Independent Research (DFF-FNU), project *Correcting on a Curve*, Grant No. 8021-00030B.

If the curve $\mathcal{X}$ is seen as a projective curve $\mathcal{X} \subseteq \mathbb{P}^n(\mathbb{F}_q)$ of degree $d > 0$ and it is not necessarily required to be nonsingular, a different question can be addressed: how large can $|\mathcal{X}(\mathbb{F}_q)|$ be with respect to d?

In a series of papers [**10**–**12**] it has been shown that if $\mathcal{X}$ is a (possibly reducible) plane curve without $\mathbb{F}_q$-linear components, then

$$|\mathcal{X}(\mathbb{F}_q)| \leq (d-1)q + 1, \tag{1.3}$$

except for curves isomorphic over $\mathbb{F}_4$ to the curve defined by

$$\mathcal{K} : (X+Y+Z)^4 + (XY+YZ+ZX)^2 + XYZ(X+Y+Z) = 0,$$

which satisfies $|\mathcal{K}(\mathbb{F}_4)| = 14$. The bound (1.3) was originally conjectured by Sziklai [**19**], and he found that some curves actually achieve this bound.

The natural question on whether the bound (1.3) is valid for curves in higher dimensional projective space $n \geq 3$ was analyzed by Homma in [**9**]. There, it is obtained that (1.3) is also true when $n \geq 3$ and $\mathcal{X}$ has no $\mathbb{F}_q$-linear components, unless $d = q = 4$ and $\mathcal{X}$ is $\mathbb{F}_q$-isomorphic to the plane curve $\mathcal{K}$.

In the same paper [**9**], an analogue of Ihara constant $A(q)$ (1.2) is given when replacing the genus g with the degree d. First, we replace $N_q(g)$ as defined in (1.1), with $M_q(d) := \max |\mathcal{X}(\mathbb{F}_q)|$ where this time the maximum is taken over all irreducible curves of a fixed degree d in a projective space of some dimension over $\mathbb{F}_q$. Here the dimension is not fixed and therefore allowed to be arbitrarily large. Then the analogue of $A(q)$ is defined as

$$D(q) := \limsup_{d\to\infty} \frac{M_q(d)}{d}, \tag{1.4}$$

which measures the asymptotic behavior of the number of rational points of projective curves over $\mathbb{F}_q$ when d becomes large. In [**9**] it was observed that since the bound (1.3) is valid for curves in any projective space $\mathbb{P}^n(\mathbb{F}_q)$, $n \geq 2$, with the exception already mentioned above, one may conclude that $D(q) \leq q$. In the same paper also the lower bound $D(q) \geq A(q)/2$ was derived, but the exact value of $D(q)$ remains unknown for all q.

In this paper, new upper and lower bounds for the value of $D(q)$, which we from now on will call Homma's constant, are found by a refinement of Homma's methods and by using towers of algebraic function fields. Our main results are summarized in the following theorem.

THEOREM 1.5. *Let $q = p^e$ be a prime power and let $D(q)$ be Homma's constant as defined in* (1.4). *Then*

1. $D(q) \leq q - 1$,
2. $D(q) \geq 1$ *provided that* $q > 2$,
3. $D(q^2) \geq \frac{q}{q+1} A(q^2) = \frac{q^2-q}{q+1}$.

Note that the lower bound $D(q) \geq 1$ is interesting for small values of q only, since otherwise Homma's lower bound $D(q) \geq A(q)/2$ is better. The values $q \leq 31$ for which the lower bound $D(q) \geq 1$ is currently the best known are listed in Remark 4.6.

The paper is organized as follows. We start by slightly improving Homma's upper bound on $D(q)$ in Section 2 by refining his argument, thus proving Item 1 of Theorem 1.5. Next we prove Item 2 of Theorem 1.5 in Section 3 by explicitly constructing a sequence of curves whose degrees are close to their number of rational

points. Finally, the main part of the paper is devoted to proving Item 3 of Theorem 1.5 in the final section.

2. An upper bound for $D(q)$: the proof of Item 1 in Theorem 1.5

The upper bound $D(q) \leq q$ obtained by Homma in [**9**, Proposition 5.4] was deduced from the bound (1.3), but in the same paper the following theorem was given.

THEOREM 2.1 ([**9**, Theorem 3.2]). *Let $\mathcal{X}$ be a nondegenerate irreducible curve of degree d in $\mathbb{P}^n(\mathbb{F}_q)$. Then*

$$|\mathcal{X}(\mathbb{F}_q)| \leq \frac{(q-1)(q^{n+1}-1)}{q(q^n-1)-n(q-1)}d. \tag{2.2}$$

Here the word *nondegenerate* means that $\mathcal{X}$ is not contained in any hyperplane of $\mathbb{P}^n(\mathbb{F}_q)$. At this point, using this result, we are ready to prove Item 1 in Theorem 1.5.

Indeed for a fixed value of q, considering equation (2.2) and dividing both sides by d gives

$$\frac{|\mathcal{X}(\mathbb{F}_q)|}{d} \leq \frac{(q-1)(q^{n+1}-1)}{q(q^n-1)-n(q-1)} = \frac{(q-1)\dfrac{(q^{n+1}-1)}{q^{n+1}}}{\dfrac{q(q^n-1)}{q^{n+1}} - \dfrac{n(q-1)}{q^{n+1}}}. \tag{2.3}$$

This observation can be used to improve the upper bound for $D(q)$. Note that by taking the $\limsup_{d\to\infty} M_q(d)/d$ as in (1.4), we are by definition of $D(q)$ considering curves of increasing degree. However, the dimension of the projective spaces containing the curves will be increasing as d increases. Indeed, if for a family of curves $(\mathcal{X}_i)_{i\geq 0}$, with degrees d_i tending to infinity as i tends to infinity, there exist an n such that for all i, $\mathcal{X}_i \subseteq \mathbb{P}^n$, then $|\mathcal{X}_i(\mathbb{F}_q)| \leq |\mathbb{P}^n(\mathbb{F}_q)| = (q^{n+1}-1)/(q-1)$, implying that $|\mathcal{X}_i(\mathbb{F}_q)|/d_i$ tends to zero as i tends to infinity.

Now let $(\mathcal{X}_i)_{i\geq 0}$, be a family of curves with degrees d_i tending to infinity such that $\limsup_{i\to\infty} |\mathcal{X}_i(\mathbb{F}_q)|/d_i > 0$. Further assume for each i that $\mathcal{X}_i$ is a nondegenerate curve contained in $\mathbb{P}^{n_i}$. We have seen that n_i tends to infinity as i tends to infinity. But then we obtain from equation (2.3):

$$D(q) \leq \lim_{i\to\infty} \frac{(q-1)\dfrac{(q^{n_i+1}-1)}{q^{n_i+1}}}{\dfrac{q(q^{n_i}-1)}{q^{n_i+1}} - \dfrac{n_i(q-1)}{q^{n_i+1}}} = q-1.$$

This proves Item 1 of Theorem 1.5.

3. A lower bound for $D(q)$: the proof of Item 2 in Theorem 1.5

For a prime power $q = p^e$ strictly larger than two, consider the tower of function fields $\mathcal{T} = (T_m)_{m\geq 1}$ over $\mathbb{F}_q$ defined recursively as

$$T_1 = \mathbb{F}_q(x_1) \qquad \text{and} \qquad T_{i+1} = T_i(x_{i+1}) \qquad \text{with} \qquad x_{i+1}^{q-1} = -1 + (x_i+1)^{q-1}.$$

The tower $\mathcal{T}$ is similar to an asymptotically good tower considered in [**18**, Proposition 7.3.3], but the variation we consider is actually not asymptotically good. It is not hard to see that the place of T_1 corresponding to the zero of x_1 is totally ramified

in the tower. In particular, the equation $x_{i+1}^{q-1} = -1 + (x_i + 1)^{q-1}$ is absolutely irreducible when viewed as a polynomial in $T_i[x_{i+1}]$. This implies in particular that the ideal $I_\ell := \langle x_2^{q-1} + 1 - (x_1+1)^{q-1}, \ldots, x_\ell^{q-1} + 1 - (x_{\ell-1}+1)^{q-1} \rangle \subseteq \mathbb{F}_q[x_1, \ldots, x_\ell]$ is a prime ideal. Since we want to deal with projective curves, the following proposition is essential.

PROPOSITION 3.1. *Let $\ell > 1$ be an integer and define $I'_\ell := \langle x_2^{q-1} + z^{q-1} - (x_1 + z)^{q-1}, \ldots, x_\ell^{q-1} + z^{q-1} - (x_{\ell-1} + z)^{q-1} \rangle \subseteq \mathbb{F}_q[x_1, \ldots, x_\ell, z]$. Then I'_ℓ is a homogeneous prime ideal and the homogenization of the prime ideal $I_\ell := \langle x_2^{q-1} + 1 - (x_1 + 1)^{q-1}, \ldots, x_\ell^{q-1} + 1 - (x_{\ell-1} + 1)^{q-1} \rangle \subseteq \mathbb{F}_q[x_1, \ldots, x_\ell]$.*

PROOF. For convenience, let us write $g_i := x_{i+1}^{q-1} + 1 - (x_i + 1)^{q-1}$ and $g'_i := x_{i+1}^{q-1} + z^{q-1} - (x_i + z)^{q-1}$. We have already seen that the ideal I_ℓ is a prime ideal. Now let $>_{\text{deglex}}$ denote the degree-lexicographic ordering with $x_\ell >_{\text{deglex}} \ldots >_{\text{deglex}} x_1$ as a monomial order in $\mathbb{F}_q[x_1, \ldots, x_\ell]$. Since under this monomial ordering the leading terms of the g_i are co-prime, the set $\{g_1, \ldots, g_{\ell-1}\}$ is a Gröbner basis of I_ℓ. Then from [**3**, § 8.4, Theorem 4] $\{g'_1, \ldots, g'_{\ell-1}\}$ is a Gröbner basis for the homogenization of I_ℓ. Hence I'_ℓ is the homogenization of the prime ideal I_ℓ and in particular I'_ℓ is a homogeneous prime ideal. □

Now consider the projective curve $\mathcal{X}_\ell \subset \mathbb{P}^\ell$ defined over $\mathbb{F}_q$ given by the homogeneous equations

$$x_{i+1}^{q-1} = -z^{q-1} + (x_i + z)^{q-1} \quad \text{for } i = 1, \ldots, \ell - 1. \tag{3.2}$$

Proposition 3.1 implies that $\mathcal{X}_\ell \subset \mathbb{P}^\ell$ is indeed an irreducible projective curve. It actually implies that $\mathcal{X}_\ell$ is a complete intersection, which in turn implies that $\deg(\mathcal{X}_\ell) = \deg(g'_1) \cdots \deg(g'_{\ell-1}) = (q-1)^{\ell-1}$.

Now we consider the number of $\mathbb{F}_q$-rational points on $\mathcal{X}_\ell$. To estimate this number, we consider the number of projective points $[x_1 : x_2 : \cdots : x_\ell : 0]$ satisfying equation (3.2). Substituting $z = 0$ in equation (3.2), we obtain that

$$x_{i+1}^{q-1} = x_i^{q-1} \quad \text{for } i = 1, \ldots, \ell - 1.$$

Choosing $x_1 = 1$, we see that any solution is defined over $\mathbb{F}_q$ and that there are exactly $(q-1)^{\ell-1}$ points at the infinity on $\mathcal{X}_\ell$. In particular, $|\mathcal{X}_\ell(\mathbb{F}_q)| \geq (q-1)^{\ell-1}$. Hence

$$D(q) \geq \limsup_{\ell \to \infty} \frac{|\mathcal{X}_\ell(\mathbb{F}_q)|}{\deg(\mathcal{X}_\ell)} \geq \frac{(q-1)^{\ell-1}}{(q-1)^{\ell-1}} = 1.$$

This completes the proof of Item 2 of Theorem 1.5.

4. A lower bound for $D(q^2)$: the proof of Item 3 in Theorem 1.5

In order to prove Item 3 in Theorem 1.5 we use a tower of function fields over $\mathbb{F}_{q^2}$ constructed recursively by Garcia and Stichtenoth in [**6**] as follows:

$$F_1 = \mathbb{F}_{q^2}(x_1) \qquad \text{and} \qquad F_{i+1} = F_i(x_{i+1}) \qquad \text{with} \qquad x_{i+1}^q + x_{i+1} = \frac{x_i^q}{x_i^{q-1} + 1}.$$

This tower is optimal in the sense that if $N_1(F_i)$ denotes the number of rational places and $g(F_i)$ the genus of F_i, then $\lim_{m \to \infty} N_1(F_m)/g(F_m) = q - 1 = A(q^2)$.

Indeed, any zero of the function $x_1 - \alpha$ in F_1 for $\alpha \in \mathbb{F}_{q^2} \setminus \{\alpha \mid \alpha^q + \alpha = 0\}$ splits completely in the extension F_m/F_1, implying that $N_1(F_m) \geq (q-1)q^m$. Moreover,

in [**6**, Remark 3.8], the genus $g(F_m)$ of F_m is computed for all $m \geq 1$. It is given by

$$g(F_m) = \begin{cases} (q^{m/2}-1)^2 & \text{if} \quad m \equiv 0 \pmod 2, \\ (q^{\frac{m+1}{2}}-1)(q^{\frac{m-1}{2}}-1) & \text{if} \quad m \equiv 1 \pmod 2. \end{cases}$$

Hence optimality of the tower follows. For computing the genus $g(F_m)$, it is proven that the pole P_∞ of $x_1 \in F_1$ is totally ramified in all extensions F_m/F_1, $m \geq 2$, see also [**15**, Proposition 1.1]. We denote by $P_\infty^{(m)}$ the unique extension of P_∞ in F_m. Note that $P_\infty^{(m)}$ is a rational place, since P_∞ is totally ramified in F_m/F_1.

Even though it is in general a difficult challenge to compute the Weierstrass semigroups at places in a tower, Pellikaan, Stichtenoth, and Torres [**15**] computed the Weierstrass semigroup at $P_\infty^{(m)}$ for all $m \geq 1$. The nice property proven by the authors in [**15**] is that the semigroups at $P_\infty^{(m)}$ can be computed from the one at $P_\infty^{(m-1)}$, following a recursive procedure. Indeed from [**15**, Theorem 3.1]

$$H(P_\infty^{(m)}) = \begin{cases} \mathbb{Z}_{\geq 0} & \text{if} \quad m = 1 \\ qH(P_\infty^{(m-1)}) \cup \mathbb{Z}_{\geq c_m} & \text{if} \quad m > 1 \end{cases} \tag{4.1}$$

where $c_m := q^m - q^{\lceil \frac{m}{2} \rceil}$ is the conductor of $H(P_\infty^{(m)})$.

Let $\{\gamma_1, \ldots, \gamma_\ell\}$ be a set of generators of $H(P_\infty^{(m)})$, so that

$$H(P_\infty^{(m)}) = \langle \gamma_1, \ldots, \gamma_\ell \rangle,$$

and $0 < \gamma_1 < \cdots < \gamma_\ell$. Note that equation (4.1) implies that $\gamma_1 = q^{m-1}$, being the smallest positive element of $H(P_\infty^{(m)})$. This implies that $H(P_\infty^{(m)}) \cap \mathbb{Z}_{<c_m+q^{m-1}}$ is a generating set and that therefore we may assume that

$$\gamma_\ell \leq c_m + q^{m-1} - 1. \tag{4.2}$$

By definition of the Weierstrass semigroup $H(P_\infty^{(m)})$, there exist functions $f_1, \ldots, f_\ell \in F_m$ such that

$$(f_i)_\infty = \gamma_i P_\infty^{(m)}, \ i = 1, \ldots, \ell.$$

In [**16**], the functions $f_1, \ldots, f_\ell$ are used to define a birational morphism between a nonsingular projective curve $\mathcal{X}$ and a curve $\mathcal{X}'$, with only one point at infinity. Since we use the language of function fields, we need to reformulate the results from [**16**] slightly. Intuitively, we simply use the functions $f_1, \ldots, f_n$ to define a map from the set of places of F_m to an algebraic curve $\mathcal{X}_m$. However, this map, which we denote by φ_m, is easiest to describe when first extending the constant field of F_m to $\overline{\mathbb{F}}_q$, the algebraic closure of $\mathbb{F}_q$, since then all places are rational:

$$\varphi_m : \mathbb{P}(\overline{\mathbb{F}}_q F_m) \longrightarrow \mathbb{P}^\ell$$

defined by

$$\begin{array}{lcll} \varphi_m(Q) & = & [1 : f_1(Q) : \cdots : f_\ell(Q)], & \text{if} \ \ Q \neq P_\infty^{(m)}, \\ \varphi_m(Q) & = & [0 : \cdots : 0 : 1], & \text{otherwise.} \end{array}$$

Note that [**7**, Theorem 4.2.2] implies that indeed the image of the map φ_m is a projective curve $\mathcal{X}_m$. Since $f_1, \ldots, f_\ell$ are defined over $\mathbb{F}_{q^2}$, so is $\mathcal{X}_m$. Therefore we will from now on consider the curve $\mathcal{X}_m$ as a curve defined over $\mathbb{F}_{q^2}$. Moreover, [**16**, Theorem 15] states among other things that the function field of $\mathcal{X}_m$, when considered over the field $\mathbb{F}_{q^2}$, is exactly F_m, that apart from possibly $\varphi_m(P_\infty^{(m)})$,

the curve has no singularities and that $P_\infty^{(m)}$ is the only place of F_m centered at $\varphi_m(P_\infty^{(m)})$. In particular φ_m induces a bijection between $\mathbb{P}(\overline{\mathbb{F}}_q F_m) \setminus \{P_\infty^{(m)}\}$ and $\mathcal{X}_m \setminus \{\varphi_m(P_\infty^{(m)})\}$.

REMARK 4.3. The curve $\mathcal{X}_m$ is a non-degenerate curve in $\mathbb{P}^\ell$. Indeed if this was not the case, then there would exist a combination $a_1 + a_2 f_1 + \cdots + a_{\ell+1} f_\ell$, for some $a_i \in \overline{\mathbb{F}}_q$ not all equal to zero, such that $a_1 + a_2 f_1 + \cdots + a_{\ell+1} f_\ell \equiv 0$, which is impossible by the linear independence of $\{1, f_1, \ldots, f_\ell\}$ over $\overline{\mathbb{F}}_q$ given by [**18**, Proposition 3.6.1].

Now we investigate the degree and number of $\mathbb{F}_{q^2}$-rational points on $\mathcal{X}_m$. The number of rational points is easy to bound, since the rational places of F_m are in bijection with the points on $\mathcal{X}_m$ defined over $\mathbb{F}_{q^2}$. Indeed, the place $P_\infty^{(m)}$ corresponds to the projective point $[0 : \cdots : 0 : 1]$, while the remaining rational points of $\mathcal{X}_m$ are non-singular and hence each corresponds to a unique rational place of F_m. This shows that

$$|\mathcal{X}_m(\mathbb{F}_{q^2})| = N_1(F_m) \geq (q-1)q^m. \tag{4.4}$$

The inequality $N_1(F_m) \geq (q-1)q^m$ was already mentioned before.

At this point we need to derive some information on the degree $\deg(\mathcal{X}_m)$ of the curve $\mathcal{X}_m$. The following inequality holds:

$$\deg(\mathcal{X}_m) \leq \gamma_\ell \leq c_m + q^{m-1} - 1. \tag{4.5}$$

This can be proven as follows. First of all, the last inequality is simply equation (4.2). Now recall that the degree can also be seen as the the maximum number of intersection points with a hyperplane. The points of intersection of the curve $\mathcal{X}_m$ and a hyperplane of equation $a_0x_0+\cdots+a_\ell x_\ell = 0$ in $\mathbb{P}^\ell$ correspond, by the definition of φ_m, to the places that are zeros of the function $\sum_{i=0}^{\ell} a_i f_i \in \mathscr{L}(\gamma_\ell \bar{P}_\infty^{(m)})$. Here $\mathscr{L}(\gamma_\ell \bar{P}_\infty^{(m)})$ denotes the Riemann–Roch space of the divisor $\gamma_\ell \bar{P}_\infty^{(m)}$. Since the pole divisor of $\sum_{i=0}^{\ell} a_i f_i$ has degree at most γ_ℓ the same is true for its zero divisor. Hence the number of intersection points is at most γ_ℓ.

Now combining equations (4.4) and (4.5), we obtain:

$$D(q^2) \geq \limsup_{m\to\infty} \frac{|\mathcal{X}_m(\mathbb{F}_{q^2})|}{\deg(\mathcal{X}_m)} \geq \limsup_{m\to\infty} \frac{(q-1)q^m}{c_m + q^{m-1} - 1} = \frac{q^2-q}{q+1}.$$

Since $A(q^2) = q-1$, Item 3 of Theorem 1.5 follows.

REMARK 4.6. Thereom 1.5 (3) improves Homma's lower bound $D(q^2) \geq A(q^2)/2$ for any values of q. The bound $D(q) \geq 1$ is instead interesting for small values of $q > 2$, since then Homma's lower bound $D(q) \geq A(q)/2$ is weaker. The following table provides for those small values of q the best known lower bound for $A(q)/2$. For all other values of q, except possibly when q is a prime, $A(q) \geq 2$.

q	$A(q)/2 \geq$	reference
3	0.2464	[**5**]
4	0.5	[**13**, **21**]
5	0.3636	[**1**, **20**]
7	0.4615	[**8**]
8	0.75	[**22**]
11	0.5714	[**8**]
13	0.6	[**14**]
17	0.8	[**14**]
19	0.8	[**8**]
23	0.9230	[**8**]
29	0.9523	[**8**]
31	0.9523	[**8**]

References

[1] C. Angels and C. Marie, *A note on tamely ramified towers of global function fields*, Finite Fields Appl. **8** (2002), 207–215.

[2] A. Bassa, P. Beelen, A. Garcia, and H. Stichtenoth, *Towers of function fields over non-prime finite fields*, Mosc. Math. J. **15** (2015), no. 1, 1–29.

[3] D. Cox, J. Little, and D. O'Shea, *Ideals, Varieties, and Algorithms An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Undergraduate Text in Math, Springer-Verlag (1991).

[4] V. G. Drinfeld and S. G. Vlăduţ, *The number of points of an algebraic curve*, Funktsional. Anal. i Prilozhen. **17** (1983), 68–69.

[5] I. Duursma and K. H. Mak, *On lower bounds for tha constants $A(2)$ and $A(3)$*, Composition math. **149** (2013), 1108–1128.

[6] A. Garcia and H. Stichtenoth, *On the asymptotic behaviour of some towers of function fields over finite fields*, Journal of number theory **61** (1996), no. 2, 248–273.

[7] D. Goldschmidt, *Algebraic functions and projective curves*, Vol. 215, Springer Science & Business Media, 2006.

[8] L. L. Hall-Seelig, *New lower bounds for the Ihara function $A(q)$ for small primes*, J. Number Theory **133** (2013), 3319–3324.

[9] M. Homma, *A bound on the number of points of a curve in a projective space over a finite field*, Theory and applications of finite fields, 2012, pp. 103–110.

[10] M. Homma and S. J Kim, *Around Sziklais conjecture on the number of points of a plane curve over a finite field*, Finite Fields Appl. **15** (2009), 468–474.

[11] ———, *Sziklais conjecture on the number of points of a plane curve over a finite field II*, in: G. McGuire, G.L. Mullen, D. Panario, I.E. Shparlinski (Eds.), Finite Fields: Theory and Applications, in: Contemp. Math. **518** (2010), 225–234.

[12] ———, *Sziklais conjecture on the number of points of a plane curve over a finite field III*, Finite Fields Appl. **16** (2010), 315–319.

[13] Y. Ihara, *Some remarks on the number of rational points of algebraic curves over finite fields*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28** (1981), 721–724.

[14] W. C. W. Li and H. Maharaj, *Coverings of curves with asymptotically many rational points*, J. Number Theory **96** (2002), 232–256.

[15] R. Pellikaan, H. Stichtenoth, and F. Torres, *Weierstrass semigroups in an asymptotically good tower of function fields*, Finite fields and their applications **4** (1998), 381–392.

[16] K. Saints and C. Heegard, *Algebraic-geometric codes and multidimensional cyclic codes: a unified theory and algorithms for decoding using Gröbner bases*, IEEE Trans. Inform. Theory **41** (1995), no. 6, part 1, 1733–1751.

[17] J.-P. Serre, *Sur le nombre des points rationnels dune courbe algbrique sur un corps fini*, C.R. Acad. Sci. Paris Sr. I Math. **296** (1983), 397–402.

[18] H. Stichtenoth, *Algebraic function fields and codes*, Vol. 254, Springer Science & Business Media, 2009.

[19] P. Sziklai, *A bound on the number of points of a plane curve*, Finite Fields Appl. **14** (2008), 41–43.
[20] A. Temkine, *Hilbert class field towers of function fields over finte fields and lower bounds for* $A(q)$, J. Number Theory **87** (2001), 189–210.
[21] M. A. Tsfasman, S. G. Vlăduţ, and T. Zink, *Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound*, Math. Nachr. **109** (1982), 21–28.
[22] T. Zink, *Degeneration of Shimura surfaces and a problem in coding theory*, Lect. Notes in Comput. Sci. **199** (1985), 503–511.

Department of Applied Mathematics and Computer Science, Technical University of Denmark, Kongens Lyngby 2800, Denmark
E-mail address: pabe@dtu.dk

Department of Applied Mathematics and Computer Science, Technical University of Denmark, Kongens Lyngby 2800, Denmark
E-mail address: marimo@dtu.dk

Department of Applied Mathematics and Computer Science, Technical University of Denmark, Kongens Lyngby 2800, Denmark
E-mail address: lavi@dtu.dk