HSJG
Hagia Sophia Journal of Geometry
e-ISSN 2687-4261
Vol. 4, No. 1, 17-19, 2022
Research Article

Embedded Projective Curves over a Finite Field and Homma Constant $D(q)$

Edoardo BALLICO

Abstract
We consider the existence of smooth projective curves embedded over a fixed finite field $\mathbb{F}_q$ and such that their ratio $\#X(\mathbb{F}_q)/\deg(X)$ is large. We discuss the geometry of curves computing the Iihara constants $A(q)$ and $A^-(q)$ and relate it to upper and lower bound of the Homma constants $D(q)$ and $D^-(q)$.

Keywords and 2020 Mathematics Subject Classification
Keywords: Finite field — curve over a finite field— curves in projective spaces
MSC: 14H50, 14N05, 12E20

University of Trento, Dept. of Mathematics, via Sommarive 14, 38123 Trento (TN), Italy
✉edoardo.ballico@unitn.it
Corresponding author: Edoardo BALLICO
Article History: Received 8 February 2022; Accepted 6 May 2022

1. Introduction

Fix a prime power q. We recall the definition of the Iihara's constant $A(q)$. For any $g \in \mathbb{N}$ let $N_q(g)$ be the maximum of all $\#X(\mathbb{F}_q)$, where X is a smooth curve of genus g. Set

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

It is known that $0 < A(q) \leq \sqrt{q}-1$, that there is $c > 0$ such that $A(q) > c\log q$ and that $A(q) = \sqrt{q}-1$ if q is a square ([1–5]). The books just quoted contain references for explicit examples of curves with high $\#X(\mathbb{F}_q)/g(X)$ and an effective way to get lower bounds for $A(q)$ is the use of towers of curves. We propose the study of embeddings in projective spaces over $\mathbb{F}_q$ of curves X with a very large ratio $\#X(\mathbb{F}_q)/g(X)$ to relate $A(q)$ and $A^-(q)$ to the Homma constants $D(q)$ and $D^-(q)$ which we will describe in the second part of the introduction.

Let X be a smooth and geometrically connected curve defined over $\mathbb{F}_q$. The *q-embedding degree* $\mathrm{embdeg}(X)_q$ of X is the minimal degree of an embedding f of X into some projective space with f defined over $\mathbb{F}_q$. The *q-injective degree* $\mathrm{injdeg}(X)_q$ is the minimal degree of a morphism f of X into some projective space defined over $\mathbb{F}_q$ such that $f_{|X(\mathbb{F}_q)}$ is injective, with the convention $\mathrm{injdeg}(X)_q = 0$ if $X(\mathbb{F}_q) = \emptyset$. The *q-gonality* $\mathrm{gon}(X)_q$ is the minimal degree of a morphism $f : X \to \mathbb{P}^1$ defined over $\mathbb{F}_q$.

Theorem 1. *Fix $g_0 \in \mathbb{N}$ and real numbers $\varepsilon > 0$, $0 < c < 2$. Then there is an integer $g \geq g_0$ and a smooth genus g curve X defined over $\mathbb{F}_q$ such that $A(q)-\varepsilon \leq \#X(\mathbb{F}_q)/g \leq A(q)+\varepsilon$ such that at least one of the following conditions is satisfied:*

i. $\mathrm{emdeg}(X)_q \geq cg$ *and* $\#X(\mathbb{F}_q)/\mathrm{embdeg}(X)_q \leq (A(q)+\varepsilon)/c$*;*

ii. $\mathrm{gon}(X)_q \leq cg$ *and* $A(q)-\varepsilon \leq c(q+1)$.

Note that if $c < (A(q)-\varepsilon)/(q+1)$, then case ii. of Theorem 1 cannot occur and hence i. holds. However, in this case the upper bound in i. is not interesting ([6, Proposition 5.4], [7, part (1) of Theorem 1.5])). If $c \sim \frac{1}{\sqrt{q}}$ the upper bound in i. is not interesting for q a square, because $A(q) = \sqrt{q}-1$ in this case, but it may still be non-trivial for q not a square.

Theorem 2. *Fix $g_0 \in \mathbb{N}$ and real numbers $\varepsilon > 0$, $0 < c < 2$. Then there is an integer $g \geq g_0$ and a smooth genus g curve defined over $\mathbb{F}_q$ such that $A^-(q) - \varepsilon \leq \#X(\mathbb{F}_q)/g \leq A^-(q) + \varepsilon$ and at least one of the following conditions is satisfied:*

i. $\mathrm{embdeg}(X)_q \geq cg$ *and* $\#X(\mathbb{F}_q)/\mathrm{embdeg}(X)_q \leq (A^-(q)+\varepsilon)/c$;

ii. $\mathrm{gon}(X)_q \leq cg$ *and* $A^-(q) - \varepsilon \leq c(q+1)$.

Remark 3. *In Theorems 1 and 2 instead of i. we may take the similar statement with* $\mathrm{injdeg}(X)_q$ *instead of* $\mathrm{embdeg}(X)_q$.

In [6, §5] M. Homma defined in the following real number $D(q)$ (called Homma constant in [7,8]).

For any positive integer d let $M_q(d)$ denote the maximal cardinality of a set $X(\mathbb{F}_q) \subset \mathbb{P}^n(\mathbb{F}_q)$ for some n and some geometrically integral curve $X \subset \mathbb{P}^n$ defined over $\mathbb{F}_q$ (we require that the inclusion $X \subset \mathbb{P}^n$ is defined over $\mathbb{F}_q$). Set

$$D(q) = \limsup_{d \to +\infty} \frac{M_q(d)}{d}.$$

By analogy with the Iihara's constant $A(q)$ and its sibling $A^-(q)$ (see [3, p. 132]) it is reasonable to define in the following way the lower Homma constant $D^-(q)$. Set

$$D^-(q) = \liminf_{d \to +\infty} \frac{M_q(d)}{d}.$$

We have $D(q) \geq A(q)/2$ ([6, Proposition 5.4]) and this lower bound was improved to $\frac{q-\sqrt{q}}{\sqrt{q}+1}$ in [7, Theorem 3.5 (3)]. In both lower bounds only smooth curves are used.

Remark 4. *The proof of [6, Proposition 5.4] gives $D^-(q) \geq A^-(q)/2$.*

There is a tension between the known upper bounds of $D(q)$, say $D(q) \leq q$, and the known lower bounds, which are of order $A(q)$ (only a bit better if q is a square). Recall again that $A(q) \leq \sqrt{q} - 1$. We think that the true upper bound of $D(q)$ (and $D^-(q)$) should be nearer to $A(q)$ (resp. $A^-(q)$) then to q). The problem is to get results on the q-injective degree of all curves with high $\#X(\mathbb{F}_q)/g(X)$ to get a better lower bound on $D(q)$ (or $D^-(q)$) in terms of $A(q)$ (or $A^-(q)$). The lower bound $D(q) \geq A(q)/2$ ([6, Proposition 5.4]) just uses that the canonical map of any non-hyperelliptic curve is an embedding and the 2 at the denominator would be substituted with the real number τ if one can prove that $\mathrm{injdeg}(X)_q \leq \tau g(X) + o(g(X))$ for enough curves (not all curves, but all curves with large ratio $\#X(\mathbb{F}_q)/g(X)$). The following result is much weaker.

Proposition 5. *Let X be a smooth and geometrically connected curve defined over $\mathbb{F}_q$. Set $g := g(X)$. Assume $g \geq 3$ and that X is not hyperelliptic. Set $z := \mathrm{gon}(X)_q$, $x := \#X(\mathbb{F}_q)$ and $\delta := 2g+1+z$ and assume $x \geq z-2$. Fix $S \subset X(\mathbb{F}_q)$ such that $\#S = z-3$. Then there is an integer $d \leq \delta$ and a morphism $f : X \to \mathbb{P}^n$, $n := g+2-z$, defined over $\mathbb{F}_q$ such that $\deg(f)\deg(f(X)) = d$ and $f_{|X(\mathbb{F}_q)\setminus S}$ is injective.*

2. The proofs

Proof of Theorem 1: Take a sequence of smooth curves $\{X_k\}_{k\in\mathbb{N}}$ evincing $A(q)$, i.e. such that $\lim \#X_k(\mathbb{F}_q)/g(X_k) = A(q)$. Thus there is $k_0 \in \mathbb{N}$ such that $g(X_k) \geq g_0$ and $A(q) - \varepsilon \leq \#X_k(\mathbb{F}_q)/g(X_k) \leq A(q) + \varepsilon$ for all $k \geq k_0$. Fix $k \geq k_0$ and set $X := X_k$ and $g := g(X_k)$. Since $\mathrm{embdeg}(X)_q \geq \mathrm{gon}(X)_q$, either $\mathrm{embdeg}(X)_q \geq cg$ or $\mathrm{gon}(X)_q \leq cg$.

a. Assume $\mathrm{gon}(X)_q \leq cg$. Thus $\#X(\mathbb{F}_q) \leq cg(q+1)$. Since $\#X(\mathbb{F}_q) \geq g(A(q)-\varepsilon)$, we get $A(q) - \varepsilon \leq c(q+1)$.

b. Assume $\mathrm{embdeg}(X)_q \geq cg$. We get $\#X(\mathbb{F}_q)/\mathrm{embdeg}(X)_q \leq \#X(\mathbb{F}_q)/cg \leq (A(q)+\varepsilon)/c$. ■

Proof of Theorem 2: By the definition of $A^-(q)$ there is an integer $g \geq g_0$ and a smooth genus g curve defined over $\mathbb{F}_q$ such that $A^-(q) - \varepsilon \leq \#X(\mathbb{F}_q)/g \leq A^-(q) - \varepsilon$. Mimic the proof of Theorem 1. ■

Proof of Proposition 5: Since $g \geq 3$, X is not hyperelliptic and the canonical line bundle of X is defined over $\mathbb{F}_q$, we see (over $\mathbb{F}_q$) as a degree $2g-2$ curve $X \subset \mathbb{P}^{g-1}$. Since $\#S < z$, the geometric form of Riemann-Roch gives $\dim\langle S\rangle = z-1$. Hence the linear projection from the linear space $\langle S\rangle$ induces a morphism $\ell_{\langle S\rangle} : \mathbb{P}^{g-1} \to \mathbb{P}^n$ defined over $\mathbb{F}_q$. Set $Z := \langle Z\rangle \cap X$, $w := \deg(Z)$ and $d := 2g-2-w$. Since X is smooth, the rational map $\ell_{\langle S\rangle|X\setminus Z} \to \mathbb{P}^n$ extends to a morphism $\ell : X \to \mathbb{P}^n$. Note that ℓ is defined over $\mathbb{F}_q$ and that $\deg(f)\deg(f(X)) = 2g-2-w$. Since $\#S \leq z-2$, no point of $X(\mathbb{F}_q) \setminus S$ is contained in $\langle S\rangle$. Since $\#S \leq z-3$, $\ell(u) \neq \ell(v)$ for any $u, v \in X(\mathbb{F}_q) \setminus S$ such that $u \neq v$. ■

3. Conclusions

We consider several remarks and proposition on the Homma constants $D(q)$ and $D(q)^-$ over the finite field $\mathbb{F}_q$. The next step would be explicit sharper bounds on the ratio $\frac{M_q(d)}{d}$ in the intermediate range for d and q.

References

[1] Niederreiter, H., & Xing, C. (2001). Rational points on curves over finite fields: theory and applications, Cambridge University Press, Cambridge.

[2] Niederreiter, H., & Xing, C. (2009). Algebraic Geometry in Coding Theory and Cryptography, Princeton University Press, Princeton, NJ.

[3] Serre, J. P., Howe, E. W., Oesterlé, J., & Ritzenthaler, C. (2020). Rational points on curves over finite fields, Documents Mathématiques, 18, Société Mathématique de France, Paris.

[4] Stichtenoth, H. (2009). Algebraic function fields and codes, Second Edition. Springer-Verlag.

[5] Tsfasman, M., Vlădut, S., & Nogin, D. (2007). *Algebraic Geometric Codes: Basic Notions*, Mathematical Surveys and Monographs, 139.

[6] Homma, M. (2012). *A bound on the number of points of a curve in a projective space over a finite field*, Theory and Applications of Finite Fields, 597, 103-110.

[7] Beelen, P., Montanucci, M., & Vicino, L. (2022). *On the constant $D(q)$ defined by Homma*. arXiv:2201.00602; accepted in Proceedings of the 18th Conference on Arithmetic, Geometry, Cryptography, and Coding Theory in the AMS book series Contemporary Mathematics (CONM).

[8] Beelen, P., & Montanucci, M. (2020). *A bound for the number of points of space curves over finite fields*. arXiv:2008.05748.