THE GENUS OF CURVES OVER FINITE FIELDS WITH MANY RATIONAL POINTS

RAINER FUHRMANN AND FERNANDO TORRES

ABSTRACT. We prove the following result which was conjectured by Stichtenoth and Xing: let g be the genus of a projective, non-singular, geometrically irreducible, algebraic curve defined over the finite field with q^2 elements whose number of rational points attains the Hasse-Weil bound; then either $4g \leq (q-1)^2$ or $2g = (q-1)q$.

Throughout, let k be the finite field of order q^2. By a curve over k we mean a projective, non-singular, geometrically irreducible, algebraic curve defined over k. This note is concerning with the genus g of maximal curves (over k); i.e., those whose number of k-rational points attains the Hasse-Weil upper bound: $q^2 + 1 + 2qg$. These curves are very useful e.g. for applications to coding theory c.f. [Sti], [Tsf-Vla]. It is known that $2g \leq (q-1)q$ ([Sti, V.3.3]), and that the Hermitian curve, defined in (2), is the only maximal curve whose genus satisfies $2g = (q-1)q$ ([R-Sti]). Here we prove the following result which was conjectured by Xing and Stichtenoth in [X-Sti].

Theorem 1. *Let $\mathcal{X}$ be a maximal curve over k of genus g. Then*

$$4g \leq (q-1)^2\,, \quad \text{or} \quad 2g = (q-1)q\,.$$

We prove this theorem by using [X-Sti, Prop. 1], [R-Sti, Lemma 1] and a particular case of the approach of Stöhr and Voloch [SV] to the Hasse-Weil bound. In Remark 1 we point out another proof of the aforementioned Rück and Stichtenoth characterization of the Hermitian curve [R-Sti]. We recall that Hirschfeld, Storme, Thas and Voloch also stated a characterization of Hermitian curves by using some results from [SV] (see [HSTV]). We use ideas from the proof of [HSTV, Lemma 1]. In [FT] is considered the case of maximal curves whose genus is bounded from above by $(q-1)^2/4$.

We are indebted to Professor J.F. Voloch for pointing out to us that the proof of the theorem above in the previous version of this note was incomplete.

2000 *Mathematics Subject Classification*: Primary 11G20; Secondary 14G05, 14G15.

Key words and phrases: finite field, the Hasse-Weil bound, curves over finite fields with many points.

The second author was supported by a grant from the International Atomic Energy Agency and UNESCO.

Manuscripta Math. 89 (1996), 103–106.

Revised version: October 2009.

Let $\mathcal{X}$ be a maximal curve of genus g over k. The starting point is the fact that there exists a k-rational point $P_0 \in \mathcal{X}$ such that q and $q+1$ are non-gaps at P_0 ([X-Sti, Prop. 1]). Thus the linear series

$$\mathcal{D} = \mathcal{D}_{\mathcal{X}} := |(q+1)P_0|$$

is simple and g and the dimension $N \geq 2$ of $\mathcal{D}$ can be related to each other via Castelnuovo's genus bound for curves in projective spaces [C], [ACGH, p. 116], [Rath, Cor. 2.8]. Therefore

$$2g \leq M(q-(N-1)+e)\,, \tag{1}$$

where M is the biggest integer $\leq q/(N-1)$ and $e = q - M(N-1)$.

Lemma 1. (cf. [X-Sti, Prop. 3]) *If* $N \geq 3$, *then* $4g \leq (q-1)^2$.

Proof. From (1) we have

$$2g \leq (q-e)(q-(N-1)+e)/(N-1) \leq (2q-(N-1))^2/4(N-1)\,,$$

and the result follows. □

Proof of Theorem 1. Let $\mathcal{X}$ be a maximal curve over k with $4g > (q-1)^2$. Then $N = 2$ by the previous lemma. The following notation and results are from [SV].

- $0 = j_0 < j_1(P) < j_2(P)$: the $(\mathcal{D}, P)$-order sequence at $P \in \mathcal{X}$;
- $0 = \epsilon_0 < 1 = \epsilon_1 < \epsilon_2$: the orders of $\mathcal{D}$;
- R the ramification divisor of $\mathcal{D}$; we have $v_P(R) \geq j_2(P) - \epsilon_2$ and
$$\deg(R) = (\epsilon_0 + \epsilon_1 + \epsilon_2)(2g-2) + 3(q+1)\,;$$
- $\nu_0 = 0 < \nu_1 \in \{1, \epsilon_2\}$ the q^2-Frobenius orders;
- S the q^2-Frobenius divisor; we have $v_P(S) \geq j_1(P) + (j_2(P) - \nu_1)$ for all $P \in \mathcal{X}(k)$ and
$$\deg(S) = \nu_1(2g-2) + (q^2+2)(q+1)\,.$$

We claim that $\nu_1 = \epsilon_2 = q$. Indeed, by [R-Sti, Lemma 1], $j_2(P) = q+1$ for any $P \in \mathcal{X}(k)$ and thus for such points $v_P(S) \geq q+1-\nu_1$. It follows that

$$\deg(S) = \nu_1(2g-2) + (q^2+2)(q+1) \geq (q+1-\nu_1)(q^2+1+2qg)\,;$$

after some computations we get

$$(q-1)(\nu_1(q+1)-q) \geq 2g(q^2 - \nu_1(q+1) + 2q)$$

so that $\nu_1 \geq q$ and $\nu_1 = \epsilon_2 \leq q+1$. We have that $\epsilon_2 = q$ by the p-adic criterion and the claim follows.

Finally, $v_P(R) \geq 1$ for any $P \in \mathcal{X}(k)$ so that

$$\deg(R) = (1+q)(2g-2) + 3(q+1) \geq q^2 + 1 + 2qg$$

i.e. $2g \geq (q-1)q$ and the result follows as we already remarked that $2g \leq (q-1)q$.

Remark 1. We close this note by proving that a maximal curve of genus $(q-1)q/2$ is k-isomorphic to the so-called Hermitian curve:

$$y^q + y = x^{q+1}\,. \tag{2}$$

The proof is inspired on the example stated in [SV, p. 16]. Let $P_0 \in \mathcal{X}(k)$ and $x, y \in k(\mathcal{X})$ such that

$$\mathrm{div}_\infty(x) = qP_0 \quad \text{and} \quad \mathrm{div}_\infty(y) = (q+1)P_0\,.$$

Then by the Riemann-Roch theorem the k-dimension of the Riemann-Roch space $\mathcal{L}(q(q+1)P_0)$ is equal to $(q+1)(q+2)/2$. Since

$$\#\{x^i y^j : (i,j) \in \mathbb{N}_0^2,\ iq + j(q+1) \le q(q+1)\} = \frac{(q+1)(q+2)}{2} + 1\,,$$

there exists a non-trivial k-linear relation:

$$F = F(x,y) = \sum_{iq+j(q+1)\le q(q+1)} a_{i,j} x^i y^j = 0\,,$$

where $a_{q+1,0} \neq 0$ and $a_{0,q} \neq 0$. Let us assume $a_{0,q} = 1$ and hence

$$F = y^q + a_{q+1,0}x^{q+1} + G = 0\,, \tag{3}$$

where

$$G = G(x,y) = \sum_{iq+j(q+1)<q(q+1)} a_{i,j} x^i y^j\,.$$

Thus $\mathcal{X}$ is k-isomorphic to the plane curve defined by $F = 0$. The fact that $\nu_1 = q$ means that

$$y^{q^2} - y = D_x y (x^{q^2} - x) \tag{4}$$

where $F_x + F_y D_x y = 0$, F_x and F_y being the partial derivatives with respect to the variables x and y respectively. Observe that $F_y \neq 0$ as $\mathcal{X}$ is non-singular. From (3) and (4) we obtain

$$-a_{q+1,0}^q x^{q^2+q} - G^q - y = D_x y (x^{q^2} - x)\,.$$

By taking a particular k-rational point of the curve, says $P_1 = (a,b) \neq P_0$, $-a_{q+1,0}^q a^{1+q} - G(a,b) - b = 0$. It follows from (3) that $a_{q+1,0} \in \mathbb{F}_q$ and thus we can assume $a_{q+1,0} = -1$ as the norm function $\mathbb{F}_{q^2} \to \mathbb{F}_q$ is surjective. So far we have the following relations:

$$y^q + G = x^{q+1}\,, \quad G_x + G_y D_y x = x^q\,. \tag{5}$$

Let v denote the valuation associated to P_0. From (4) $v(D_x y) = -q^2$ and hence $v(x^q - G_x) = v(x^q) = q^2$; it follows from (5) that $v(G_y) = 0$. We deduce that $G_y = a_{0,1} \neq 0$. Thus once again from (4) and (5)

$$a_{0,1}x^{q^2+q} - a_{0,1}G^q - a_{0,1}y = x^{q^2+q} - x^{q+1} - G_x x^{q^2} + G_x x\,,$$

and so $a_{0,1} = 1$, $G_x = 0$. Finally $D_y x = x^q$ and thus $y^{q^2} - y = x^q(x^{q^2} - x)$ gives

$$(y^q + y - x^{q+1})^q = y^q + y - x^{q+1}$$

and the remark follows.

References

[ACGH] E. Arbarello, M. Cornalba, P.A., Griffiths and J. Harris, "Geometry of algebraic curves", Vol. I, Springer-Verlag, New York 1985.

[C] G. Castelnuovo, *Ricerche di geometria sulle curve algebriche*, Atti. R. Acad. Sci. Torino **24** (1889), 196–223.

[FT] R. Furhmann and F. Torres, *Curves over finite fields with the maximal number of rational points*, in preparation.

[HSTV] J.W.P. Hirschfeld, L. Storme, J.A. Thas and J.F. Voloch, *A characterization of Hermitian curves*, J. Geom. **41** (1991), 72–78.

[Rath] J. Rathmann, *The uniform position principle for curves in characteristic* p, Math. Ann. **276** (1987), 565–579.

[R-Sti] H.G. Rück and H. Stichtenoth, *A characterization of Hermitian function fields over finite fields*, J. reine. angew. Math. **457** (1994), 185–188.

[Sti] H. Stichtenoth, "Algebraic functions fields and codes", Springer-Verlag, Berlin, 1993.

[SV] K.O. Stöhr and J.F. Voloch, *Weierstrass points and curves over finite fields*, Proc. London Math. Soc. (3) **52** (1986), 1–19.

[Tsf-Vla] M. Tsfasman and S.G. Vladut, "Algebraic-Geometric Codes", Kluwer Academic Publishers, Dordrecht-Boston-London 1991.

[X-Sti] C. Xing and H. Stichtenoth, *The genus of maximal functions fields*, Manuscripta Math. **86** (1995), 217–224.

Fachbereich 6 Mathematik und Informatik Universität Essen, W - 4300 Essen 1, FRG

E-mail address: `rfuhr@de.ibm.com`

Mathematics Section ICTP, P.O. Box 586-34100, Trieste-Italy

E-mail address: `feto@ ictp.trieste.it`