ACTA ARITHMETICA
151.2 (2012)

On a tower of Ihara and its limit

by

Nicolás Caro and Arnaldo Garcia (Rio de Janeiro)

1. Introduction. Towers of function fields over a fixed finite field have attracted much attention, especially in view of connections with coding theory and cryptography (see [TV], [NX], [Z], [GS2] and [GS3]). Ihara was the first to realize that the so-called Hasse–Weil upper bound is weak if the genus of the function field is large with respect to the cardinality of the finite field (see [Iha]). The first explicit tower (i.e., one with the function fields given by explicit polynomial equations) with an optimal asymptotic behaviour was obtained over square finite fields (see [GS]). Zink has shown the existence of towers over cubic finite fields with an exceptional asymptotic behaviour (see [Z]). The first explicit tower with this behaviour was obtained by van der Geer and van der Vlugt over the finite field with eight elements (see [GV]). Generalizations of the tower in [GV] were obtained in [BeGS] and [BaGS].

Here we study another tower $\mathcal{F}_0$ over cubic finite fields, also generalizing the tower in [GV]. This tower was introduced by Ihara [Ih] as a subtower of the tower in [BeGS]. A detailed exposition of $\mathcal{F}_0$ can be found in [C] where the genera of the function fields of the tower in [BaGS] are also determined.

Let k be a finite field. A *tower* $\mathcal{F}$ over k is an infinite sequence

$$\mathcal{F} = (F_1 \subseteq F_2 \subseteq \cdots)$$

of function fields F_n over k such that:

(a) k is algebraically closed in F_n for all $n \in \mathbb{N}$,

(b) $g(F_n) \to \infty$ as $n \to \infty$, where $g(\cdot)$ denotes the genus.

We can assume that the extensions F_n/F_1 are finite and separable. The *ramification locus* $R(\mathcal{F})$ is the set of places P of the first field F_1 that are ramified in $\mathcal{F}$; i.e., for some $n \geq 2$ and some place Q of F_n above P we have $e(Q|P) > 1$, where $e(Q|P)$ denotes the ramification index. When $R(\mathcal{F})$ is a

2010 *Mathematics Subject Classification*: Primary 11G20; Secondary 14H05, 14H25.
Key words and phrases: function fields, finite fields, rational places, genus, towers, limit of towers.

DOI: 10.4064/aa151-2-3

finite set we denote $\deg R(\mathcal{F}) := \sum \deg P$, where we sum over $P \in R(\mathcal{F})$. The *splitting locus* $S(\mathcal{F})$ is the set of k-rational places P of the first field F_1 such that, for every $n \geq 2$, the number of places of F_n above P is equal to the degree $[F_n : F_1]$. In particular, any such place of F_n is again k-rational.

The tower $\mathcal{F}$ has a limit (see Lemma 7.2.3 of [Sti])

$$\lambda(\mathcal{F}) := \lim_{n\to\infty} \frac{N(F_n)}{g(F_n)},$$

where $N(F_n)$ is the number of k-rational places of F_n.

A tower $\mathcal{F}$ over k is said to be *recursive* if there is a polynomial $f(X,Y) \in k[X,Y]$ such that for each $n \in \mathbb{N}$,

$$F_n = k(x_1,\dots,x_n) \quad \text{and} \quad f(x_i,x_{i+1}) = 0 \quad \text{for } i = 1,\dots,n-1.$$

In the particular case of a cubic finite field $k = \mathbb{F}_{q^3}$, it is shown in [BeGS] that the equation

$$\text{(1.1)} \qquad \frac{1-Y}{Y^q} = \frac{X^q + X - 1}{X}$$

defines a recursive tower $\mathcal{F}_1$ over $\mathbb{F}_{q^3}$ with an exceptional asymptotic behaviour, i.e.,

$$\text{(1.2)} \qquad \lambda(\mathcal{F}_1) \geq \frac{2(q^2-1)}{q+2}.$$

A tower $\mathcal{F} = (F_n)_{n\in\mathbb{N}}$ is said to be a *subtower* of $\mathcal{E} = (E_m)_{m\in\mathbb{N}}$ if for each $n \in \mathbb{N}$ we have

$$F_n \subseteq E_m \quad \text{for some } m = m(n).$$

For a subtower $\mathcal{F}$ of $\mathcal{E}$ we have $\lambda(\mathcal{F}) \geq \lambda(\mathcal{E})$ (see Prop. 7.2.8 of [Sti]).

Ihara [Ih] shows that the equation

$$\text{(1.3)} \qquad Y^{q+1} + Y = \frac{X+1}{X^{q+1}}$$

defines a subtower $\mathcal{F}_0$ of the tower $\mathcal{F}_1$ above. Actually Ihara used (5.3) below to define the recursive tower $\mathcal{F}_0$.

Hence we also have

$$\text{(1.4)} \qquad \lambda(\mathcal{F}_0) \geq \frac{2(q^2-1)}{q+2}.$$

The objective of this note is to give a direct proof of (1.4), without using the fact that $\mathcal{F}_0$ is a subtower of $\mathcal{F}_1$. This direct proof is much simpler than the proof of inequality (1.2) in [BeGS].

The novelty here is that although the extensions in the pyramid associated to the tower $\mathcal{F}_0$ are not Galois for $q \neq 2$, they become Galois after completion at certain places.

The paper is organized as follows:

Section 2 describes ramification indices and different exponents in the two basic extensions associated to (1.3):

$$k(X,Y)/k(X) \quad \text{and} \quad k(X,Y)/k(Y).$$

Section 3 introduces the concept of B-bounded towers and gives a formula for its limit (see (3.1) below). A basic reference in this section is [GS2].

Only in Section 4 do we show that $\mathcal{F}_0$ is indeed a tower of function fields over the cubic finite field $k = \mathbb{F}_{q^3}$. In that section we give the strategy to show that the tower $\mathcal{F}_0$ is B-bounded with $B = q/(q-1)$.

Using completion at certain places in the tower $\mathcal{F}_0$ and showing that after completion the bottom extensions become Galois, we finish in Section 5 the proof that $B = q/(q-1)$. Here we use Proposition 12 of [GS2] in a fundamental way. We end up with a remark showing that a tower of Ihara (see [Ih]) given by (5.3) below is the same as the tower $\mathcal{F}_0$ given by (1.3).

2. The tower $\mathcal{F}_0$ over $\mathbb{F}_{q^3}$. We consider the tower $\mathcal{F}_0$ over $k = \mathbb{F}_\ell$ with $\ell = q^3$ given recursively by the equation

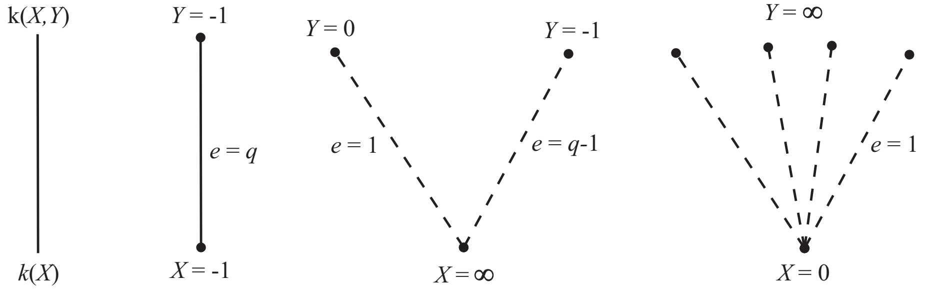
$$Y^{q+1} + Y = \frac{X+1}{X^{q+1}}. \tag{2.1}$$

We stress that we will show that $\mathcal{F}_0$ is indeed a tower over k only in Section 4. Note that $T^{q+1} + T + 1 = 0$ is separable and has all roots in $\mathbb{F}_{q^3}$, and also, from (2.1),

$$X^{q+1} + X + 1 = 0 \ \Rightarrow \ Y^{q+1} + Y + 1 = 0.$$

This shows that $x_1^{q+1} + x_1 + 1 = 0$ is completely splitting over $\mathbb{F}_{q^3}$ and hence the splitting locus $S(\mathcal{F}_0)$ satisfies $\#S(\mathcal{F}_0) \geq q+1$.

Note that (2.1) is not irreducible; in fact, one can easily see that $Y = -(X+1)/X$ is a root of it. Actually, we will see that (2.1) defines a tower $\mathcal{F}_0 = (F_1, F_2, \ldots)$ over the cubic finite field $\mathbb{F}_{q^3}$ with $[F_{n+1} : F_n] = q$. We have the following pattern for the ramification in the basic extension $k(X,Y)/k(X)$ associated to (2.1):



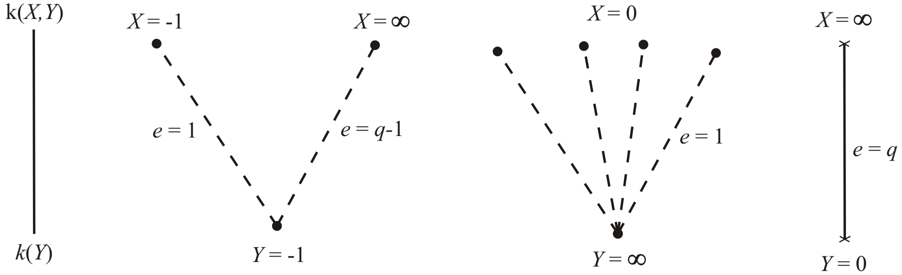
Above we have $[k(X,Y):k(X)]=q$ and also the place of $k(X)$ with $X=0$ has above it q places P of $\bar{k}(X,Y)$ with $Y=\infty$ and ramification index $e=1$. Here $\bar{k}$ denotes an algebraic closure of k. To see the last assertion, we substitute $Y=y-\frac{X+1}{X}$ into (2.1), and get the following equation:

$$(2.2)\qquad (Xy)^q=(X+1)(Xy)^{q-1}+1.$$

From (2.2) we see that at the places P of $\bar{k}(X,Y)$ above $X=0$, we have

$$(Xy)(P)=\alpha^{-1}\quad \text{with } \alpha\in\bar{k} \text{ such that } \alpha^q+\alpha=1.$$

Similarly for the extension $k(X,Y)/k(Y)$ we get:



For the different exponents we have (see Prop. 3.5.12 of [Sti]):

- $d(Q_1|P_1)=q$, where Q_1 is the unique place of $k(X,Y)$ above $P_1:=(X=-1)$ of $k(X)$.
- $d(R_1|S_1)=q$, where R_1 is the unique place of $k(X,Y)$ above $S_1:=(Y=0)$ of $k(Y)$.

We first show that $d(Q_1|P_1)=q$. In fact, (2.2) can be written as

$$Z^q=(X+1)(Z+1)^{q-1}\quad\text{where}\quad Z:=Xy-1.$$

The derivative is $(X+1)(Z+1)^{q-2}$ and its value at the place Q_1 is equal to q.

Similarly we have $d(R_1|S_1)=q$. Again in this case we rewrite (2.2) as

$$W^q=Y(W+1)^{q-1}+Y^q,\quad\text{where}\quad W:=\frac{1}{X}+Y.$$

The derivative is $Y(W+1)^{q-2}$ and its value at the place R_1 is equal to q.

3. Bounded towers. A place P_n of a field F_n in a tower $\mathcal{F}=(F_1\subseteq F_2\subseteq\cdots)$ is called B-*bounded* if

$$d(P_n|P_1)\le B(e(P_n|P_1)-1),$$

where P_1 is the restriction of P_n to the first field F_1, $d(P_n|P_1)$ denotes the exponent of the different and $e(P_n|P_1)$ denotes the ramification index.

The tower $\mathcal{F}$ is called B-bounded if all places P_n of F_n, for every $n\in\mathbb{N}$, are B-bounded.

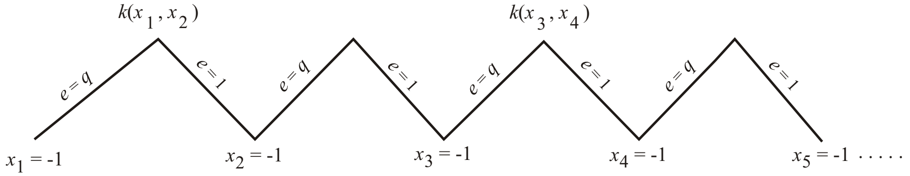
We have the following result for the limit of a B-bounded tower $\mathcal{F}$ with finite ramification locus $R(\mathcal{F})$ and nonempty splitting locus $S(\mathcal{F})$ (see [GS2]):

$$\lambda(\mathcal{F}) \geq \frac{\#S(\mathcal{F})}{g(F_1) - 1 + \frac{B}{2} \cdot \deg R(\mathcal{F})}. \tag{3.1}$$

In the case of the tower $\mathcal{F}_0$ given recursively by (2.1), the point here is to show that it is B-bounded with $B = q/(q-1)$. From (3.1) we then get the limit (using $\#S(\mathcal{F}_0) = q+1$ and $\deg R(\mathcal{F}_0) = 3$)

$$\lambda(\mathcal{F}_0) \geq \frac{q+1}{-1 + \frac{3}{2} \cdot \frac{q}{q-1}} = \frac{2(q^2-1)}{q+2}.$$

4. Strategy to show that $B = q/(q-1)$. We first show that the place $P_1 := (x_1 = -1)$ is fully ramified in the tower $\mathcal{F}_0$, i.e., it is fully ramified in all extensions F_n/F_1 for $n \geq 2$. Indeed we have the following pattern:



This shows that P_1 is fully ramified in F_n. At the same time it shows that $\mathcal{F}_0$ is a tower with $[F_{n+1} : F_n] = q$, and in particular also that $k = \mathbb{F}_{q^3}$ is algebraically closed in each field F_n for $n \geq 1$. Denoting by P_n the unique place of F_n above P_1 we have

$$e(P_{n+1}|P_n) = d(P_{n+1}|P_n) = q \quad \text{for all } n \geq 1.$$

This shows that P_n is B-bounded with $B = q/(q-1)$, as follows from the transitivity of different exponents (see [GS2]).

Another possible pattern of ramification is as follows:

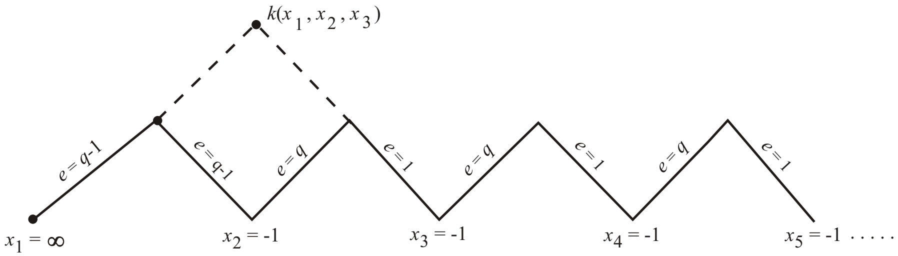
We denote by Q_2 the unique place of F_2 with $x_1 = \infty$ and $x_2 = -1$. We have a unique place Q_n of F_n above Q_2, for each $n \geq 3$. For the place extension $Q_3|Q_2$, using Abhyankar's lemma and the transitivity of differents (see [Sti, Sections 3.5 and 3.9]), we have

$$d(Q_3|Q_2) + q(q-2) = q - 2 + (q-1)q. \tag{4.1}$$

Hence $Q_3|Q_2$ is 2-bounded; more precisely, $d(Q_3|Q_2) = 2(q-1)$. With similar arguments we find that $Q_n|Q_2$ is 2-bounded for all $n \geq 3$; more precisely,

$$d(Q_n|Q_2) = 2(e(Q_n|Q_2) - 1) \quad \text{for } n \geq 3.$$

We then have a situation of ramification as follows:



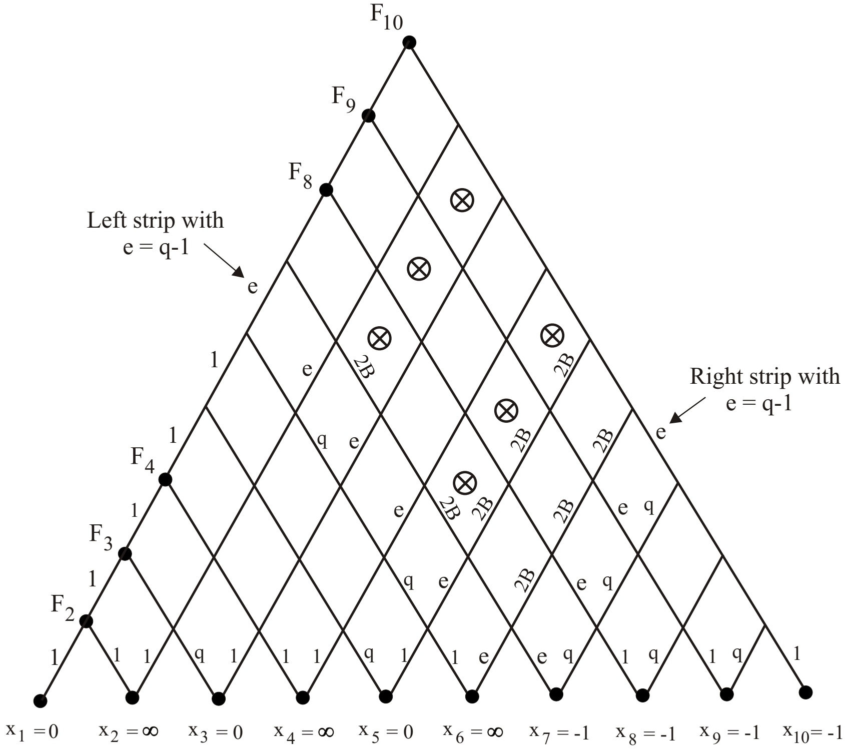


Fig. 1

In the extension F_2/F_1 the place Q_2 is tamely ramified with ramification index $e = q-1$ and in the extension F_n/F_2 the place Q_n of F_n above Q_2 is fully ramified and 2-bounded. From the transitivity and denoting $E = e(Q_n|Q_2)$, we get

$$\begin{aligned} d(Q_n|Q_2) + E(q-2) &= 2(E-1) + E(q-2) \\ &= Eq - 2 \leq \frac{q}{q-1}((q-1)E-1). \end{aligned} \tag{4.2}$$

Note that $(q-1)E$ is the ramification index of Q_n over the first field F_1 of the tower $\mathcal{F}_0$. This shows that the places Q_n above, for $n \geq 3$, are B-bounded with $B = q/(q-1)$.

In Figure 1 we write ramification indices over the edges of the pyramid, with the notation $e := q - 1$. We have also written $2B$ over an edge to indicate that the corresponding place extension is 2-bounded, more precisely to indicate that

$$\text{different exponent} = 2 \cdot \text{ramification index} - 2.$$

The argument for the equality above is the one given in (4.1). Of course the situation in Figure 1 is just a concrete instance that helps understand the strategy.

We are then left with the problem of deciding the behaviour of different exponents in a diamond of Fig. 2, where A denotes a place, B, C and D denote the restrictions of A to the corresponding subfields, and we know that

$$d(B|D) = 2(e(B|D) - 1), \quad d(C|D) = 2(e(C|D) - 1).$$

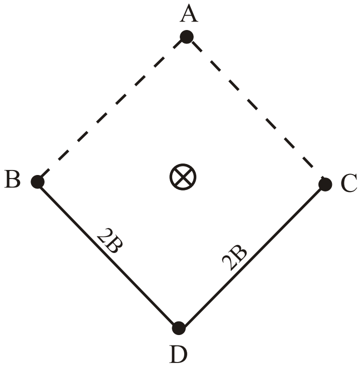


Fig. 2

The main difficulty of the tower $\mathcal{F}_0$ is to show that in Figure 2 we always have

$$d(A|B) = 2(e(A|B) - 1), \quad d(A|C) = 2(e(A|C) - 1). \tag{4.3}$$

If the bottom field extensions in Figure 2 were both Galois, then this would follow directly from Proposition 12 in [GS2]. But in our case of the tower $\mathcal{F}_0$, those extensions are Galois only if $q = 2$. What we are going to show in the next section is that after completion at the places in Figure 2, the bottom extensions become Galois, thus allowing the use of Proposition 12 of [GS2]. Once we know that the completions are Galois, the proof ends as follows (using here Figure 1 for clarity): we first deal with the diamonds (going upwards to the right) marked ⊗ situated on the strip between $x_4 = \infty$

and $x_5 = 0$; having obtained the behaviour in (4.3) for the upper sides of those diamonds, we move upwards to the left and we deal with the diamonds marked $\otimes$ situated on the strip between $x_2 = \infty$ and $x_3 = 0$, and so on.

At the end (if $x_1 = 0$ or $x_1 = \infty$, and $x_n = -1$ for some $n \geq 2$) we will have in the tower $\mathcal{F}_0$ a situation where a ramification index $e = q-1$ occurs first and it is followed by the 2-bounded behaviour:

$$\text{different exponent} = 2 \cdot \text{ramification index} - 2.$$

Now the argument in (4.2) finishes the proof that $\mathcal{F}_0$ is B-bounded with $B = q/(q-1)$.

5. Galois after completion. In Figure 1 we now have to focus on the diamonds marked $\otimes$. Any such diamond for the tower $\mathcal{F}_0$ is represented in Figure 2. We are going to show that after completion at the corresponding places, the bottom extensions of the diamond become Galois. We will see that the right (resp. left) strip with $e = q-1$ in Figure 1 is responsible for the bottom right (resp. left) extension in Figure 2 to become Galois.

We just prove here the right extension case, the left one is done similarly. For the bottom right extension we have an equation (see (2.2))

$$\left(\frac{1}{Xy}\right)^q + (X+1)\left(\frac{1}{Xy}\right) = 1,$$

where $X = x_n$ and $y = x_{n+1} + (x_n+1)/x_n$ for some n. For simpliciy we write $T = 1/Xy$ and we want to determine the Galois closure of the equation

$$T^q + (X+1)T - 1 = 0. \tag{5.1}$$

If $T+V$ is another root,

$$(T+V)^q + (X+1)(T+V) - 1 = 0,$$

then we get the Kummer extension

$$V^{q-1} + (X+1) = 0. \tag{5.2}$$

So to move to the Galois closure of equation (5.1) we have to add on top a Kummer extension given by (5.2). At the places we are considering, $X+1$ has a zero whose order is a multiple of $e = q-1$, as follows from the right strip with $e = q-1$ (see Figure 1). This shows that the places we are considering are unramified in the Kummer extension given by (5.2) and hence we conclude that the completion becomes Galois.

This finishes the proof that the tower $\mathcal{F}_0$ has the exceptional asymptotic behaviour of (2.1). The strategy used above to deal with $\mathcal{F}_0$ is inspired by [GS1] and [BS]. The novelty here is the phenomenon of becoming Galois after completion at certain places.

Remark. In [Ih] it is shown that the equation

$$\frac{y-1}{y^{q+1}} = \frac{-x^q}{(1-x)^{q+1}} \tag{5.3}$$

over $k = \mathbb{F}_{q^3}$ defines a subtower of the tower $\mathcal{F}_1$ considered in [BeGS]. This subtower is the same as the tower $\mathcal{F}_0$ considered in this paper; in fact the substitutions

$$x = \frac{1}{X+1} \quad \text{and} \quad y = \frac{1}{Y+1}$$

transform equation (5.3) of Ihara into our equation (2.1).

References

[BaGS] A. Bassa, A. Garcia and H. Stichtenoth, *A new tower over cubic finite fields*, Moscow Math. J. 8 (2008), 401–418.

[BS] A. Bassa and H. Stichtenoth, *A simplified proof for the limit of a tower over a cubic finite field*, J. Number Theory 123 (2007), 154–169.

[BeGS] J. Bezerra, A. Garcia and H. Stichtenoth, *An explicit tower of function fields over cubic finite fields and Zink's lower bound*, J. Reine Angew. Math. 589 (2005), 159–199.

[C] N. Caro, *Towers of function fields over cubic finite fields*, Ph.D. Thesis, IMPA, 2009; www.preprint.impa.br/Shadows/SERIE_C/2010/98.html.

[GS] A. Garcia and H. Stichtenoth, *A tower of Artin–Schreier extensions of function fields attaining the Drinfeld–Vladut bound*, Invent. Math. 121 (1995), 211–222.

[GS1] —, —, *Some Artin–Schreier towers are easy*, Moscow Math. J. 5 (2005), 767–774.

[GS2] —, —, *On the Galois closure of towers*, in: Recent Trends in Coding Theory and its Applications, AMS/IP Stud. Adv. Math. 41, Amer. Math. Soc., Providence, RI, 2007, 83–92.

[GS3] —, —, (eds.), *Topics in Geometry, Coding Theory and Cryptography*, Algebra Appl. 6, Springer, Dordrecht, 2007.

[GV] G. van der Geer and M. van der Vlugt, *An asymptotically good tower of curves over the field with eight elements*, Bull. London Math. Soc. 34 (2002), 291–300.

[Iha] Y. Ihara, *Some remarks on the number of points of algebraic curves over finite fields*, J. Fac. Sci. Tokyo 28 (1982), 721–724.

[Ih] —, *Some remarks on the BGS tower over finite cubic fields*, in: Proc. Conf. Arithmetic Geometry, Related Area and Applications (Chuo University, 2006), 2007, 127–131.

[NX] H. Niederreiter and C. P. Xing, *Rational Points on Curves over Finite Fields: Theory and Applications*, London Math. Soc. Lecture Note Ser. 285, Cambridge Univ. Press, Cambridge, 2001.

[Sti] H. Stichtenoth, *Algebraic Function Fields and Codes*, Grad. Texts in Math. 254, Springer, Berlin, 2009.

[TV] M. Tsfasman and S. Vladut, *Algebraic Geometric Codes*, Kluwer, Dordrecht, 1991.

[Z] T. Zink, *Degeneration of Shimura surfaces and a problem in coding theory*, in: Fundamentals of Computation Theory (Cottbus, 1985), Lecture Notes in Comput. Sci. 199, Springer, Berlin, 1985, 503–511.

Nicolás Caro, Arnaldo Garcia
IMPA-Instituto de Matemática Pura e Aplicada
Estrada Dona Castorina 110
22.460-320, Rio de Janeiro, Brazil
E-mail: nickarus@impa.br
garcia@impa.br

Received on 5.10.2010
and in revised form on 4.4.2011 (6509)