Journal de Théorie des Nombres de Bordeaux

anciennement Séminaire de Théorie des Nombres de Bordeaux

Stéphane BALLET et Robert ROLLAND

Lower bounds on the class number of algebraic function fields defined over any finite field

Tome 24, n° 3 (2012), p. 505-540.

<http://jtnb.cedram.org/item?id=JTNB_2012__24_3_505_0>

Journal de Théorie des Nombres
de Bordeaux **24** (2012), 505-540

Lower bounds on the class number of algebraic function fields defined over any finite field

par Stéphane BALLET et Robert ROLLAND

Résumé. Nous donnons des bornes inférieures sur le nombre de diviseurs effectifs de degré $\leq g-1$ par rapport au nombre de places d'un certain degré d'un corps de fonctions algébriques de genre g défini sur un corps fini. Nous déduisons des bornes inférieures du nombre de classes qui améliorent les bornes de Lachaud-Martin-Deschamps et des bornes inférieures asymptotiques atteignant celles de Tsfasman-Vladut. Nous donnons des exemples de tours de corps de fonctions algébriques ayant un grand nombre de classes.

Abstract. We give lower bounds on the number of effective divisors of degree $\leq g-1$ with respect to the number of places of certain degrees of an algebraic function field of genus g defined over a finite field. We deduce lower bounds for the class number which improve the Lachaud - Martin-Deschamps bounds and asymptotically reaches the Tsfasman-Vladut bounds. We give examples of towers of algebraic function fields having a large class number.

1. Introduction

1.1. General context. We recall that the class number $h(F/\mathbb{F}_q)$ of an algebraic function field $F/\mathbb{F}_q$ defined over a finite field $\mathbb{F}_q$ is the cardinality of the Picard group of $F/\mathbb{F}_q$. This numerical invariant corresponds to the number of $\mathbb{F}_q$-rational points of the Jacobian of any curve $X(\mathbb{F}_q)$ having $F/\mathbb{F}_q$ as algebraic function field. Estimating the class number of an algebraic function field is a classic problem. By the standard estimates deduced from the results of Weil [16] [17], we know that

$$(\sqrt{q}-1)^{2g} \leq h(F/\mathbb{F}_q) \leq (\sqrt{q}+1)^{2g},$$

where g is the genus of $F/\mathbb{F}_q$. Moreover, these estimates hold for any Abelian variety. Finding good estimates for the class number $h(F/\mathbb{F}_q)$ is a difficult problem. For $g=1$, namely for elliptic curves, the class number $\mathbb{F}_q$ is the

Manuscrit reçu le 29 juin 2011.
Mots clefs. Finite field, function field, class number.
Classification math. 14H05, 12E20.

number of $\mathbb{F}_q$-rational points of the curve and this case has been extensively studied. So, from now on we assume that $g \geq 2$. In [8], Lachaud - Martin-Deschamps obtain the following result:

Theorem 1.1. *Let X be a smooth absolutly irreducible projective algebraic curve of genus g defined over $\mathbb{F}_q$; Let J_X be the Jacobian of X and $h = \mid J_X(\mathbb{F}_q) \mid$. Then:*

(1)

$$h \geq q^{g-1} \frac{(q-1)^2}{(q+1)(g+1)};$$

(2)

$$h \geq (\sqrt{q}-1)^2 \frac{q^{g-1}-1}{g} \frac{\mid X(\mathbb{F}_q) \mid +q-1}{q-1};$$

(3) *if $g > \frac{\sqrt{q}}{2}$ and if X has at least a rational point over $\mathbb{F}_q$, then*

$$h \geq (q^g - 1) \frac{q-1}{q+g+gq}.$$

This result was improved in certain cases by the following result of Perret in [10]:

Theorem 1.2. *Let J_X the Jacobian variety of the projective smooth irreducible curve X of genus g defined over $\mathbb{F}_q$. Then*

$$\#J_X(\mathbb{F}_q) \geq \left(\frac{\sqrt{q}+1}{\sqrt{q}-1} \right)^{\frac{\#X(\mathbb{F}_q)-(q+1)}{2\sqrt{q}} - 2\delta} (q-1)^g$$

with $\delta = 1$ if $\frac{\#X(\mathbb{F}_q)-(q+1)}{2\sqrt{q}} \notin \mathbb{Z}$ and $\delta = 0$ otherwise.

Moreover, Tsfasman [12] and Tsfasman-Vladut [13] [14] obtain asymptotics for the Jacobian; these best known results can also be found in [15]. We recall the following three important theorems contained in this book. The first one concerns the so-called asymptotically good families.

Theorem 1.3. *Let $\{X_i\}_i$ be a family of curves over $\mathbb{F}_q$ (called asymptotically good) of growing genus such that*

$$\lim_{i \to +\infty} \frac{N(X_i)}{g(X_i)} = A > 0,$$

where $N(X_i)$ denotes the number of rational points of X_i over $\mathbb{F}_q$. Then

$$\liminf_{g \to +\infty} \frac{log_q h(X_i)}{g(X_i)} \geq 1 + A \log_q \left(\frac{q}{q-1} \right).$$

The second important result, established by Tsfasman in [12, Corollary 2], relates to particular families of curves, which are called asymptotically exact, namely the families of (smooth, projective, absolutly irreducible) curves $\mathcal{X}/\mathbb{F}_q = \{X_i\}_i$ defined over $\mathbb{F}_q$ such that $g(X_i) \to +\infty$ and for any $m \in \mathbb{N}$ the limit

$$\beta_m = \beta_m(\mathcal{X}/\mathbb{F}_q) = \lim_{i \to +\infty} \frac{B_m(X_i)}{g(X_i)}$$

exists, where $B_m(X_i)$ denotes the number of points of degree m of X_i over $\mathbb{F}_q$ (in term of the dual language of algebraic function field theory, it corresponds to the number of places of degree m of the algebraic function field $F(X_i)/\mathbb{F}_q$ of the curve $X_i/\mathbb{F}_q$).

Theorem 1.4. *For an asymptotically exact family of curves $\mathcal{X}/\mathbb{F}_q = \{X_i\}_i$ defined over $\mathbb{F}_q$, the limit*

$$H(\mathcal{X}/\mathbb{F}_q) = \lim_{i \to +\infty} \frac{1}{g(X_i)} \log_q h(X_i)$$

exists and equals

$$H(\mathcal{X}/\mathbb{F}_q) = 1 + \sum_{m=1}^{\infty} \beta_m . \log_q \frac{q^m}{q^m - 1}.$$

The third theorem (cf. [12, Theorem 5], [13, Theorem 3.1]) is a general result concerning the family of all curves defined over $\mathbb{F}_q$.

Theorem 1.5. *Let $\{X_i\}_i$ be the family of all curves over $\mathbb{F}_q$ (one curve from each isomorphism class). Then, we have*

$$1 \leq \liminf_{g \to +\infty} \frac{\log_q h(X_i)}{g(X_i)} \leq \limsup_{g \to +\infty} \frac{\log_q h(X_i)}{g(X_i)} \leq 1 + (\sqrt{q} - 1) \log_q \left(\frac{q}{q-1} \right).$$

Then, Lebacque [9, Theorem 7] obtains an explicit version of the Generalized Brauer-Siegel theorem valid in the case of smooth absolutly irreducible abelian varieties defined over a finite field and for the number fields under GRH. Specialized to the case of smooth absolutly irreducible curves defined over a finite field, this theorem leads to the following result:

Theorem 1.6. *For any smooth absolutly irreducible curve X of genus g defined over the finite field $\mathbb{F}_r$, one has, as $N \to \infty$:*

$$\sum_{m=1}^{N} \Phi_{r^m} \log \left(\frac{r^m}{r^m - 1} \right) = \log N + \gamma + \log(\aleph_X \log r) + \mathcal{O}(\frac{1}{N}) + g\mathcal{O}(\frac{r^{-N/2}}{N})$$

where $\Phi_{r^m} := \#\{\mathfrak{p} \in \mid X \mid\mid \deg(\mathfrak{p}) = m\}$, $\mid X \mid$ denotes the set of closed points of X and $\aleph_X$ denotes the residue at $s = 1$ of the zeta function ζ_X of X. Moreover, the $\mathcal{O}$ constants are effective and do not depend on X.

Passing to the limit in the previous result gives the asymptotics of Tsfasman-Vladut [13] [14]. Note also that as the constants are effective, this result could lead to effective non-asymptotic lower bounds of the class number h.

1.2. New results.

1.2.1. ***Quick overview.*** In this paper, we prove and we extend the results announced in [2]. First, we obtain in Theorem 3.1 and Corollary 3.2 bounds for the class number valid for all $g \geq 2$, namely mainly:

Theorem 1.7. *Let $F/\mathbb{F}_q$ be an algebraic function field defined over $\mathbb{F}_q$ of genus $g \geq 2$ and h the class number of $F/\mathbb{F}_q$. Suppose that the numbers B_1 and B_r of places of degree respectively 1 and r are strictly positive. Then:*

$$h \geq \frac{(q-1)^2}{(g+1)(q+1)} q^{g-1} \left(\frac{q^{r\lfloor \frac{(g-2)}{r} \rfloor} - 1}{q^{r(\lfloor \frac{(g-2)}{r} \rfloor - 1)}(q^r - 1)} + \frac{(B_r - 1)}{q^r} f_r \right);$$

where

$$f_r = \begin{cases} 0 & \text{if} \quad \frac{g-2}{2} < r \leq g-2; \\ 1 & \text{if} \quad r \leq \frac{g-2}{2} \text{ and } B_r < q^r; \\ \min\left(\lfloor \frac{B_r - q^r}{q^r - 1} \rfloor + 1, \lfloor \frac{(g-2)}{r} \rfloor - 1 \right) & \text{if} \quad r \leq \frac{g-2}{2} \text{ and } B_r \geq q^r; \end{cases}.$$

Note that the estimate of Theorem 1.7 is completely effective in contrast to that of Theorem 1.6 for which the computation of the $\mathcal{O}$ constants is far from straightforward. Next, we obtain as direct consequence of Theorems 4.9 and 4.10 the following asymptotical result announced in [2]:

Theorem 1.8. *Let $\mathcal{F}/\mathbb{F}_q = (F_k/\mathbb{F}_q)_k$ be a sequence of algebraic functions fields defined over a finite field $\mathbb{F}_q$ and $\mathcal{G}/\mathbb{F}_{q^r} = (G_k/\mathbb{F}_q)_k$ be the sequence of functions fields over $\mathbb{F}_{q^r}$ obtained from $\mathcal{F}/\mathbb{F}_q$ by constant field extension. Set g_k the genus of F_k, $h(F_k/\mathbb{F}_q)$ the class number of $F_k/\mathbb{F}_q$ and $B_i(F_k/\mathbb{F}_q)$ the number of places of degree i of $F_k/\mathbb{F}_q$. Suppose for any integer k, $B_1(F_k/\mathbb{F}_q) \geq 1$.*

Let $\alpha > 0$ be a real number. Suppose there exists an integer $r \geq 1$ such that one of two following conditions is satisfied:

(1) $\liminf_{k\to\infty} \frac{B_r(F_k/\mathbb{F}_q)}{g_k} = \mu_r(\mathcal{F}/\mathbb{F}_q) > \alpha$.

(2) $\frac{1}{r} \liminf_{k\to\infty} \sum_{i|r} \frac{iB_i(F_k/\mathbb{F}_q)}{g_k} = \frac{1}{r}\mu_1(\mathcal{G}/\mathbb{F}_{q^r}) > \alpha$.

Then

$$h(F_k/\mathbb{F}_q) \geq C \left(\left(\frac{q^r}{q^r - 1} \right)^{\alpha} q \right)^{g_k},$$

where $C > 0$ is a constant with respect to k.

This asymptotical lower bound of the class number of a sequence of algebraic functions fields could be possibly obtained without the assumption of a "asymptotically exact sequence" from the sophisticated proof of Theorem 1.4 of Tsfasman [12, Corollary 2] by using the lower limit instead of the assumption "asymptotically exact". We give here a completely different proof based upon elementary combinatorial considerations. Moreover, we extend Theorem 1.3 by using points of degree r and assuming only that $\frac{B_r(k)}{g_k}$ has a strictly positive lower limit, where $B_r(k)$ is the number of places of degree r of F_k; in particular this shows that the lower bound 1 of Theorem 1.5 can be widely improved if there is at least a place of degree 1 in each F_k and an integer $r \geq 1$ such that $\liminf_{k \to +\infty} \frac{B_r(k)}{g_k} > 0$.

1.2.2. *Details and methods.* We remark that Theorems 1.1 and 1.2 in the non-asymptotic case and Theorem 1.3 in the asymptotic case involve rational points of the curve. But in many cases the number of rational points is low while the number of places of a certain degree r is large. Then it may be interesting to give formulas that are based on the number of points of degree $r \geq 1$. This is the main idea of the article, even if the formula applied with $r = 1$ gives in many cases better lower bounds for the class number than Theorems 1.1 and 1.2.

In this paper we give lower bounds on the class number of an algebraic function field of one variable over the finite field $\mathbb{F}_q$ in the two following situations:

- in the non-asymptotic case, namely when the function field is fixed; in this context, we extend the formulas of Theorem 1.1 which is given under very weak assumptions, to obtain more precise bounds taking into account the number of points of a given degree $r \geq 1$, possibly of degree one.

- in the asymptotic case, where we consider a sequence of function fields F_k of genus g_k growing to infinity.

Let $A_n = A_n(F/\mathbb{F}_q)$ be the number of effective divisors of degree n of an algebraic function field $F/\mathbb{F}_q$ defined over $\mathbb{F}_q$ of genus $g \geq 2$ and $h = h(F/\mathbb{F}_q)$ the class number of $F/\mathbb{F}_q$. Let $B_n = B_n(F/\mathbb{F}_q)$ the number of places of degree n of $F/\mathbb{F}_q$.

Let us set

$$S(F/\mathbb{F}_q) = \sum_{n=0}^{g-1} A_n + \sum_{n=0}^{g-2} q^{g-1-n} A_n \quad \text{and} \quad R(F/\mathbb{F}_q) = \sum_{i=1}^{g} \frac{1}{\mid 1 - \pi_i \mid^2},$$

where $(\pi_i, \overline{\pi_i})_{1 \leq i \leq g}$ are the reciprocal roots of the numerator of the zeta-function $Z(F/\mathbb{F}_q, T)$ of $F/\mathbb{F}_q$. By a result due to G. Lachaud and M. Martin-Deschamps [8], we know that

$$S(F/\mathbb{F}_q) = hR(F/\mathbb{F}_q). \tag{1.1}$$

Therefore, to find good lower bounds on h, just find a good lower bound on $S(F/\mathbb{F}_q)$ and a good upper bound on $R(F/\mathbb{F}_q)$.

It is known by [8] that the quantity $R(F/\mathbb{F}_q)$ is bounded by the following upper bound:

$$R(F/\mathbb{F}_q) \leq \frac{g}{(\sqrt{q}-1)^2}, \tag{1.2}$$

or with this best inequality:

$$R(F/\mathbb{F}_q) \leq \frac{1}{(q-1)^2}\left((g+1)(q+1) - B_1(F/\mathbb{F}_q)\right). \tag{1.3}$$

Moreover, the inequality (1.3) is obtained as follows:

$$R(F/\mathbb{F}_q) = \sum_{i=1}^{g} \frac{1}{(1-\pi_i)(1-\overline{\pi_i})} = \sum_{i=1}^{g} \frac{1}{1+q-(\pi_i+\overline{\pi_i})}.$$

Multiplying the denominators by the corresponding conjugated quantities, we get:

$$R(F/\mathbb{F}_q) \leq \frac{1}{(q-1)^2}\sum_{i=1}^{g}(1+q+\pi_i+\overline{\pi_i}).$$

This last inequality associated to the following formula deduced from the Weil's formulas:

$$\sum_{i=1}^{g}(\pi_i+\overline{\pi_i}) = 1+q-B_1(F/\mathbb{F}_q)$$

gives the inequality (1.3). This inequality cannot be improved in the general case.

Hence, in this paper, we propose to study some lower bounds on $S(F/\mathbb{F}_q)$. In this aim, we determine some lower bounds on the number of effective divisors of degree $n \leq g-1$ obtained from the number of effective divisors of degree $n \leq g-1$ containing in their support a maximum number of places of a fixed degree $r \geq 1$. We deduce lower bounds on the class number. It is a successful strategy that allows us to improve the known lower bounds on h in the general case (except if there is no place of degree one). It also allows us to obtain the best known asymptotics for h when we specialize our study to some families of curves having asymptotically a large number of places of degree r for some value of r, namely when $\liminf_{g\rightarrow+\infty} \frac{B_r(g)}{g} > 0$.

1.3. Organization of the paper. In Section 2 we study the number of effective divisors of an algebraic function field over the finite field $\mathbb{F}_q$. As we saw in the introduction, this is the main point to estimate the class number. By combinatorial considerations, we give a lower bound on the number of these divisors. Then we estimate the two terms $\Sigma_1 = \sum_{n=0}^{g-1} A_n$ and $\Sigma_2 = \sum_{n=0}^{g-2} q^{g-1-n} A_n$ of the number $S(F/\mathbb{F}_q)$ introduced in Paragraph 1.2. Then, in Sections 3 and 4, we deduce lower bounds on the class number and asymptotical class number, respectively. The final section 5 presents several examples where we obtain asymptotical lower bounds on the class number.

2. Lower bounds on the number of effective divisors

In this section, we obtain a lower bound on the number of effective divisors of degree $\leq g-1$. We derive a lower bounds on $S(F/\mathbb{F}_q)$.

Let $B_r(F/\mathbb{F}_q)$ be the number of places of degree r. In the first time, we determine lower bounds on the number of effective divisors of degree $\leq g-1$.

By definition, we have $S(F/\mathbb{F}_q) = \sum_{n=0}^{g-1} A_n + \sum_{n=0}^{g-2} q^{g-1-n} A_n$. We will denote by Σ_1 the first sum of the right member and Σ_2 the second one:

$$\Sigma_1 = \sum_{n=0}^{g-1} A_n \quad \text{and} \quad \Sigma_2 = \sum_{n=0}^{g-2} q^{g-1-n} A_n. \tag{2.1}$$

Let us fix a degree n and set

$$U_n = \left\{ b = (b_1, \cdots, b_n) \mid b_i \geq 0 \text{ et } \sum_{i=1}^{n} i b_i = n \right\}.$$

Note first that if $B_i \geq 1$ and $b_i \geq 0$, the number of solutions of the equation $n_1 + n_2 + \cdots + n_{B_i} = b_i$ with integers ≥ 0 is:

$$\binom{B_i + b_i - 1}{b_i}. \tag{2.2}$$

Then the number of effective divisors of degree n is given by the following result, already mentioned in [13]:

Proposition 2.1. *The number of effective divisors of degree n of an algebraic function field $F/\mathbb{F}_q$ is:*

$$A_n = \sum_{b \in U_n} \left[\prod_{i=1}^{n} \binom{B_i + b_i - 1}{b_i} \right].$$

Proof. It is sufficient to consider that in the formula, b_i is the sum of coefficients that are applied to the places of degree i. So, the sum of the terms ib_i is the degree n of the divisor. The number of ways to get a divisor of degree ib_i with some places of degre i is given by the binomial coefficient (2.2). For a given b , the product of the second member is the number of effective divisors for which the weight corresponding to the places of degree i is ib_i. Then it remains to compute the sum over all possible b to get the number of effective divisors. □

From Proposition 2.1 we obtain in the next proposition a lower bound on the number of effective divisors of degree $n \leq g-1$. This lower bound is constructed using only places of degree 1 and r (possibly 1) as follows: the weight associated to places of degree r is maximum, namely $\lfloor \frac{n}{r} \rfloor$. The weight associated to places of degree 1 is $n \mod r$.

Proposition 2.2. *Let r and n be two integers > 0. Suppose that B_1 and B_r are different from zero. Then*

$$A_n \geq \binom{B_r + m_r(n) - 1}{B_r - 1} \binom{B_1 + s_r(n) - 1}{B_1 - 1} \tag{2.3}$$

where $m_r(n)$ and $s_r(n)$ are respectively the quotient and the remainder of the Euclidian division of n by r.

Proof. Let $a = (a_i)_{1 \leq i \leq n}$ be the following element of U_n:

$$a = (s_r(n), 0, \cdots 0, m_r(n), 0, \cdots, 0).$$

Then by Proposition (2.1), we have:

$$\begin{aligned} A_n &= \sum_{b \in U_n} \prod_{i=1}^{n} \binom{B_i + b_i - 1}{b_i} \\ &\geq \prod_{i=1}^{n} \binom{B_i + a_i - 1}{a_i} \\ &= \binom{B_r + m_r(n) - 1}{B_r - 1} \binom{B_1 + s_r(n) - 1}{B_1 - 1}. \end{aligned}$$

□

In particular, if $r = 1$ we obtain: $A_n \geq \binom{B_1 + n - 1}{n} = \binom{B_1 + n - 1}{B_1 - 1}$.

2.1. Lower bound on the sum Σ_1. By using the same lower bound for each term A_n as in Proposition 2.2, then by associating the r indexes n with the same $m_r(n)$, we obtain:

$$\begin{aligned} \Sigma_1 \geq &\sum_{m=0}^{m_r(g-1)-1} \left(\sum_{i=0}^{r-1} \binom{B_1 + i - 1}{B_1 - 1} \right) \binom{B_r + m - 1}{B_r - 1} \\ &+ \binom{B_r + m_r(g-1) - 1}{B_r - 1} \sum_{i=0}^{s_r(g-1)} \binom{B_1 + i - 1}{B_1 - 1} \end{aligned} \tag{2.4}$$

which gives the following lemma:

Lemma 2.3. *Suppose $B_1 > 0$ and $B_r > 0$, then we have the following lower bound on the sum $\Sigma_1 = \sum_{n=0}^{g-1} A_n$:*

$$\Sigma_1 \geq K_1(r-1, B_1) \binom{B_r + m_r(g-1) - 1}{B_r} + K_1\left(s_r(g-1), B_1\right) \binom{B_r + m_r(g-1) - 1}{B_r - 1} \tag{2.5}$$

where

$$K_1(i, B) = \binom{B+i}{B}.$$

Proof. It is sufficient to apply three times to the second member of the inequality (2.4) the following combinational formula: for all the integers k and l,

$$\sum_{j=0}^{l} \binom{k+j}{k} = \binom{k+l+1}{k+1}.$$

We obtain

$$\Sigma_1 = \sum_{n=0}^{g-1} A_n \geq \binom{B_1 + r - 1}{B_1} \binom{B_r + m_r(g-1) - 1}{B_r} + \binom{B_r + m_r(g-1) - 1}{B_r - 1} \binom{B_1 + s_r(g-1)}{B_1}.$$

□

Remark 2.4. Note that for any $B_1 \geq 1$ we have $K_1(r-1, B_1) \geq B_1 + r - 1$, the value r being reached for $B_1 = 1$.

Remark 2.5. If $r = 1$ then

$$m_r(n) = n,\ s_r(n) = 0,\ K_1(r-1, B_1) = 1,\ K_1\left(s_r(g-1), B_1\right) = 1.$$

We conclude in this case that:

$$\Sigma_1 = \sum_{n=0}^{g-1} A_n \geq \binom{B_1 + g - 1}{B_1} = \binom{B_1 + g - 1}{g-1} = K_1(g-1, B_1).$$

2.2. Lower bound on the sum Σ_2. Now let us study the second sum: $\Sigma_2 = q^{g-1} \sum_{n=0}^{g-2} \frac{A_n}{q^n}$. We have:

$$\Sigma_2 \geq q^{g-1} \left(\sum_{i=0}^{r-1} \frac{1}{q^i} \binom{B_1 + i - 1}{B_1 - 1} \right) \sum_{m=0}^{m_r(g-2)-1} \frac{1}{q^{mr}} \binom{B_r + m - 1}{B_r - 1} + q^{s_r(g-2)+1} \binom{B_r + m_r(g-2) - 1}{B_r - 1} \sum_{i=0}^{s_r(g-2)} \frac{1}{q^i} \binom{B_1 + i - 1}{B_1 - 1}. \tag{2.6}$$

In order to give a lower bound on Σ_2, we need to study more precisely the following quantity Q_r which occurs in the previous inequality (2.6):

$$Q_r = \sum_{m=0}^{m_r(g-2)-1} \frac{1}{(q^r)^m} \begin{pmatrix} B_r + m - 1 \\ B_r - 1 \end{pmatrix}.$$

Remark 2.6. For $g = 2$ and $g = 3$, we have respectively $Q_r = 0$ and $Q_r = 1$.

The value Q_r depends on the parameters q, g, r and B_r. We give several lower bounds whose accuracy depends on the ranges in which the parameters vary. These lower bounds are specified in the following three lemmas. Then we can suppose in the study of Q_r that $g > 3$.

Lemma 2.7. *Let q and r be two integers > 0 and let $g > 3$ be an integer. Suppose that $B_1 \geq 1$ and $B_r \geq 1$. Let Q_r be the sum defined by:*

$$Q_r = \sum_{m=0}^{m_r(g-2)-1} \frac{1}{(q^r)^m} \begin{pmatrix} B_r + m - 1 \\ B_r - 1 \end{pmatrix},$$

where $m_r(n)$ denotes the quotient of the Euclidian division of n by r. Let us set

$$f_r = \begin{cases} 0 & \text{if} \quad \frac{g-2}{2} < r \leq g-2; \\ 1 & \text{if} \quad r \leq \frac{g-2}{2} \text{ and } B_r < q^r; \\ \min\left(\lfloor \frac{B_r - q^r}{q^r - 1} \rfloor + 1, m_r(g-2) - 1\right) & \text{if} \quad r \leq \frac{g-2}{2} \text{ and } B_r \geq q^r; \end{cases}$$

then

$$Q_r \geq \frac{q^{rm_r(g-2)} - 1}{q^{r(m_r(g-2)-1)}(q^r - 1)} + \frac{(B_r - 1)}{q^r} f_r.$$

Proof. Let us write

$$Q_r = \sum_{m=0}^{m_r(g-2)-1} \frac{1}{(q^r)^m} + \Delta_r,$$

where

$$\Delta_r = \sum_{m=0}^{m_r(g-2)-1} \frac{1}{(q^r)^m} \left[\begin{pmatrix} B_r + m - 1 \\ B_r - 1 \end{pmatrix} - 1 \right].$$

Then

$$Q_r = \frac{q^{rm_r(g-2)} - 1}{q^{r(m_r(g-2)-1)}(q^r - 1)} + \Delta_r.$$

First, if $\frac{g-2}{2} < r \leq g-2$ then $m_r(g-2) = 1$, hence $\Delta_r = 0$. Let us suppose now that $r \leq \frac{g-2}{2}$, then $m_r(g-2) \geq 2$. Hence, the sum Δ_r has at least two terms, namely 0 (for $m=0$) and $\frac{1}{q^r}(B_r-1)$ (for $m=1$). Let us set for any $n\geq 0$:

$$u_n=\frac{1}{q^{rn}}\left(\begin{array}{c}B_r+n-1\\ B_r-1\end{array}\right),$$

and compute:

$$\frac{u_{n+1}}{u_n}=\frac{1}{q^r}\frac{B_r+n}{n+1}.$$

Let us set $n_0=\lfloor\frac{B_r-q^r}{q^r-1}\rfloor+1$. Then, if $0\leq n<n_0$, we have $u_{n+1}\geq u_n$ and then $u_{n+1}-\frac{1}{q^{r(n+1)}}\geq u_n-\frac{1}{q^{rn}}$. If $B_r<q^r$, then $n_0\leq 1$. Let us give in this case a lower bound on the sum Δ_r by considering only the sum of the two first terms i.e $(B_r-1)/q^r$. If $B_r\geq q^r$, then $n_0\geq 1$. If we set $f_r=\min\left(n_0, m_r(g-2)-1\right)$, the sequence $u_n-\frac{1}{q^{rn}}$ is increasing from the term of index 1 (which is equal to $(B_r-1)/q^r$) until the term of index f_r. Hence

$$\Delta_r\geq\frac{(B_r-1)}{q^r}f_r.$$

□

Remark 2.8. Note that when the genus g is growing to infinity and when $B_r>q^r$, then $f_r=\left\lfloor\frac{B_r-q^r}{q^r-1}\right\rfloor+1$ for g sufficiently large, by the Drinfeld-Vladut bound.

Lemma 2.9. *Let q and r be two integers >0 and let $g>3$ be an integer. Suppose that $B_1\geq 1$ and $B_r\geq 1$. Let Q_r be the sum defined by:*

$$Q_r=\sum_{m=0}^{m_r(g-2)-1}\frac{1}{(q^r)^m}\left(\begin{array}{c}B_r+m-1\\ B_r-1\end{array}\right),$$

where $m_r(n)$ denotes the quotient of the Euclidian division of n by r. We have the following lower bound

$$Q_r\geq\begin{cases}1 & \text{if } r>\frac{g-2}{2},\\ \left(\frac{q^r}{q^r-1}\right)^{B_r-1} & \text{if } B_r\leq m_r(g-2),\\ \left(1+\frac{B_r}{q^r(m_r(g-2)-1)}\right)^{m_r(g-2)-1} & \text{if } B_r>m_r(g-2) \text{ and } r\leq\frac{g-2}{2}.\end{cases}$$

Proof. Let N and k be two integers such that $N\geq k\geq 0$. Let us study the following sum:

$$Q(N,k,x)=\sum_{i=0}^{N-k}\left(\begin{array}{c}k+i\\ k\end{array}\right)x^i. \tag{2.7}$$

By derivating k times the classical equality

$$\sum_{i=0}^{N}x^i=\frac{1-x^{N+1}}{1-x},$$

the following formula holds:

$$Q(N,k,x) = \frac{1}{(1-x)^{k+1}} - \frac{x^{N-k+1}}{1-x} \sum_{i=0}^{k} \binom{N+1}{k-i} \left(\frac{x}{1-x}\right)^{i}. \tag{2.8}$$

Let us set $j = N+1-k+i$ in the previous formula, then

$$Q(N,k,x) = \frac{1}{(1-x)^{k+1}} - (1-x)^{N-k} \sum_{j=N+1-k}^{N+1} \binom{N+1}{j} \left(\frac{x}{1-x}\right)^{j}.$$

Then

$$\begin{aligned} Q(N,k,x) = \frac{1}{(1-x)^{k+1}} &- (1-x)^{N-k} \sum_{j=0}^{N+1} \binom{N+1}{j} \left(\frac{x}{1-x}\right)^{j} \\ &+ (1-x)^{N-k} \sum_{j=0}^{N-k} \binom{N+1}{j} \left(\frac{x}{1-x}\right)^{j}, \end{aligned}$$

$$\begin{aligned} Q(N,k,x) = \frac{1}{(1-x)^{k+1}} &- (1-x)^{N-k} \left(1 + \frac{x}{1-x}\right)^{N+1} \\ &+ (1-x)^{N-k} \sum_{j=0}^{N-k} \binom{N+1}{j} \left(\frac{x}{1-x}\right)^{j}, \end{aligned}$$

$$Q(N,k,x) = (1-x)^{N-k} \sum_{j=0}^{N-k} \binom{N+1}{j} \left(\frac{x}{1-x}\right)^{j}. \tag{2.9}$$

Let us remark that $Q_r = Q\left(m_r(g-2) + B_r - 2, B_r - 1, 1/q^r\right)$. From Formula (2.9) we obtain

$$Q_r = \left(\frac{q^r-1}{q^r}\right)^{m_r(g-2)-1} \left(\sum_{j=0}^{m_r(g-2)-1} \binom{m_r(g-2)+B_r-1}{j} \left(\frac{1}{q^r-1}\right)^{j} \right).$$

If $B_r \leq m_r(g-2)$ then $m_r(g-2) \geq \frac{1}{2}\left(m_r(g-2) + B_r\right)$. Let us set

$$s = \left\lfloor \frac{1}{2}\left(m_r(g-2) + B_r - 1\right) \right\rfloor.$$

Let us remark that

$$\sum_{j=0}^{s} \binom{m_r(g-2)+B_r-1}{j} \left(\frac{1}{q^r-1}\right)^j + \left(\frac{1}{q^r-1}\right) \left(\sum_{j=s+1}^{m_r(g-2)+B_r-1} \binom{m_r(g-2)+B_r-1}{j} \left(\frac{1}{q^r-1}\right)^{j-1} \right) = \left(\frac{q^r}{q^r-1}\right)^{m_r(g-2)+B_r-1}.$$

But

$$\sum_{j=0}^{s} \binom{m_r(g-2)+B_r-1}{j} \left(\frac{1}{q^r-1}\right)^j \geq \sum_{s+1}^{m_r(g-2)+B_r-1} \binom{m_r(g-2)+B_r-1}{j} \left(\frac{1}{q^r-1}\right)^{j-1}.$$

Then

$$\sum_{j=0}^{s} \binom{m_r(g-2)+B_r-1}{j} \left(\frac{1}{q^r-1}\right)^j \geq \frac{q^r-1}{q^r} \left(\frac{q^r}{q^r-1}\right)^{m_r(g-2)+B_r-1}.$$

Therefore

$$\begin{aligned} Q_r &\geq \left(\frac{q^r-1}{q^r}\right)^{m_r(g-2)-1} \frac{q^r-1}{q^r} \left(\frac{q^r}{q^r-1}\right)^{m_r(g-2)+B_r-1} \\ &\geq \left(\frac{q^r}{q^r-1}\right)^{B_r-1}. \end{aligned}$$

If $B_r > m_r(g-2)$, then

$$\frac{\binom{m_r(g-2)+B_r-1}{j}}{\binom{m_r(g-2)-1}{j}} = \prod_{i=0}^{j-1} \frac{m_r(g-2)+B_r-1-i}{m_r(g-2)-1-i} \geq \left(\frac{m_r(g-2)+B_r-1}{m_r(g-2)-1}\right)^j.$$

Then

$$\sum_{j=0}^{m_r(g-2)-1} \binom{m_r(g-2)+B_r-1}{j} \left(\frac{1}{q^r-1}\right)^j$$
$$\geq \sum_{j=0}^{m_r(g-2)-1} \binom{m_r(g-2)-1}{j} \left[\left(\frac{1}{q^r-1}\right)\left(\frac{m_r(g-2)+B_r-1}{m_r(g-2)-1}\right)\right]^j$$
$$\geq \left(1+\frac{m_r(g-2)+B_r-1}{(q^r-1)(m_r(g-2)-1)}\right)^{m_r(g-2)-1}.$$

Therefore

$$Q_r \geq \left(\frac{q^r-1}{q^r}\right)^{m_r(g-2)-1} \left(1+\frac{m_r(g-2)+B_r-1}{(q^r-1)(m_r(g-2)-1)}\right)^{m_r(g-2)-1}$$
$$\geq \left(1+\frac{B_r}{q^r(m_r(g-2)-1)}\right)^{m_r(g-2)-1}.$$

□

Lemma 2.10. *Let q and r be two integers >0 and let $g>3$ be an integer. Suppose that $B_1 \geq 1$ and $B_r \geq 1$. Let Q_r be the sum defined by:*

$$Q_r = \sum_{m=0}^{m_r(g-2)-1} \frac{1}{(q^r)^m} \binom{B_r+m-1}{B_r-1},$$

where $m_r(n)$ denotes the quotient of the Euclidian division of n by r. If $B_r+1 \leq (m_r(g-2)-1)(q^r-1)$ we get the following lower bound

$$Q_r \geq \left(\frac{q^r}{q^r-1}\right)^{B_r} - B_r \binom{B_r+m_r(g-2)-1}{B_r} \left(\frac{1}{q^r}\right)^{m_r(g-2)}.$$

Proof. The term $\left(\frac{q^r}{q^r-1}\right)^{B_r}$ is the value of the infinite sum

$$\sum_{m=0}^{\infty} \frac{1}{(q^r)^m} \binom{B_r+m-1}{B_r-1}.$$

As proved later in Lemma 4.2 the term

$$B_r \binom{B_r+m_r(g-2)-1}{B_r} \left(\frac{1}{q^r}\right)^{m_r(g-2)}$$

is an upper bound of the remainder. □

3. Lower bounds on the class number

In this section, using the lower bounds obtained in the previous section, we derive lower bounds on the class number $h = h(F/\mathbb{F}_q)$ of an algebraic function field $F/\mathbb{F}_q$. Let $B_r = B_r(F/\mathbb{F}_q)$ be the number of places of degree r.

Theorem 3.1. *Let $F/\mathbb{F}_q$ be an algebraic function field defined over $\mathbb{F}_q$ of genus $g \geq 2$ and h the class number of $F/\mathbb{F}_q$. Suppose that the numbers B_1 and B_r of places of degree respectively 1 and r are such that $B_1 \geq 1$ and $B_r \geq 1$. Let us denote by $K_1(i,B)$ and $K_2(q,j,B)$ the following numbers:*

$$K_1(i,B) = \binom{B+i}{B} \quad \textit{and} \quad K_2(q,j,B) = \sum_{i=0}^{j} \frac{1}{q^i} \binom{B+i-1}{B-1}.$$

Then, the following inequality holds:

$$\begin{aligned}
h \geq\ & \frac{(q-1)^2 K_2(q,r-1,B_1)}{(g+1)(q+1)-B_1} q^{g-1} Q_r \\
&+ \frac{q(q-1)^2 K_2\left(q, s_r(g-2), B_1\right)}{(g+1)(q+1)-B_1} \binom{B_r + m_r(g-2)-1}{B_r-1} \\
&+ \frac{(q-1)^2 K_1(r-1,B_1)}{(g+1)(q+1)-B_1} \binom{B_r + m_r(g-1)-1}{B_r} \\
&+ \frac{(q-1)^2 K_1\left(s_r(g-1), B_1\right)}{(g+1)(q+1)-B_1} \binom{B_r + m_r(g-1)-1}{B_r-1}
\end{aligned} \tag{3.1}$$

where Q_r can be bounded by any of the three lemmas 2.7, 2.9 and 2.10.

Proof. The result is a direct consequence of the equality (1.1) which gives an expression of h, the upper bound (1.3), the lower bound (2.5) and Lemmas 2.7, 2.9 and 2.10. Remark that for $g = 2$ and $g = 3$, we have respectively $Q_r = 0$ and $Q_r = 1$ (cf. Remark 2.6). □

Let us give some simplified formulas which are slightly less accurate but more readable. Note that these simplified formulas are not interesting for $g = 2$, hence we have:

Corollary 3.2. *Let $F/\mathbb{F}_q$ be an algebraic function field defined over $\mathbb{F}_q$ of genus $g \geq 3$ and h the class number of $F/\mathbb{F}_q$. Suppose that the numbers B_1 and B_r of places of degree respectively 1 and r are such that $B_1 \geq 1$ and $B_r \geq 1$. Then the following four results hold:*

(1) *Let us set*

$$f_r = \begin{cases} 0 & \textit{if} \quad \frac{g-2}{2} < r \leq g-2; \\ 1 & \textit{if} \quad r \leq \frac{g-2}{2} \textit{ and } B_r < q^r; \\ \min\left(\lfloor \frac{B_r - q^r}{q^r-1} \rfloor + 1, m_r(g-2)-1\right) & \textit{if} \quad r \leq \frac{g-2}{2} \textit{ and } B_r \geq q^r; \end{cases}$$

then

$$h \geq \frac{(q-1)^2}{(g+1)(q+1)} q^{g-1} \left(\frac{q^{rm_r(g-2)}-1}{q^{r(m_r(g-2)-1)}(q^r-1)} + \frac{(B_r-1)}{q^r} f_r \right);$$

(2) *if* $B_r \leq m_r(g-2)$ *then*

$$h \geq \frac{(q-1)^2}{(g+1)(q+1)} q^{g-1} \left(\frac{q^r}{q^r-1} \right)^{B_r-1};$$

(3) *if* $B_r > m_r(g-2)$ *and* $r \leq \frac{g-2}{2}$ *then*

$$h \geq \frac{(q-1)^2}{(g+1)(q+1)} q^{g-1} \left(1 + \frac{B_r}{q^r(m_r(g-2)-1)} \right)^{m_r(g-2)-1};$$

(4) *if* $B_r + 1 \leq (m_r(g-2)-1)(q^r-1)$ *then*

$$h \geq \frac{(q-1)^2}{(g+1)(q+1)} q^{g-1} \left[\left(\frac{q^r}{q^r-1} \right)^{B_r} - B_r \binom{B_r + m_r(g-2) - 1}{B_r} \left(\frac{1}{q^r} \right)^{m_r(g-2)} \right].$$

Remark 3.3. If we set $L_1 = q^{g-1} \frac{(q-1)^2}{(q+1)(g+1)-B_1}$ which corresponds, to the first lower bound on h given in [8, Theorem 2] and if we denote by L'_r the bound (3.1), then

$$\begin{aligned} L'_r = {} & K_2(q, r-1, B_1)\, Q_r L_1 \\ & + \frac{q(q-1)^2 K_2\left(q, s_r(g-2), B_1\right)}{(g+1)(q+1)-B_1} \binom{B_r + m_r(g-2) - 1}{B_r - 1} \\ & + \frac{(q-1)^2 K_1(r-1, B_1)}{(g+1)(q+1)-B_1} \binom{B_r + m_r(g-1) - 1}{B_r} \\ & + \frac{(q-1)^2 K_1(s_r(g-1), B_1)}{(g+1)(q+1)-B_1} \binom{B_r + m_r(g-1) - 1}{B_r - 1}, \end{aligned}$$

which gives in the case $r = 1$ and if we choose the lower bound on Q_r given by Lemma 2.7:

$$\begin{aligned} L'_1 = {} & \left(\frac{q^{g-2}-1}{q^{g-3}(q-1)} + \frac{(B_1-1) f_1}{q} \right) L_1 \\ & + \frac{q(q-1)^2}{(g+1)(q+1)-B_1} \binom{B_1 + g - 3}{B_1 - 1} \\ & + \frac{(q-1)^2}{(g+1)(q+1)-B_1} \binom{B_1 + g - 1}{B_1}. \end{aligned}$$

Remark 3.4. Let us remark that in [8, Theorem 2] Lachaud - Martin-Deschamps study the worst case (see also Theorem 1.1). In the worst case $r = 1$, $B_1 = 1$ and $g \geq 2$ (third bound given in [8, Theorem 2]) we obtain the same lower bound. More precisely, if we denote by L_3 the third bound in [8, Theorem 2]), namely

$$L_3 = (q^g - 1)\frac{q-1}{q+g+qg},$$

then our bound L_1' obtained using the lower bound of Q_r given by Lemma 2.7 satisfies the following inequality:

$$L_1' \geq L_3 + \frac{(q-1)^2 q^{g-1}}{q+g+gq}\,\frac{B_1 - 1}{q}\,f_1.$$

4. Asymptotical bounds with respect to the genus g

We now give asymptotical bounds on the class number of certain sequences of algebraic function fields defined over a finite field when g tends to infinity and when there exists an integer r such that:

$$\liminf_{k\to+\infty} \frac{B_r(F_k/\mathbb{F}_q)}{g(F_k)} > 0.$$

We consider a sequence of function fields $F_k/\mathbb{F}_q$ defined over the finite field $\mathbb{F}_q$. Let us denote by g_k the genus of F_k and by $B_r(k)$ the number of places of degree r of F_k. We suppose that the sequence g_k is growing to infinity and that for a certain r the following holds:

$$\liminf_{k\to+\infty} \frac{B_r(k)}{g_k} = \mu_r > 0.$$

We also assume that $B_1(k) \geq 1$ for any k.

Let us denote by $m_r(x)$ the Euclidean quotient of x by r. Let a and b be two constant integers and let η be any given number such that $0 < \eta < 1$. Then there is an integer $k_0 > 0$ such that for any integer $k \geq k_0$ the following inequalities hold:

$$\mu_r g_k(1-\eta) < B_r(k) < \frac{g_k}{r}\left(q^{\frac{r}{2}} - 1\right)(1+\eta). \tag{4.1}$$

$$\frac{g_k}{r}(1-\eta) < m_r(g_k - a) - b < \frac{g_k}{r}(1+\eta). \tag{4.2}$$

We study the asymptotic behaviour of the binomial coefficient

$$\binom{B_r(k) + m_r(g_k - a) - b}{B_r(k)},$$

and for this purpose we do the following:

(1) we use the generalized binomial coefficients (defined for example with the Gamma function);

(2) we remark that if u and v are positive real numbers and if $u' \geq u$ and $v' \geq v$, then the following inequality between generalized binomial coefficients holds:

$$\binom{u'+v'}{u'} \geq \binom{u+v}{u};$$

(3) we use the Stirling formula.

So, we obtain:

Lemma 4.1. *For any real numbers ϵ, η such that $\epsilon > 0$ and $0 < \eta < 1$, there exists an integer k_1 such that for any integer $k \geq k_1$ the following holds:*

$$(1-\epsilon)\frac{C_1}{\sqrt{g_k}} q_1^{g_k} < \binom{B_r(k) + m_r(g_k - a) - b}{B_r(k)} < (1+\epsilon)\frac{C_2}{\sqrt{g_k}} q_2^{g_k}, \tag{4.3}$$

where

$$C_1 = \sqrt{\frac{r\mu_r + 1}{2\pi r \mu_r (1-\eta)}}$$

and

$$C_2 = \sqrt{\frac{q^{\frac{r}{2}}}{2\pi(q^{\frac{r}{2}} - 1)(1+\eta)}}$$

are two positive constants depending upon η and where

$$q_1 = \left(\frac{\left(\mu_r + \frac{1}{r}\right)^{\mu_r + \frac{1}{r}}}{\mu_r^{\mu_r} \left(\frac{1}{r}\right)^{\frac{1}{r}}} \right)^{1-\eta}$$

and

$$q_2 = \left(\left(\frac{q^{\frac{r}{2}}}{q^{\frac{r}{2}} - 1} \right)^{\frac{1}{r}(q^{\frac{r}{2}} - 1)} \sqrt{q} \right)^{1+\eta}.$$

Proof. By the previous remark we know that:

$$\binom{g_k(1-\eta)\left(\mu_r + \frac{1}{r}\right)}{g_k(1-\eta)\mu_r} \leq \binom{B_r(k) + m_r(g_k - a) - b}{B_r(k)}$$
$$\leq \binom{\frac{g_k}{r} q^{\frac{r}{2}}(1+\eta)}{\frac{g_k}{r}\left(q^{\frac{r}{2}} - 1\right)(1+\eta)}.$$

Using the Stirling formula we get

$$\left(\begin{array}{c} g_k(1-\eta)\left(\mu_r+\frac{1}{r}\right) \\ g_k(1-\eta)\mu_r \end{array}\right) \underset{k\to+\infty}{\sim} \frac{C_1}{\sqrt{g_k}}\left(\left(\frac{\left(\mu_r+\frac{1}{r}\right)^{\mu_r+\frac{1}{r}}}{\mu_r^{\mu_r}\left(\frac{1}{r}\right)^{\frac{1}{r}}}\right)^{1-\eta}\right)^{g_k}$$

and

$$\left(\begin{array}{c} \frac{g_k}{r}q^{\frac{r}{2}}(1+\eta) \\ \frac{g_k}{r}\left(q^{\frac{r}{2}}-1\right)(1+\eta) \end{array}\right) \underset{k\to+\infty}{\sim} \frac{C_2}{\sqrt{g_k}}\left(\left(\left(\frac{q^{\frac{r}{2}}}{q^{\frac{r}{2}}-1}\right)^{\frac{1}{r}(q^{\frac{r}{2}}-1)}\sqrt{q}\right)^{1+\eta}\right)^{g_k}.$$

$\square$

Let us recall that for evaluating asymptotically the class number h_k, we need to evaluate asymptotically the sums $\Sigma_1(k)$ and $\Sigma_2(k)$, respectively defined by the formulas (2.5) and (2.6), with respect to the parameter k.

4.1. Asymptotical lower bound on $\boldsymbol{\Sigma_2(k)}$. First, let us consider the sum

$$\Sigma_2(k) = q^{g_k-1}\sum_{n=0}^{g_k-2}\frac{A_n}{q^n} \geq q^{g_k-1}K_2\left(q,r-1,B_1(k)\right)Q_r(k),$$

where

$$K_2\left(q,r-1,B_1(k)\right) = \sum_{i=0}^{r-1}\frac{1}{q^i}\left(\begin{array}{c} B_1(k)+i-1 \\ B_1(k)-1 \end{array}\right)$$

and

$$Q_r(k) = \sum_{n=0}^{m_r(g_k-2)-1}\frac{1}{q^{nr}}\left(\begin{array}{c} B_r(k)+n-1 \\ B_r(k)-1 \end{array}\right).$$

For evaluating asymptotically the sum $\Sigma_2(k)$, we have to evaluate asymptotically $Q_r(k)$. Let us set

$$T_r(X,k) = \sum_{n=0}^{M_r(k)}\left(\begin{array}{c} B_r(k)+n-1 \\ B_r(k)-1 \end{array}\right)X^n,$$

where $M_r(k) = m_r(g_k-2)-1$, then

$$Q_r(k) = T_r\left(\frac{1}{q^r},k\right).$$

Let us set

$$S_r(X,k) = \sum_{n=0}^{\infty}\left(\begin{array}{c} B_r(k)+n-1 \\ B_r(k)-1 \end{array}\right)X^n,$$

then

$$S_r(X,k) = \frac{1}{(1-X)^{B_r(k)}}.$$

But $S_r(X,k) = T_r(X,k) + R_r(X,k)$, where

$$R_r(X,k) = \sum_{n > M_r(k)} \begin{pmatrix} B_r(k)+n-1 \\ B_r(k)-1 \end{pmatrix} X^n.$$

By the Taylor formula the following holds:

$$R_r(X,k) = \int_0^X \frac{(X-t)^{M_r(k)}}{M_r(k)!} S_r^{(M_r(k)+1)}(t,k)dt.$$

We have to compute the successive derivatives of $S_r(X,k)$:

$$S_r^{(M_r(k)+1)}(X,k) = \frac{B_r(k)\, M_r(k)!}{(1-X)^{B_r(k)+M_r(k)+1}} \begin{pmatrix} B_r(k)+M_r(k) \\ B_r(k) \end{pmatrix}.$$

Then

$$R_r(X,k) = B_r(k) \begin{pmatrix} B_r(k)+M_r(k) \\ B_r(k) \end{pmatrix} \int_0^X \frac{(X-t)^{M_r(k)}}{(1-t)^{B_r(k)+M_r(k)+1}} dt$$

Lemma 4.2. *There is an integer k_2 such that for $k \geq k_2$ the function*

$$f_k(t) = \frac{(\frac{1}{q^r}-t)^{M_r(k)}}{(1-t)^{B_r(k)+M_r(k)+1}}$$

is decreasing on $[0, \frac{1}{q^r}]$.

Proof.

$$f'(t) =$$

$$\frac{(\frac{1}{q^r}-t)^{M_r(k)-1}}{(1-t)^{M_r(k)+B_r(k)+2}} \left(-M_r(k)(1-t) + \left(M_r(k)+B_r(k)+1\right)\left(\frac{1}{q^r}-t\right)\right).$$

The derivative vanishes for $t_1 = \frac{1}{q^r}$ and for

$$t_0 = -\frac{M_r(k)}{B_r(k)+1}\left(1-\frac{1}{q^r}\right) + \frac{1}{q^r}.$$

Let us choose a real number ϵ such that $0 < \epsilon < 1$. From (4.1) and (4.2) there exists an integer k_2 such that for $k \geq k_2$ the following holds:

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

Hence

$$t_0 \leq -\frac{(1-\epsilon)(q^r-1)}{q^{\frac{r}{2}}-1}\frac{1}{q^r} + \frac{1}{q^r}.$$

If ϵ is choosen sufficiently small, then

$$\frac{(1-\epsilon)(q^r-1)}{q^{\frac{r}{2}}-1} > 1,$$

and $t_0 < 0$. □

We conclude that

$$R_r\left(\frac{1}{q^r},k\right) \leq B_r(k)\left(\begin{array}{c} B_r(k)+M_r(k) \\ B_r(k) \end{array}\right)\left(\frac{1}{q^r}\right)^{M_r(k)+1}.$$

Lemma 4.3. *Let q be a prime power and let $r \geq 1$ be an integer. Then if $q \geq 4$ or $r \geq 2$, the sequence of remainder terms $R_r\left(\frac{1}{q^r},k\right)$ is such that*

$$\lim_{k\to+\infty} \frac{R_r\left(\frac{1}{q^r},k\right)}{S_r(\frac{1}{q^r},k)} = 0$$

Proof. By Lemma (4.1), for any real number ϵ and η such that $\epsilon > 0$ and $0 < \eta < 1$, we get

$$R_r\left(\frac{1}{q^r},k\right) < (1+\epsilon)B_r(k)\frac{C_2}{\sqrt{g_k}}q_2^{g_k}\left(\frac{1}{q^r}\right)^{M_r(k)+1}$$

where

$$q_2 = \left(\left(\frac{q^{\frac{r}{2}}}{q^{\frac{r}{2}}-1}\right)^{\frac{1}{r}(q^{\frac{r}{2}}-1)}\sqrt{q}\right)^{1+\eta} \quad \text{and } C_2 = \sqrt{\frac{q^{\frac{r}{2}}}{2\pi(q^{\frac{r}{2}}-1)(1+\eta)}}.$$

But

$$\ln\left(\left(\frac{q^{\frac{r}{2}}}{q^{\frac{r}{2}}-1}\right)^{\frac{1}{r}(q^{\frac{r}{2}}-1)}\right) = \frac{1}{r}(q^{\frac{r}{2}}-1)\ln\left(1+\frac{1}{q^{\frac{r}{2}}-1}\right) < \frac{1}{r}.$$

Then

$$\left(\frac{q^{\frac{r}{2}}}{q^{\frac{r}{2}}-1}\right)^{\frac{1}{r}(q^{\frac{r}{2}}-1)} < e^{\frac{1}{r}}. \tag{4.4}$$

A direct computation for the two particular cases $q = 2, r = 2$ and $q = 4, r = 1$ shows that for these values we have

$$\left(\frac{q^{\frac{r}{2}}}{q^{\frac{r}{2}}-1}\right)^{\frac{1}{r}(q^{\frac{r}{2}}-1)} = \sqrt{q}.$$

In all the other cases we derive from the inequality (4.4)

$$\left(\frac{q^{\frac{r}{2}}}{q^{\frac{r}{2}}-1}\right)^{\frac{1}{r}(q^{\frac{r}{2}}-1)} < \sqrt{q}.$$

Hence, if $\left(\frac{q^{\frac{r}{2}}}{q^{\frac{r}{2}}-1}\right)^{\frac{1}{r}(q^{\frac{r}{2}}-1)} < \sqrt{q}$ then for η sufficiently small, $q_2 < q$ and so

$$\lim_{k\to+\infty} B_r(k) q_2^{g_k}\left(\frac{1}{q^r}\right)^{M_r(k)+1} = 0.$$

Moreover,

$$S_r\left(\frac{1}{q^r}, k\right) = \left(\frac{q^r}{q^r-1}\right)^{B_r(k)}$$

which tends to the infinity.

Now if $\left(\frac{q^{\frac{r}{2}}}{q^{\frac{r}{2}}-1}\right)^{\frac{1}{r}(q^{\frac{r}{2}}-1)} = \sqrt{q}$ (i.e if $q = 2$ and $r = 2$ or if $q = 4$ and $r = 1$) we have $q_2 = q^{1+\eta}$. But $B_r(k) \geq \alpha g_k$ where α is a positive constant. Then for η sufficiently small, we have

$$1 < \frac{q_2}{q} = q^\eta < \left(\frac{q^r}{q^r-1}\right)^\alpha,$$

which implies

$$\left(\frac{q_2}{q}\right)^{g_k} \in o\left(S_r\left(\frac{1}{q^r}, k\right)\right).$$

$\square$

Now, we can establish the following proposition:

Proposition 4.4. *Let q be a prime power q and let $r \geq 1$ be an integer. Assume that*

$$\liminf_{k\to+\infty} \frac{B_r(k)}{g_k} = \mu_r > 0.$$

Then, the sum

$$Q_r(k) = \sum_{n=0}^{m_r(g_k-2)-1} \frac{1}{q^{nr}} \binom{B_r(k)+n-1}{B_r(k)-1}$$

satisfies

$$Q_r(k) \underset{k\to+\infty}{\sim} \left(\frac{q^r}{q^r-1}\right)^{B_r(k)}.$$

Hence, there exists a constant $C > 0$ such that for any k

$$\Sigma_2(k) = q^{g_k-1} \sum_{n=0}^{g_k-2} \frac{A_n}{q^n} \geq C\left(\frac{q^r}{q^r-1}\right)^{B_r(k)} q^{g_k}.$$

Proof. If $q \geq 4$ or $r \geq 2$, the result is given by Lemma 4.3. Let us consider the particular cases of $r = 1$ and $q = 2$ or $q = 3$. In these cases, first assume that the following limit exists:

$$\mu_1 = \lim_{k \to +\infty} \frac{B_1(k)}{g_k} > 0.$$

Let us do the same study as in Lemma 4.1. Let a be a constant integer and let η be any given number such that $0 < \eta < 1$. Then there is an integer $k_0 > 0$ such that for any integer $k \geq k_0$ the following inequalities hold:

$$\mu_1 g_k (1 - \eta) < B_1(k) < \mu_1 g_k (1 + \eta). \tag{4.5}$$

We study the asymptotic behaviour of the binomial coefficient:

$$\binom{B_1(k) + g_k - a}{B_1(k)}.$$

For any real numbers ϵ, η such that $\epsilon > 0$ and $0 < \eta < 1$, there exists an integer k_1 such that for any integer $k \geq k_1$ the following holds:

$$(1 - \epsilon) \frac{C_1}{\sqrt{g_k}} q_1^{g_k} < \binom{B_1(k) + g_k - a}{B_1(k)} < (1 + \epsilon) \frac{C_2}{\sqrt{g_k}} q_2^{g_k}, \tag{4.6}$$

where

$$C_1 = \sqrt{\frac{\mu_1 + 1}{2\pi \mu_1 (1 - \eta)}}$$

and

$$C_2 = \sqrt{\frac{\mu_1 + 1}{2\pi \mu_1 (1 + \eta)}}$$

are two positive constants depending upon η and where

$$q_1 = \left(\frac{(\mu_1 + 1)^{\mu_1 + 1}}{\mu_1^{\mu_1}} \right)^{1 - \eta}$$

and

$$q_2 = \left(\frac{(\mu_1 + 1)^{\mu_1 + 1}}{\mu_1^{\mu_1}} \right)^{1 + \eta}.$$

Hence,

$$\lim_{k \to +\infty} \frac{R_1\left(\frac{1}{q}, k\right)}{S_1(\frac{1}{q}, k)} = 0. \tag{4.7}$$

Indeed, for any real number ϵ and η such that $\epsilon > 0$ and $0 < \eta < 1$, we get

$$R_1\left(\frac{1}{2},k\right) < C_2 q^2 (1+\epsilon)(1+\eta)\mu_1\sqrt{g_k}\left(\frac{(\mu_1+1)^{\mu_1+1}}{\mu_1^{\mu_1}}\right)^{g_k(1+\eta)}\left(\frac{1}{q}\right)^{g_k}$$

and

$$S_1(\frac{1}{q},k) \geq \left(\frac{q}{q-1}\right)^{\mu_1 g_k(1-\eta)}.$$

Then

$$\frac{R_1\left(\frac{1}{2},k\right)}{S_1(\frac{1}{q},k)} \leq C_2 q^2 (1+\epsilon)(1+\eta)\mu_1\sqrt{g_k}$$
$$\times\left[\left(\frac{(\mu_1+1)^{\mu_1+1}}{\mu_1^{\mu_1}}\right)^{(1+\eta)}\left(\frac{q-1}{q}\right)^{\mu_1(1-\eta)}\left(\frac{1}{q}\right)\right]^{g_k}.$$

Let us study for $0 < \mu_1 \leq \sqrt{q}-1$ the function

$$f(\mu_1) = \left(\frac{(\mu_1+1)^{\mu_1+1}}{\mu_1^{\mu_1}}\right)\left(\frac{q-1}{q}\right)^{\mu_1}\frac{1}{q}.$$

This function is increasing since the derivative

$$(\log(f(\mu_1))' = \frac{f'(\mu_1)}{f(\mu_1)} = \log\left(\left(1+\frac{1}{\mu_1}\right)\left(1-\frac{1}{q}\right)\right) > 0$$

with $\mu_1 \leq \sqrt{q}-1$. In particular, we have:

(1) for $q=2$, $f(\mu_1) < 0.89$;
(2) for $q=3$, $f(\mu_1) < 0.81$.

Then in each case, for η sufficiently small,

$$\left[\left(\frac{(\mu_1+1)^{\mu_1+1}}{\mu_1^{\mu_1}}\right)^{(1+\eta)}\left(\frac{q-1}{q}\right)^{\mu_(1-\eta)}\left(\frac{1}{q}\right)\right] < 1, \tag{4.8}$$

and consequently we obtain the limit (4.7). Then as

$$\lim_{k\to+\infty}\frac{B_1(k)}{g_k} = \mu_1 > 0,$$

for any $\epsilon > 0$ there exists k_0 such that for each $k \geq k_0$

$$Q_1(k) \geq (1-\epsilon)\left(\frac{q}{q-1}\right)^{B_1(k)}.$$

Suppose now that we have the weaker assumption

$$\liminf_{k\to+\infty}\frac{B_1(k)}{g_k} = \mu_1 > 0$$

and suppose that there is a real number $\epsilon > 0$ such that for any k_0, there exists an integer $k \geq k_0$ such that

$$Q_1(k) < (1-\epsilon)\left(\frac{q}{q-1}\right)^{B_1(k)}.$$

We can construct an infinite subsequence $(Q_1(k_i))_i$ of $(Q_1(k))_k$such that the previous inequality holds for any i. Next we can extract from k_i a subsequence k_{i_j} such that

$$\lim_{j\to+\infty} \frac{B_1(k_{i_j})}{g_k} = \mu \geq \mu_1 > 0.$$

Using the previous result we conclude that for j sufficiently large

$$Q_1(k_{i_j}) \geq (1-\epsilon)\left(\frac{q}{q-1}\right)^{B_1(k)},$$

which gives a contradiction.

□

Corollary 4.5. *Let q be a prime power q and let $r \geq 1$ be an integer. Assume that*

$$\liminf_{k\to+\infty} \frac{B_r(k)}{g_k} = \mu_r > 0.$$

For any α such that $0 < \alpha < \mu_r$ there exists a constant $C > 0$ such that for any k:

$$\Sigma_2(k) \geq C\left[\left(\frac{q^r}{q^r-1}\right)^{\alpha} q\right]^{g_k}.$$

4.2. Asymptotical lower bound on $\boldsymbol{\Sigma_1(k)}$. Let us consider now the sum

$$\Sigma_1(k) = \sum_{n=0}^{g_k-1} A_n.$$

Using the inequality (2.5), we will obtain for this sum a lower bound which is negligible compared with the one obtained for $\Sigma_2(k)$. More precisely, the best we can do with this inequality is given by the following proposition:

Proposition 4.6. *For any η such that $0 < \eta < 1$, there exists a constant $C > 0$ such that for any k*

$$\Sigma_1(k) \geq C\frac{q_1^{g_k}}{\sqrt{g_k}}$$

where

$$q_1 = \left(\frac{\left(\mu_r+\frac{1}{r}\right)^{\mu_r+\frac{1}{r}}}{\mu_r^{\mu_r}\left(\frac{1}{r}\right)^{\frac{1}{r}}}\right)^{1-\eta}.$$

Proof. From the inequality (2.5) we know that

$$\Sigma_1(k) \geq K_1(r, B_1(k)) \begin{pmatrix} B_r(k) + m_r(g_k - 1) \\ B_r(k) \end{pmatrix} +$$

$$K_1\left(s_r(g-1), B_1(k)\right) \begin{pmatrix} B_r(k) + m_r(g_k - 1) \\ B_r(k) - 1 \end{pmatrix}.$$

This inequality can be written in the following way

$$\Sigma_1(k) \geq \left(K_1(r, B_1(k)) + \frac{B_r(k)}{m_r(g_k - 1)} K_1\left(s_r(g-1), B_1(k)\right)\right) \times \begin{pmatrix} B_r(k) + m_r(g_k - 1) \\ B_r(k) \end{pmatrix}.$$

As for k sufficiently large the following holds:

$$r\mu_r \left(\frac{1-\eta}{1+\eta}\right) \leq \frac{B_r(k)}{m_r(g_k - 1)} \leq (q^{\frac{r}{2}} - 1)\left(\frac{1+\eta}{1-\eta}\right).$$

Then, the best we can obtain is

$$\Sigma_1(k) = \Omega\left(\begin{pmatrix} B_r(k) + m_r(g_k - 1) \\ B_r(k) \end{pmatrix}\right).$$

where big Omega is the standard Landau notation.

Using Lemma 4.1 we obtain

$$\Sigma_1(k) \in \Omega\left(\frac{q_1^{g_k}}{\sqrt{g_k}}\right),$$

where

$$q_1 = \left(\frac{\left(\mu_r + \frac{1}{r}\right)^{\mu_r + \frac{1}{r}}}{\mu_r^{\mu_r}\left(\frac{1}{r}\right)^{\frac{1}{r}}}\right)^{1-\eta}.$$

□

Proposition 4.7. *The value q_1 introduced in the previous proposition is such that*

- *if $q \geq 4$ or $r \geq 2$ then $q_1 < q$;*
- *if $r = 1$ and $q = 2$ or $q = 3$ then for η sufficiently small*

$$q_1 < \left(\frac{q^r}{q^r - 1}\right)^{\mu_1(1-\eta)} q.$$

Proof. The function

$$v(x) = \left(\frac{\left(x + \frac{1}{r}\right)^{x + \frac{1}{r}}}{x^x\left(\frac{1}{r}\right)^{\frac{1}{r}}}\right)$$

is an increasing function. Then

$$v(\mu_r) \leq v\left(\frac{1}{r}\left(q^{\frac{r}{2}}-1\right)\right),$$

namely,

$$q_1 \leq \left(\left(\frac{q^{\frac{r}{2}}}{q^{\frac{r}{2}}-1}\right)^{\frac{1}{r}(q^{\frac{r}{2}}-1)} \sqrt{q}\right)^{1-\eta}.$$

We refer to the proof of Lemma 4.3 to see that when $q \geq 4$ or $r \geq 2$, the right member of this last formula is $\leq q^{1-\eta}$. When $r=1$ and $q=2$ or $q=3$ the formula (4.8) obtained in the proof of Proposition 4.4 holds and gives us the result. □

Conclusion 4.8. We conclude that in any case, the lower bound found on Σ_2 is better than the lower bound found on Σ_1.

4.3. Asymptotical lower bounds on the class number. In this section, we obtain asymptotical lower bounds on the class number of certain sequences of algebraic function fields as the consequence of the conclusion of the previous section and of Proposition 4.4.

Theorem 4.9. *Let $\mathcal{F}/\mathbb{F}_q = (F_k/\mathbb{F}_q)_k$ be a sequence of function fields over a finite field $\mathbb{F}_q$. Let us denote by g_k the genus of F_k, by $h(F_k/\mathbb{F}_q)$ the class number of $F_k/\mathbb{F}_q$ and by $B_i(F_k/\mathbb{F}_q)$ the number of places of degree i of $F_k/\mathbb{F}_q$. Let us suppose that for any k we have $B_1(F_k/\mathbb{F}_q) \geq 1$ and that there is an integer $r \geq 1$ such that*

$$\liminf_{k\to\infty} \frac{B_r(F_k/\mathbb{F}_q)}{g_k} = \mu_r(\mathcal{F}/\mathbb{F}_q) > 0.$$

Then for any α such that $0 < \alpha < \mu_r(\mathcal{F}/\mathbb{F}_q)$, there exists a constant $C > 0$ such that for any k

$$h(F_k/\mathbb{F}_q) \geq C\left(\left(\frac{q^r}{q^r-1}\right)^{\alpha} q\right)^{g_k}.$$

Moreover, we can improve the previous theorem in the following way:

Theorem 4.10. *Let $\mathcal{F}/\mathbb{F}_q = (F_k/\mathbb{F}_q)_k$ be a sequence of function fields over a finite field $\mathbb{F}_q$ and let $r \geq 1$ an integer. Let $\mathcal{G}/\mathbb{F}_{q^r} = (G_k/\mathbb{F}_{q^r})_k$ be the degree r constant field extension sequence of the sequence $\mathcal{F}/\mathbb{F}_q$, namely for any k we have $G_k/\mathbb{F}_{q^r} = F_k \otimes_{\mathbb{F}_q} \mathbb{F}_{q^r}$. Let us denote by g_k the genus of F_k and G_k, by $h(F_k/\mathbb{F}_q)$ the class number of $F_k/\mathbb{F}_q$ and by $B_r(F_k/\mathbb{F}_q)$ the number of places of degree r of $F_k/\mathbb{F}_q$. Let us suppose that*

$$\liminf_{k\to\infty} \sum_{i|r} \frac{iB_i(F_k/\mathbb{F}_q)}{g_k} = \mu_1(\mathcal{G}/\mathbb{F}_{q^r}) > 0.$$

Then for any α such that $0 < \alpha < \frac{1}{r}\mu_1(\mathcal{G}/\mathbb{F}_{q^r})$, there exists a constant $C > 0$ such that for any k

$$h(F_k/\mathbb{F}_q) \geq C\left(\left(\frac{q^r}{q^r-1}\right)^{\alpha} q\right)^{g_k}.$$

Proof. For $r = 1$ the result is yet proved by the previous study, then we suppose $r > 1$. We know that

$$B_1(G_k/\mathbb{F}_{q^r}) = \sum_{i|r} iB_i(F_k/\mathbb{F}_q),$$

then

$$\liminf_{k\to\infty} \sum_{i|r} \frac{iB_i(F_k/\mathbb{F}_q)}{g_k} = \liminf_{k\to\infty} \frac{B_1(G_k/\mathbb{F}_{q^r})}{g_k} = \mu_1(\mathcal{G}/\mathbb{F}_{q^r}).$$

Let us consider the families $\mathcal{D} = (D_i)_{i|r}$ where $D_i = \{Q_{i,1}, \cdots, Q_{i,c_i}\}$ and where the c_i elements $Q_{i,j}$ are formal symbols. Given a positive integer n, let us denote by $N_n(\mathcal{D})$ the number of formal combinations $\sum_{i,j} \alpha_{i,j} Q_{i,j}$ such that all the $\alpha_{i,j}$ are positive and $\sum_i i \sum_j \alpha_{i,j} = n$. For each k we define the two following families $\mathcal{D}_k$ and $\mathcal{D}'_k$:

- for $\mathcal{D}_k$, D_i is the set of places of degree i of the function field $F_k/\mathbb{F}_q$ and consequently $c_i(k) = B_i(F_k/\mathbb{F}_q)$.
- for $\mathcal{D}'_k$, we choose $c'_1(k) = 1$ and $c'_r(k)$ such that $\sum_{i|r} ic_i(k) = rc'_r(k) + s_k + 1$ with $0 \leq s_k \leq r-1$. For $1 < i < r$ we choose $c_i(k) = 0$. Then the following holds:

  $$c'_r(k) = \frac{1}{r}\left(\sum_{i|r} iB_i(F_k/\mathbb{F}_q) - s_k - 1\right).$$

  We note that

  $$\sum_{i|n} ic'_i(k) = 1 + rc'_r(k) \leq \sum_{i|r} ic_i,$$

  namely the total number of points in $\cup D'_i$ is less than the number of points in $\cup D_i$ and their degrees are bigger. We conclude that $N_n(\mathcal{D}_k) \geq N_n(\mathcal{D}'{}_k)$.

We also have

$$\liminf_{k\to\infty} \frac{c'_r(k)}{g_k} = \frac{1}{r} \liminf_{k\to\infty} \frac{\sum_{i|r} iB_i(F_k/\mathbb{F}_q) - s_k - 1}{rg_k} = \frac{\mu_1(\mathcal{G}/\mathbb{F}_{q^r})}{r}.$$

Using the Drinfeld Vladut bound on the constant field extension $(G_k/F_{q^r})_k$ of $(F_k/F_q)_k$ we get

$$\begin{aligned}\limsup_{k\to\infty}\frac{c'_r(k)}{g_k} &= \frac{1}{r}\limsup_{k\to\infty}\frac{\sum_{i|r} iB_i(F_k/\mathbb{F}_q)-s_k-1}{rg_k}\\ &= \frac{1}{r}\limsup_{k\to\infty}\frac{B_1(G_k/\mathbb{F}_{q^r})-s_k-1}{rg_k}\\ &\leq \frac{1}{r}\left(q^{\frac{r}{2}}-1\right).\end{aligned}$$

Then we can apply the previous study with $\mu = \frac{\mu_1(\mathcal{G}/\mathbb{F}_{q^r})}{r}$ to find an asymptotic lower bound on $N_n(\mathcal{D}')_k$ and consequently an asymptotic lower bound on $N_n(\mathcal{D})_k$ and on $h(F_k/\mathbb{F}_q)$. □

Remark 4.11. We find the asymptotical bounds of Tsfasman (cf. Theorem 1.4 [12, Corollary 2]) and those of Lebacque (cf. Theorem 1.6 [9, Theorem 7]) in the particular case of families reaching the Generalized Drinfeld-Vladut bound (by attaining the Drinfeld-Vladut of order r [1]). But we give here a completely different proof based upon elementary combinatorial considerations.

5. Examples

In this section, we study the class number of certain known towers $\mathcal{F}/\mathbb{F}_q = (F_k/F_q)$ of algebraic functions fields defined over a finite field $\mathbb{F}_q$. Let $r \geq 1$ be an integer. As previously, we consider the limit $\mu_r(\mathcal{F}/\mathbb{F}_q)$ for the tower $\mathcal{F}/\mathbb{F}_q$, defined as follows:

$$\mu_r(\mathcal{F}/\mathbb{F}_q) = \liminf_{k\to\infty}\frac{B_r(k)}{g_k}.$$

5.1. Sequences $\mathcal{F}/\mathbb{F}_q$ with $\mu_r(\mathcal{F}/\mathbb{F}_q) = \frac{1}{r}(q^{\frac{r}{2}}-1)$. In this section, for any prime power q and for any integer $r = 2^f$ such that f is an integer ≥ 1, we exhibit some examples of sequences of algebraic function fields defined over $\mathbb{F}_q$ reaching the Generalized Drinfeld-Vladut bound of order r [1].

Moreover, we know accurate lower bounds on the number of places of concerned degree r. Then, by using the results of the previous sections, we can give lower bounds on the class number for each step of these towers. Note that we also obtain asymptotical bounds which reach the bounds of Tsfasman [12]. However, these can be obtained directly from [12, Corollary 2] since it is known that any tower is asymptotically exact by [7].

We consider the Garcia-Stichtenoth's tower $T_0/\mathbb{F}_{q^r}$ over $\mathbb{F}_{q^r}$ constructed in [5]. Recall that this tower is defined recursively in the following way. We set $F_1 = \mathbb{F}_{q^r}(x_1)$ the rational function field over $\mathbb{F}_{q^r}$, and for $i \geq 1$ we define

$$F_{i+1} = F_i(z_{i+1}),$$

where z_{i+1} satisfies the equation

$$z_{i+1}^{q^{\frac{r}{2}}} + z_{i+1} = x_i^{q^{\frac{r}{2}}+1},$$

with

$$x_i = \frac{z_i}{x_{i-1}} \text{ for } i \geq 2.$$

Let us denote by g_k the genus of F_k in $T_0/\mathbb{F}_{q^r}$. Let $T_1/\mathbb{F}_{q^{\frac{r}{2}}} = \left(G_i/\mathbb{F}_{q^{\frac{r}{2}}}\right)$ be the descent of the tower $T_0/\mathbb{F}_{q^r}$ on the finite field $\mathbb{F}_{q^{\frac{r}{2}}}$ and let $T_2/\mathbb{F}_q = (H_i/\mathbb{F}_q)$ be the descent of the tower $T_0/\mathbb{F}_{q^r}$ on the finite field $\mathbb{F}_q$, namely, for any integer i,

$$F_i = G_i \otimes_{\mathbb{F}_{q^{\frac{r}{2}}}} \mathbb{F}_{q^r} \text{ and } F_i = H_i \otimes_{\mathbb{F}_q} \mathbb{F}_{q^r}.$$

Let us prove a proposition establishing that the tower $T_2/\mathbb{F}_q$ reaches the Generalized Drinfeld-Vladut Bound of order r.

Proposition 5.1. *Let q be prime power and $r = 2^f$ where f is an integer ≥ 1. The tower $T_2/\mathbb{F}_q$ is such that*

$$\lim_{k \to +\infty} \frac{B_r(H_k)}{g_k} = \frac{1}{r}(q^{\frac{r}{2}} - 1),$$

and

$$B_1(H_k) \geq 1 \textit{ for any integer } k.$$

Proof. First, note that as the algebraic function field $F_k/\mathbb{F}_{q^r}$ is a constant field extension of $G_k/\mathbb{F}_{q^{\frac{r}{2}}}$, above any place of degree one in $G_k/\mathbb{F}_{q^{\frac{r}{2}}}$ there exists a unique place of degree one in $F_k/\mathbb{F}_{q^r}$. Consequently, let us use the classification given in [5, p. 221] of the places of degree one of $F_k/\mathbb{F}_{q^r}$. Let us remark that the number of places of degree one which are not of type (A), is less or equal to $2q^r$ (see [5, Remark 3.4]). Moreover, the genus g_k of the algebraic function fields $G_k/\mathbb{F}_{q^{\frac{r}{2}}}$ and $F_k/\mathbb{F}_{q^r}$ is such that $g_k \geq q^k$ by [5, Theorem 2.10], then we can focus our study on places of type (A). The places of type (A) are built recursively in the following way (cf. [5, p. 220 and Proposition 1.1 (iv)]). Let $\alpha \in \mathbb{F}_{q^r} \setminus \{0\}$ and P_α be the place of $F_1/\mathbb{F}_{q^r}$ which is the zero of $x_1 - \alpha$. For any $\alpha \in \mathbb{F}_{q^r} \setminus \{0\}$ the polynomial equation $z_2^{q^{\frac{r}{2}}} + z_2 = \alpha^{q^{\frac{r}{2}}+1}$ has $q^{\frac{r}{2}}$ distinct roots $u_1, \cdots u_{q^{\frac{r}{2}}}$ in $\mathbb{F}_{q^r}$, and for each u_i there is a unique place $P_{(\alpha,i)}$ of $F_2/\mathbb{F}_{q^r}$ above P_α and this place $P_{(\alpha,i)}$ is a zero of $z_2 - u_i$. We iterate now the process starting from the places $P_{(\alpha,i)}$ to obtain successively the places of type (A) of $F_3/\mathbb{F}_{q^r}, \cdots, F_k/\mathbb{F}_{q^r}, \cdots$; then, each place P of type (A) of $F_k/\mathbb{F}_{q^r}$ is a zero of $z_k - u$ where u is itself a zero of $u^{q^{\frac{r}{2}}} + u = \gamma$ for some $\gamma \neq 0$ in $\mathbb{F}_{q^r}$. Let us denote by P_u this place. Now, we want to count the number of places P'_u of degree one in $G_k/\mathbb{F}_{q^{\frac{r}{2}}}$, that is to say the only places which admit a unique place of degree one P_u in $F_k/\mathbb{F}_{q^r}$ lying over P'_u.

First, note that it is possible only if u is a solution in $\mathbb{F}_{q^{\frac{r}{2}}}$ of the equation $u^{q^{\frac{r}{2}}}+u=\gamma$ where γ is in $\mathbb{F}_{q^{\frac{r}{2}}}\setminus\{0\}$. Indeed, if u is not in $\mathbb{F}_{q^{\frac{r}{2}}}$, there exists an automorphism σ in the Galois group $Gal(F_k/G_k)$ of the degree two Galois extension $F_k/\mathbb{F}_{q^r}$ of $G_k/\mathbb{F}_{q^{\frac{r}{2}}}$ such that $\sigma(P_u)\neq P_u$. Hence, the unique place of $G_k/\mathbb{F}_{q^{\frac{r}{2}}}$ lying under P_u is a place of degree 2. But $u^{q^{\frac{r}{2}}}+u=\gamma$ has one solution in $\mathbb{F}_{q^{\frac{r}{2}}}$ if $p\neq 2$ and no solution in $\mathbb{F}_{q^{\frac{r}{2}}}$ if $p=2$. Hence the number of places of degree one of $G_k/\mathbb{F}_{q^{\frac{r}{2}}}$ which are lying under a place of type (A) of $F_k/\mathbb{F}_{q^r}$ is equal to zero if $p=2$ and equal to $q^{\frac{r}{2}}-1$ if $p\neq 2$. We conclude that

$$\lim_{k\to+\infty}\frac{B_1(G_k/\mathbb{F}_{q^{\frac{r}{2}}})}{g_k}=0.$$

Let us remark that in any case, the number of places of degree one of $G_k/\mathbb{F}_{q^{\frac{r}{2}}}$ is less or equal to $2q^r$. Moreover, as $G_k/\mathbb{F}_{q^{\frac{r}{2}}}$ is the constant field extension of $H_k/\mathbb{F}_q$ of degree $\frac{r}{2}$, any place of $H_k/\mathbb{F}_q$ of degree $i<r$ dividing r is totally decomposed in $G_k/\mathbb{F}_{q^{\frac{r}{2}}}$ by [11, Lemma 5.1.9] since $r=2^f$ and so is a place of $H_k/\mathbb{F}_q$ lying under only some places of degree one (at most $\frac{r}{2}$) belonging to $G_k/\mathbb{F}_{q^{\frac{r}{2}}}$. Hence, we have for any integer i dividing r such that $i<r$,

$$\lim_{k\to+\infty}\frac{B_i(H_k/\mathbb{F}_q)}{g_k}=0.$$

Then, as the Garcia-Stichtenoth tower $T_0/\mathbb{F}_{q^r}$ attains the Drinfeld-Vladut bound [5], we deduce the first assertion by the relation $\sum_{i=1,i|r}^{r} iB_i(H_k/\mathbb{F}_q) = B_r(F_k/\mathbb{F}_{q^r})$. Now, consider the place P_∞ in $F_1/\mathbb{F}_{q^r}$ of degree one corresponding to the pole of x_1 in $F_1/\mathbb{F}_{q^r}$. Then, by [5, Lemma 2.1], the place P_∞ is totally ramified in F_2/F_1. Moreover, the unique place P' in $F_2/\mathbb{F}_{q^r}$ lying above P_∞ has degree one and is totally ramified in F_k/F_2 for any integer k since P' is a place of type (B) by [5, Section 3]. Hence, since the place P_∞ is invariant under the action of the Galois group $Gal(\mathbb{F}_{q^r}/\mathbb{F}_q)$, the place $P_\infty\cap H_1/\mathbb{F}_q$ in $H_1/\mathbb{F}_q$ has degree one and is totally ramified in H_k/H_1 for any integer k, and the proof is complete.

□

Remark 5.2. In the previous example, we explicitly prove that the tower $T_2/\mathbb{F}_q$ reaches the Generalized Drinfeld-Vladut Bound of order r for any integer r such that $r=2^f$ where f is an integer >0. In fact, it is possible to prove that the tower $T_2/\mathbb{F}_q$ reaches the Generalized Drinfeld-Vladut bound of order r for any even integer r. Indeed, let us set $r=2t$, then as

$\lim_{k\to+\infty} \frac{B_1(F_k/\mathbb{F}_{q^{2t}})}{g_k} = q^t - 1$ and $B_1(F_k/\mathbb{F}_{q^{2t}}) = \sum_{i|r} iB_i(H_k/\mathbb{F}_q)$, we have:

$$\liminf_{g_k\to+\infty} \frac{1}{g_k}\sum_{i=1}^{2t} \frac{iB_i(H_k/\mathbb{F}_q)}{q^t-1} \geq \frac{1}{g_k}\sum_{i|2t} \frac{iB_i(H_k/\mathbb{F}_q)}{q^t-1} = \liminf_{g_k\to+\infty} \frac{B_1(F_k/\mathbb{F}_{q^{2t}})}{g_k(q^t-1)} = 1.$$

Hence, it shows that for a certain integer $m \geq 1$, we have:

$$\liminf_{g_k\to+\infty} \frac{1}{g_k}\sum_{i=1}^{m} \frac{iB_i(H_k/\mathbb{F}_q)}{q^{\frac{m}{2}}-1} \geq 1,$$

which implies : $\lim_{g_k\to+\infty} \frac{mB_m(H_k/\mathbb{F}_q)}{g_k} = q^{\frac{m}{2}} - 1$ by [3, Lemma IV.3].

Theorem 5.3. *Let q be prime power and $r = 2^f$ where f is an integer ≥ 1. Let us consider the algebraic function fields $F_k/\mathbb{F}_{q^r}$ and $H_k/\mathbb{F}_q$ of genus g_k constituting respectively the towers $T_0/\mathbb{F}_{q^r}$ and $T_2/\mathbb{F}_q$. There are two positive real numbers c and c' such that the following holds: for any $\epsilon > 0$ there exists an integer k_0 such that for any integer $k \geq k_0$, we have*

$$h(F_k/\mathbb{F}_{q^r}) \geq c\left(\frac{q^r}{q^r-1}\right)^{B_1(F_k/\mathbb{F}_{q^r})} q^{rg_k},$$

where $B_1(F_k/\mathbb{F}_{q^r}) \geq (q^r-1).q^{\frac{r}{2}(k-1)} + 2q^{\frac{r}{2}}$ and

$$h(H_k/\mathbb{F}_q) \geq c'\left(\frac{q^r}{q^r-1}\right)^{B_r(H_k/\mathbb{F}_q)} q^{g_k},$$

where $B_r(H_k/\mathbb{F}_q) \geq \frac{g_k}{r}\left(q^{\frac{r}{2}}-1\right)(1-\epsilon)$ and

$$g_k = \begin{cases} (q^r)^n + (q^r)^{n-1} - (q^r)^{\frac{n+1}{2}} - 2(q^r)^{\frac{n-1}{2}} + 1 & \text{if } n \text{ is odd },\\ (q^r)^n + (q^r)^{n-1} - \frac{1}{2}(q^r)^{\frac{n}{2}+1} - \frac{3}{2}(q^r)^{\frac{n}{2}} - (q^r)^{\frac{n}{2}-1} + 1 & \text{if } n \text{ is even }.\end{cases}$$

Proof. By a property of the Garcia-Stichtenoth tower [5] and by Proposition 5.1, we have

$$\beta_1(T_0/\mathbb{F}_{q^r}) = \lim_{g_k\to+\infty} \frac{B_1(F_k/\mathbb{F}_{q^r})}{g_k} = q^{\frac{r}{2}} - 1$$

and

$$\beta_r(T_2/\mathbb{F}_q) = \lim_{g_k\to+\infty} \frac{B_r(H_k/\mathbb{F}_q)}{g_k} = \frac{1}{r}(q^{\frac{r}{2}} - 1).$$

Moreover, we have $B_1(F_k/\mathbb{F}_{q^r}) \geq (q^r-1).q^{\frac{r}{2}(k-1)} + 2q^{\frac{r}{2}}$ by [5] and we have $B_1(H_k/\mathbb{F}_q) > 0$ by Proposition 5.1. Hence, we have also

$$\sum_{i|r} iB_i(H_k/\mathbb{F}_q) \geq (q^r-1).q^{\frac{r}{2}(k-1)} + 2q^{\frac{r}{2}}.$$

Then, we can use Theorem 4.9 for the tower $T_0/\mathbb{F}_{q^r}$ and use Theorem 4.10 for the tower $T_2/\mathbb{F}_q$ for assertion (2). □

Remark 5.4. Note that it is absolutely natural to use the descent of the Garcia-Stichtenoth tower since the recursive equation of this tower is defined over $\mathbb{F}_q$. Another argument would be to use the fact that this tower is a tower of Drinfeld modular curves by Elkies [4] which implies that it is defined over $\mathbb{F}_q$.

5.2. Sequences $\mathcal{F}/\mathbb{F}_q$ with $\mu_r(\mathcal{F}/\mathbb{F}_q) > 0$ for certain integers $r \geq 1$. In this section, we study the class number of few towers defined over different finite fields $\mathbb{F}_q$, whose we only know that for a certain integer r, we have $\mu_r(\mathcal{F}/\mathbb{F}_q) > 0$ or $\mu_1(\mathcal{F}/\mathbb{F}_{q^r}) > 0$. Hence, we only obtain asymptotical lower bounds on the class number of these towers, which could also be obtained from the Generalized Brauer-Siegel Theorem ([12, Corollary 2], [14, Part II]). The studied towers are all tame towers exhibited by Garcia and Stichtenoth in [6]. Let us recall the recursive definition of an arbitrary tower defined over $\mathbb{F}_q$.

Definition 5.5. A tower $\mathcal{T}$ is defined by the equation $\psi(y) = \phi(x)$ if $\psi(y)$ and $\phi(x)$ are two rational functions over $\mathbb{F}_q$ such that

$$\mathcal{T} = \mathbb{F}_q(x_0, x_1, x_2, ...) \text{ with } \psi(x_{i+1}) = \phi(x_i) \text{ for all } i \geq 0.$$

5.2.1. *Examples 1: some tame towers of Fermat type.* Let us recall some generalities about the towers of Fermat Type [6].

Definition 5.6. A tower $\mathcal{T}$ over $\mathbb{F}_q$ defined by the equation

$$y^m = a(x+b)^m + c, \text{ with } (m,q) = 1$$

is said to be a Fermat tower if for each $i \geq 0$, the field $\mathbb{F}_q$ is algebraically closed in F_i and $[F_{i+1} : F_i] = m$.

Now, we can give the following result:

Proposition 5.7. *Let l be a power of the characteristic of $\mathbb{F}_q$ and let $q = l^r$ with $r \geq 1$. Assume that*

$$r \equiv 0 \mod 2 \text{ or } l \equiv 0 \mod 2.$$

Then the equation

$$y^{l-1} = -(x+b)^{l-1} + 1, \text{ with } b \in \mathbb{F}_l^*$$

define a tower $\mathcal{F}/\mathbb{F}_l = (F_0, F_1, ...F_n, ...)$ over $\mathbb{F}_l$ such that for any α satisfying $0 < \alpha < \frac{2}{r(l-2)}$, we have:

$$h(F_k/\mathbb{F}_l) \in \Omega\left(\left(\left(\frac{q}{q-1}\right)^{\alpha} l\right)^{g_k}\right).$$

Proof. By Theorem 3.10 in [6], the equation

$$y^{l-1} = -(x+b)^{l-1} + 1, \text{ with } b \in \mathbb{F}_l^*$$

defines a Fermat tower $\mathcal{T}/\mathbb{F}_q = (T_0, T_1, ...T_n, ...)$ over $\mathbb{F}_q$ such that $\mu_1(\mathcal{T}/\mathbb{F}_q) = \frac{2}{l-2}$. Then the tower $\mathcal{F}/\mathbb{F}_l$ is the tower such that $\mathcal{T} = \mathbb{F}_q \otimes_{\mathbb{F}_l} \mathcal{F}$ is the constant field extension tower of $\mathcal{F}$ of degree r. Hence, the tower $\mathcal{F}/\mathbb{F}_l$ satisfies $\liminf_{k\to\infty} \sum_{i|r} \frac{iB_i(F_k/\mathbb{F}_l)}{g_k} = \mu_1(\mathcal{T}/\mathbb{F}_q) = \frac{2}{l-2}$ and we conclude by using Theorem 4.10. □

We can obtain a similar result with other examples of Fermat towers exhibited in Section 3 of [6], in particular Example 3.12.

5.2.2. ***Examples 2: some tame quadratic towers.*** Let us give few other examples of towers for which we are be able to give very good asymptotics for the class number.

Proposition 5.8. *Let us consider the tower $\mathcal{F}/\mathbb{F}_3$ defined over $\mathbb{F}_3$ recursiveley by the equation*

$$y^2 = \frac{x(x-1)}{x+1}.$$

Then the tower $\mathcal{F}/\mathbb{F}_3 = (F_0, F_1, ...F_n, ...)$ defined over $\mathbb{F}_3$ satisfies

$$h(F_k/\mathbb{F}_3) \in \Omega\left(\left(3\left(\frac{9}{8}\right)^{\frac{1}{3}}\right)^{g_k}\right).$$

Proof. By Example 4.3 in [6], the equation $y^2 = \frac{x(x-1)}{x+1}$ defines a tower $\mathcal{T}/\mathbb{F}_9 = (T_0, T_1, ...T_n, ...)$ over $\mathbb{F}_9$ such that $\mu_1(\mathcal{T}/\mathbb{F}_9) \geq 2/3$. Then the tower $\mathcal{F}/\mathbb{F}_3$ is the tower such that $\mathcal{T} = \mathbb{F}_9 \otimes_{\mathbb{F}_3} \mathcal{F}$ is the constant field extension tower of $\mathcal{F}$ of degree $r = 2$. Hence, the tower $\mathcal{F}/\mathbb{F}_3$ satisfies $\liminf_{k\to\infty} \sum_{i|r} \frac{iB_i(F_k/\mathbb{F}_l)}{g_k} = \mu_1(\mathcal{T}/\mathbb{F}_9) \geq \frac{2}{3}$ and we conclude by using Theorem 4.10. □

Now, we also have the following result:

Proposition 5.9. *Let us consider the tower $\mathcal{F}/\mathbb{F}_3$ defined over $\mathbb{F}_3$ recursively by the equation*

$$y^2 = \frac{x(1-x)}{x+1}.$$

Then the tower $\mathcal{F}/\mathbb{F}_3 = (F_0, F_1, ...F_n, ...)$ defined over $\mathbb{F}_3$ satisfies

$$h(F_k/\mathbb{F}_3) \in \Omega\left(\left(3\left(\frac{81}{80}\right)^{\frac{1}{2}}\right)^{g_k}\right).$$

Proof. By Example 4.5 and Remark 4.6 in [6], the equation $y^2 = \frac{x(1-x)}{x+1}$ defines a tower $\mathcal{T}/\mathbb{F}_{81} = (T_0, T_1, ...T_n, ...)$ over $\mathbb{F}_{81}$ such that $\mu_1(\mathcal{T}/\mathbb{F}_{81}) \geq 2$. Then the tower $\mathcal{F}/\mathbb{F}_3$ is the tower such that $\mathcal{T} = \mathbb{F}_{81} \otimes_{\mathbb{F}_3} \mathcal{F}$ is the constant field extension tower of $\mathcal{F}$ of degree $r = 4$. Hence, the tower $\mathcal{F}/\mathbb{F}_3$ satisfies $\liminf_{k\to\infty} \sum_{i|r} \frac{iB_i(F_k/\mathbb{F}_l)}{g_k} = \mu_1(\mathcal{T}/\mathbb{F}_{81}) \geq \frac{1}{2}$ and we conclude by using Theorem 4.10. □

Then, we also have:

Proposition 5.10. *Let us consider the tower $\mathcal{F}/\mathbb{F}_5$ defined over $\mathbb{F}_5$ recursively by the equation*

$$y^2 = \frac{x(x+2)}{x+1}.$$

Then the tower $\mathcal{F}/\mathbb{F}_5 = (F_0, F_1, ...F_n, ...)$ defined over $\mathbb{F}_3$ satisfies

$$h(F_k/\mathbb{F}_5) \in \Omega\left(\left(5\left(\frac{25}{24}\right)^{\frac{1}{2}}\right)^{g_k}\right).$$

Proof. By Example 4.8 and Remark 4.6 in [6], the equation $y^2 = \frac{x(x+2)}{x+1}$ defines a tower $\mathcal{T}/\mathbb{F}_{25} = (T_0, T_1, ...T_n, ...)$ over $\mathbb{F}_{81}$ such that $\mu_1(\mathcal{T}/\mathbb{F}_{25}) \geq 1$. Then the tower $\mathcal{F}/\mathbb{F}_5$ is the tower such that $\mathcal{T} = \mathbb{F}_{25} \otimes_{\mathbb{F}_5} \mathcal{F}$ is the constant field extension tower of $\mathcal{F}$ of degree $r = 2$. Hence, the tower $\mathcal{F}/\mathbb{F}_5$ satisfies $\liminf_{k\to\infty} \sum_{i|r} \frac{iB_i(F_k/\mathbb{F}_l)}{g_k} = \mu_1(\mathcal{T}/\mathbb{F}_{25}) \geq \frac{1}{2}$ and we conclude by using Theorem 4.10. □

References

[1] Stéphane Ballet and Robert Rolland, *Families of curves over any finite field attaining the generalized drinfeld-vladut bound.* Publ. Math. Univ. Franche-Comté Besançon Algébr. Théor. Nr., 5–18, 2011.

[2] Stéphane Ballet and Robert Rolland, *Minorations du nombre de classes des corps de fonctions algébriques définis sur un corps fini.* Comptes Rendus de l'Académie des Sciences (Paris), Ser.I, **349** (2011), 709–712.

[3] Ignacio Cascudo, Ronald Cramer, Chaoping Xing, An Yang, *Asymptotic bound for Multiplication complexity in the extensions of small finite fields.* IEEE Transactions on Information Theory, to appear.

[4] Noam Elkies, *Explicit towers of Drinfeld modular curves.* European Congress of Mathematics (Barcelona 2000), Progr. Math., Birkausel, Basel, Vol. II, **202**, 189–198, 2001.

[5] Arnaldo Garcia and Henning Stitchtenoth, *A tower of artin-schreier extensions of function fields attaining the drinfeld-vladut bound.* Inventiones Mathematicae **121** (1995), 211–222.

[6] Arnaldo Garcia, Henning Stitchtenoth, and Hans-Georg Ruck, *On tame towers over finite fields.* Journal fur die reine und angewandte Mathematik, **557** (2003), 53–80.

[7] T. Hasegawa, *A note on optimal towers over finite fields.* Tokyo J. Math. **30** (2007) (2) , 477–487.

[8] Gilles Lachaud and Mireille Martin-Deschamps, *Nombre de points des jacobiennes sur un corps finis.* Acta Arithmetica **56** (1990) (4), 329–340.

[9] Philippe Lebacque, *Generalised Mertens and Brauer-Siegel theorems.* Acta Arithmetica **130** (2007) (4), 333–350.

[10] Marc Perret, *Number of points of Prym varieties over finite fields.* Glasg. Math. J. **48** (2006), no. 2, 275–280.

[11] Henning Stitchtenoth, *Algebraic function fields and codes.* Springer, Graduate texts in Mathematics, **254**, second edition, 2009.

[12] Michael Tsfasman, *Some remarks on the asymptotic number of points.* In H. Stichtenoth and M.A. Tsfasman, editors, Coding Theory and Algebraic Geometry, volume **1518** of Lecture Notes in Mathematics, pages 178–192, Berlin, 1992. Springer-Verlag. Proceedings of AGCT-3 conference, June 17-21, 1991, Luminy.

[13] Michael Tsfasman and Serguei Vladut, *Asymptotic properties of zeta-functions.* Journal of Mathematical Sciences **84** (1997) (5), 1445–1467.

[14] MICHAEL TSFASMAN AND SERGUEI VLADUT, *Infinite global fields and the generalized Brauer-Siegel theorem*. Mosc. Math. J. **2** (2002) (2), 329–402.

[15] MICHAEL TSFASMAN, SERGUEI VLADUT, AND DMITRY NOGIN, *Algebraic Geometric Codes: Basic Notions*, volume **139** of Mathematical Surveys and Monographs. American Mathematical Society, 2007.

[16] ANDRÉ WEIL, *Sur les courbes algébriques et les variétés qui s'en déduisent. Variétés abéliennes et courbes algébriques*. Hermann, 1948. Publications de l'Institut de mathématiques de l'Université de Strasbourg, fasc. VII et VIII.

[17] ANDRÉ WEIL, *Basic Number Theory*. Springer, 1967.

Stéphane BALLET
Aix-Marseille Université
Institut de Mathématiques de Luminy
Équipe Arithmétique et Théorie de l'Information
et
Groupe d'Études et Recherche en Informatique
des Systèmes Communicants Sécurisés.
Case 907
F13288 Marseille cedex 9
France
E-mail: stephane.ballet@univ-amu.fr
URL: http://iml.univ-mrs.fr/~ballet

Robert ROLLAND
Aix-Marseille Université
Institut de Mathématiques de Luminy
Équipe Arithmétique et Théorie de l'Information
et
Groupe d'Études et Recherche en Informatique
des Systèmes Communicants Sécurisés.
Case 907
F13288 Marseille cedex 9
France
E-mail: robert.rolland@acrypta.fr
URL: http://robert.rolland.acrypta.com