



HAL
open science

On the number of effective divisors in algebraic function fields defined over a finite field

Stéphane Ballet, Gilles Lachaud, Rolland Robert

► **To cite this version:**

Stéphane Ballet, Gilles Lachaud, Rolland Robert. On the number of effective divisors in algebraic function fields defined over a finite field. *Arithmetic, Geometry, Cryptography and Coding Theory*, May 2021, Marseille, France. hal-03657775

HAL Id: hal-03657775

<https://hal.science/hal-03657775>

Submitted on 3 May 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

ON THE NUMBER OF EFFECTIVE DIVISORS IN ALGEBRAIC FUNCTION FIELDS DEFINED OVER ANY FINITE FIELD

STÉPHANE BALLEZ, GILLES LACHAUD, AND ROBERT ROLLAND

ABSTRACT. Nous étudions le nombre de diviseurs effectifs, ayant un degré donné, d'un corps de fonctions algébriques sur un corps fini. Nous déterminons tout d'abord des bornes inférieures et des bornes supérieures de ce nombre quand le corps de fonctions, le degré des diviseurs et le corps fini sous-jacent sont fixés. Nous étudions ensuite le comportement de ce nombre de diviseurs effectifs quand certains paramètres, notamment le corps fini, le degré des diviseurs effectifs, le corps de fonctions algébriques, sont des variables.

We study the number of effective divisors of a given degree of an algebraic function field defined over a finite field. We first give lower bounds and upper bounds when the function field, the degree and the underlying finite field are fixed. Then we study the behavior of the number of effective divisors when some of the parameters, namely the underlying finite field, the degree of the effective divisors, the algebraic function field can be variable.

1. INTRODUCTION

The algebraic properties of algebraic function fields defined over a finite field is somehow reflected by their numerical properties, namely their numerical invariants such as the number of places of degree one over a given ground field extension, the number of classes of its Picard group, the number of effective divisors of a given degree and so on. In this paper, we are interested in the study of the number of effective divisors of a given degree and in the asymptotic behavior of this number under various assumptions.

The context of our study is as follows. We consider a function field F/\mathbb{F}_q of genus g over the finite field \mathbb{F}_q with q elements. Sometimes we will use the dual language of curves. We will denote by X a curve

Date: July 11, 2019.

2000 Mathematics Subject Classification. Primary 12E20; Secondary 14H05.

Key words and phrases. finite field, algebraic function field, algebraic curve, divisor, effective divisor, class number, zeta-function.

defined over \mathbb{F}_q , having F/\mathbb{F}_q for algebraic function field over \mathbb{F}_q and by $X(\mathbb{F}_q)$ the set of \mathbb{F}_q -rational points of X , corresponding to the set of places of degree one of F/\mathbb{F}_q .

For any integer $n \geq 0$, let $A_n(F/\mathbb{F}_q)$ be the number of effective divisors of degree n of F/\mathbb{F}_q , $h(F/\mathbb{F}_q)$ its class number and $B_n = B_n(F/\mathbb{F}_q)$ its number of places of degree n . If there is no ambiguity we will set $A_n = A_n(F/\mathbb{F}_q)$, $h = h(F/\mathbb{F}_q)$ and $B_n = B_n(F/\mathbb{F}_q)$.

In the study of the quantity A_n , we need distinguish the two following cases:

- (a) $n \leq g - 1$;
- (b) arbitrary n .

Indeed, in the first case the quantity A_n is linked to the functional equation (1) involving several fundamental invariants, in particular the class number of the algebraic function field and the following $S(F/\mathbb{F}_q)$ and $R(F/\mathbb{F}_q)$ quantities:

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

where $(\alpha_i, \bar{\alpha}_i)_{1 \leq i \leq g}$ 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 [7], we know that

$$(1) \quad S(F/\mathbb{F}_q) = hR(F/\mathbb{F}_q).$$

Let us also recall that the zeta-funtion of F/\mathbb{F}_q is given by:

$$Z(t) = \sum_{m=0}^{+\infty} A_m t^m = \frac{L(t)}{(1-t)(1-qt)}$$

where $L(t) = \sum_{i=0}^{2g} a_i t^i$ is in $\mathbb{Z}[t]$.

2. ORGANIZATION

The paper is organized in the following way. In Section 3 the study is done when the finite field \mathbb{F}_q and the algebraic function field F/\mathbb{F}_q are fixed. We first give in Subsection 3.1 general results and general *formulae* on the numbers A_n for any positive n . Then in Subsection 3.2 we present some lower bounds on A_n for any positive n and finally in Subsection 3.3 we give when $1 \leq n \leq g - 1$ some upper bounds on $\frac{A_n}{h}$.

Next in Section 4 we study the asymptotic behavior of $A_n(F/\mathbb{F}_q)$ when some of the parameters n, F, q are variable. More precisely, in Subsection 4.1 we study the case of a fixed curve X , a fixed degree n for the effective divisors and q growing to infinity, namely, starting from a finite field \mathbb{F}_{q_1} we consider a sequence of extensions \mathbb{F}_{q_i} of \mathbb{F}_{q_1} where q_i is growing to infinity. In Subsection 4.2 we suppose that the field \mathbb{F}_q is fixed and we consider a sequence of curves $(X_k)_k$ of genus $g_k = g(X_k)$ growing to infinity. For each curve X_k we fix a degree d_k . In this case we study the behavior of the sequence $(A_{d_k}(F_k/\mathbb{F}_q))_k$ where F_k/\mathbb{F}_q is the algebraic function field associated with the curve X_k and where d_k is linked to g_k in some way.

3. NON-ASYMPTOTICAL CASE

3.1. General results. In this section, we consider the case where the degree n is an arbitrary integer. Let us set

$$\Delta = \{i \in \mathbb{N} \mid 1 \leq i \leq g - 1 \text{ and } B_i \geq 1\}.$$

$$U_n = \left\{ b = (b_i)_{i \in \Delta} \mid b_i \geq 0 \text{ and } \sum_{i \in \Delta} ib_i = n \right\}.$$

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

$$(2) \quad \binom{B_i + b_i - 1}{b_i} = \binom{B_i + b_i - 1}{B_i - 1}.$$

Then the number of effective divisors of degree n is given by the following result, already mentioned in [10], [3] and [4]:

Proposition 3.1. *The number of effective divisors of degree n of an algebraic function field F/\mathbb{F}_q is:*

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

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 degree i is given by the binomial coefficient (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. \square

Proposition 3.2. *Let \mathbf{F}/\mathbb{F}_q be a function field of genus g and let $L(t) = \sum_{i=0}^{2g} a_i t^i$ be the numerator of its zeta-function. Moreover, let us set $a_i = 0$ for any integer $i > 2g$. Then, for any integer $n \geq 0$, we have:*

$$(3) \quad A_n = \sum_{i=0}^n \frac{q^{n-i+1} - 1}{q - 1} a_i$$

and

$$(4) \quad \delta_n = A_{n+1} - A_n = \sum_{i=0}^{n+1} q^{n-i+1} a_i.$$

In particular, if $B_1 > 0$, we have $\delta_n \geq 0$.

Proof. The zeta-function can be written as

$$Z(t) = \sum_{n=0}^{+\infty} A_n t^n = \frac{L(t)}{(1-t)(1-qt)} = \frac{\sum_{i=0}^{2g} a_i t^i}{(1-t)(1-qt)}.$$

From the equality $\frac{1}{(1-t)(1-qt)} = \frac{H}{1-t} + \frac{G}{1-qt}$ where $H = \frac{-1}{q-1}$ and $G = \frac{q}{q-1}$, and the power series expansions

$$\frac{1}{1-t} = 1 + t + t^2 + \dots + t^k + \dots$$

and

$$\frac{1}{1-qt} = 1 + qt + q^2 t^2 + \dots + q^k t^k + \dots,$$

we obtain:

$$\sum_{n=0}^{\infty} A_n t^n = \left(\sum_{n=0}^{\infty} (H + q^n G) t^n \right) \times \sum_{n=0}^{\infty} a_n t^n.$$

Hence,

$$A_n = \sum_{i+j=n} (H + q^j G) a_i = \sum_{i+j=n} \left(\frac{-1}{q-1} + \frac{q^{j+1}}{q-1} \right) a_i.$$

Then, we have:

$$A_n = \sum_{i=0}^n \left(\frac{q^{n-i+1} - 1}{q-1} \right) a_i.$$

The value of δ_n follows.

If $B_1 > 0$, let P be a place of degree one. The map ϕ_P from the set of effective divisors of degree n to the set of effective divisors of degree $n+1$ defined by $\phi_P(\mathcal{D}) = \mathcal{D} + P$ is injective. Hence $A_{n+1} \geq A_n$. \square

3.2. Lower bounds on A_n . From Proposition 3.1 we obtain in the next proposition a lower bound on the number of effective divisors of degree n containing in their support only places of some fixed distinct degrees $r_1, r_2, \dots, r_k \geq 1$.

Proposition 3.3. *Let $(r_\mu)_{\mu=1, \dots, p}$ be a family of distinct integers ≥ 1 such that $B_{r_\mu} > 0$ and n be an integer > 0 . Suppose that $B_1 > 0$. Then*

$$(5) \quad A_n \geq \sum_{\mu=1}^p \binom{B_{r_\mu} + m_{r_\mu}(n) - 1}{B_{r_\mu} - 1} \binom{B_1 + s_{r_\mu}(n) - 1}{B_1 - 1}$$

where $m_{r_\mu}(n)$ and $s_{r_\mu}(n)$ are respectively the quotient and the remainder of the Euclidian division of n by r_μ .

Proof. For any integer r_μ , let $a_\mu = (a_{\mu,i})_{i \in \Delta} \in U_n$ such that $a_{\mu,i} = 0$ for $i \in \Delta \setminus \{1, r_\mu\}$, $a_{\mu,1} = s_{r_\mu}(n)$ and $a_{\mu,r_\mu} = m_{r_\mu}(n)$. Then by Proposition (3.1), we have:

$$\begin{aligned} A_n &= \sum_{b \in U_n} \prod_{i \in \Delta} \binom{B_i + b_i - 1}{b_i} \geq \sum_{\mu=1}^p \prod_{i \in \Delta} \binom{B_i + a_{\mu,i} - 1}{a_{\mu,i}} = \\ & \sum_{\mu=1}^p \binom{B_{r_\mu} + m_{r_\mu}(n) - 1}{B_{r_\mu} - 1} \binom{B_1 + s_{r_\mu}(n) - 1}{B_1 - 1}. \end{aligned}$$

□

In particular, if $p = 1$ and $r_1 = 1$ we obtain:

$$A_n \geq \binom{B_1 + n - 1}{n} = \binom{B_1 + n - 1}{B_1 - 1}.$$

Moreover, if the degrees r_μ are > 1 and divide n , we do not need the assumption of the existence of places of degree one.

Proposition 3.4. *Let n be an integer > 0 . Let $(r_\mu)_{\mu=1, \dots, p}$ be a family of distinct integers ≥ 1 dividing n . Suppose that $B_{r_\mu} > 0$ for any $\mu = 1, \dots, p$. Then*

$$(6) \quad A_n \geq \sum_{\mu=1}^p \binom{B_{r_\mu} + m_{r_\mu}(n) - 1}{B_{r_\mu} - 1}$$

where $m_r(n)$ is the quotient of the Euclidian division of n by r_μ .

Proof. For any integer r_μ , let $a_\mu = (a_{\mu,i})_{i \in \Delta} \in U_n$ such that $a_{\mu,i} = 0$ for $i \in \Delta \setminus \{r_\mu\}$ and $a_{\mu,r_\mu} = m_{r_\mu}(n)$. Then by Proposition (3.1), we have:

$$A_n = \sum_{b \in U_n} \prod_{i \in \Delta} \binom{B_i + b_i - 1}{b_i} \geq \sum_{\mu=1}^p \prod_{i \in \Delta} \binom{B_i + a_{\mu,i} - 1}{a_{\mu,i}} =$$

$$\sum_{\mu=1}^p \binom{B_{r_\mu} + m_{r_\mu}(n) - 1}{B_{r_\mu} - 1}.$$

□

Proposition 3.5. *Let $(r_\mu)_{\mu=1,\dots,p}$ be a family of distinct integers > 1 such that $B_{r_\mu} > 0$ and n be an integer > 0 . Suppose that $B_1 \geq 1$. Let $m = (m_{r_\mu})_{\mu=1,\dots,p}$ be a family of integers ≥ 0 such that*

$$\sum_{\mu=1}^p m_{r_\mu} r_\mu \leq n.$$

Then

$$(7) \quad A_n \geq \binom{B_1 + n - 1}{B_1} + \prod_{\mu=1}^p \binom{B_{r_\mu} + m_{r_\mu}}{B_{r_\mu}}.$$

Proof. Let

$$V_n = \left\{ b = (b_{r_\mu})_{\mu=1,\dots,p} \mid b_{r_\mu} \geq 0, \sum_{\mu=1}^p r_\mu b_{r_\mu} \leq n \right\}.$$

As $B_1 \geq 1$ the following holds:

$$A_n = \sum_{b \in U_n} \left[\prod_{i \in \Delta} \binom{B_i + b_i - 1}{b_i} \right] \geq \sum_{b \in V_n} \left[\prod_{\mu=1}^p \binom{B_{r_\mu} + b_{r_\mu} - 1}{b_{r_\mu}} \right].$$

Let $C_n = \prod_{\mu=1}^p \{0, \dots, m_{r_\mu}\}$. Then $C_n \subset V_n$, hence

$$A_n \geq \sum_{b \in C_n} \left[\prod_{\mu=1}^p \binom{B_{r_\mu} + b_{r_\mu} - 1}{b_{r_\mu}} \right].$$

But

$$\begin{aligned} \sum_{b \in C_n} \left[\prod_{\mu=1}^p \binom{B_{r_\mu} + b_{r_\mu} - 1}{b_{r_\mu}} \right] &= \prod_{\mu=1}^p \sum_{b_{r_\mu}=0}^{m_{r_\mu}} \binom{B_{r_\mu} + b_{r_\mu} - 1}{b_{r_\mu}} \\ &= \prod_{\mu=1}^p \binom{B_{r_\mu} + m_{r_\mu}}{m_{r_\mu}}. \end{aligned}$$

In the previous estimate, we did not take into account the effective divisors built only with places of degree one. Hence, the result is obtained by adding the number of such divisors. □

Example 3.6. Let us suppose that $r_\mu = \mu + 1$ for any $1 \leq \mu \leq p$ and that we only know the value of B_1 and that $B_{\mu+1} \geq 1$. Then the m_i are such that $\sum_{i=2}^{p+1} im_i \leq n$ and

$$A_n \geq \binom{B_1 + n - 1}{B_1} + \prod_{i=2}^{p+1} (1 + m_i).$$

Let us set $x_i = 1 + m_i$. Then

$$\sum_{i=2}^{p+1} ix_i \leq \frac{(p+1)(p+2)}{2} - 1 + n.$$

To optimize the choice of the m_i , we will optimize the product $\prod_{i=2}^{p+1} x_i$ under the constraint $\sum_{i=2}^{p+1} ix_i = K$ where $K = \frac{(p+1)(p+2)}{2} - 1 + n$. This is done by the method of Lagrange's multipliers. Let us introduce the following function:

$$L(x_2, \dots, x_{p+1}, \lambda) = \prod_{i=2}^{p+1} x_i - \lambda \left(\sum_{i=2}^{p+1} ix_i - K \right).$$

Let us denote by π_j the incomplete product:

$$x_2 x_3 \cdots x_{j-1} x_{j+1} \cdots x_{p+1}.$$

We have to solve the system:

$$\begin{cases} \frac{\partial L(x_2, \dots, x_{p+1}, \lambda)}{\partial x_2} = \pi_2 - 2\lambda = 0, \\ \vdots \\ \frac{\partial L(x_2, \dots, x_{p+1}, \lambda)}{\partial x_{p+1}} = \pi_{p+1} - (p+1)\lambda = 0, \\ \frac{\partial L(x_2, \dots, x_{p+1}, \lambda)}{\partial \lambda} = \sum_{i=2}^{p+1} ix_i - K = 0. \end{cases}$$

Hence $x_i = \frac{2}{i} x_2$. Hence

$$\sum_{i=2}^{p+1} ix_i = 2px_2 = K.$$

This gives a value for x_2 and then for the x_i . These values are not always integers. Then we have to choose the best way to give to each x_i a integer value near the computed value, in order to obtain an optimal solution for the $m_i = x_i - 1$. For example if $p = 3$ and $n = 9$, then $K = 18$. We conclude that $x_2 = 3$, $x_3 = 2$, $x_4 = 3/2$. Then we can try $m_2 = 3$, $m_3 = 1$ and $m_4 = 0$. or $m_2 = 1$, $m_3 = 1$ and $m_4 = 1$ or $m_2 = 2$, $m_3 = 0$ and $m_4 = 1$. The two first solutions give the maximum 8 for the product $(1 + m_2)(1 + m_3)(1 + m_4)$ (it is impossible to do better).

3.3. Upper Bounds in the case $n \leq g - 1$.

Proposition 3.7. *Let F/\mathbb{F}_q be a function field of genus g and let $L(t) = \sum_{i=0}^{2g} a_i t^i$ be the numerator of its zeta-function. Then*

$$A_{g-k} = \frac{1}{q-1} \left[q^{-k+1} \left(h - \sum_{i=0}^{g+k-1} a_i \right) - \sum_{i=0}^{g-k} a_i \right].$$

Proof. From

$$Z(t) = \sum_{m=0}^{+\infty} A_m t^m = \frac{L(t)}{(1-t)(1-qt)} = \frac{\sum_{i=0}^{2g} a_i t^i}{(1-t)(1-qt)}$$

we deduce that for all $0 \leq m \leq 2g$,

$$A_m = \sum_{i=0}^m \frac{q^{m-i+1} - 1}{q-1} a_i.$$

In particular,

$$(q-1)A_{g-k} = \sum_{i=0}^{g-k} (q^{g-k-i+1} - 1) a_i.$$

Since $a_i = q^{i-g} a_{2g-i}$, for all $i = 0, \dots, g$, we get

$$(q-1)A_{g-k} = q^{g-k+1} \sum_{i=0}^{g-k} q^{-i} a_i - \sum_{i=0}^{g-k} a_i = q^{g-k+1} \sum_{i=0}^{g-k} q^{-i} q^{i-g} a_{2g-i} - \sum_{i=0}^{g-k} a_i.$$

Hence

$$(q-1)A_{g-k} = q^{-k+1} \sum_{i=0}^{g-k} (a_{2g-i} - a_i) - \sum_{i=0}^{g-k} a_i + q^{-k+1} \sum_{i=0}^{g-k} a_i.$$

Furthermore, we know that $h = L(1) = \sum_{i=0}^{2g} a_i$, therefore

$$\sum_{i=0}^{g-k} (a_{2g-i} - a_i) = h - \sum_{i=0}^{g+k-1} a_i - \sum_{i=0}^{g-k} a_i,$$

which completes the proof. \square

Remark 3.8. For $k = 1$ one obtains the two following equalities in the interesting particular case of divisors of degree $g - 1$:

$$(8) \quad A_{g-1} = \frac{1}{q-1} \left[h - \left(a_g + 2 \sum_{i=0}^{g-1} a_i \right) \right].$$

$$(9) \quad A_{g-1} = \sum_{i=0}^{g-1} (a_{2g-i} - a_i).$$

Now we can give general bounds about the quantity $\frac{A_d}{h}$ which can be of interest.

Let us give different useful bounds for $R(F/\mathbb{F}_q)$.

Proposition 3.9.

$$(10) \quad R(F/\mathbb{F}_q) \leq \frac{g}{(\sqrt{q} - 1)^2}.$$

$$(11) \quad R(F/\mathbb{F}_q) \geq \frac{g}{(\sqrt{q} + 1)^2}.$$

$$(12) \quad R(F/\mathbb{F}_q) \leq \frac{1}{(q-1)^2} ((g+1)(q+1) - B_1(F/\mathbb{F}_q)).$$

$$(13) \quad R(F/\mathbb{F}_q) \leq \frac{1}{(q-1)^2} ((g+1)(q+1)).$$

$$(14) \quad R(F/\mathbb{F}_q) \geq \frac{1}{(q+1)^2} ((g+1)(q+1) - B_1(F/\mathbb{F}_q)).$$

Proof. It is known by [7] that the quantity $R(F/\mathbb{F}_q)$ is bounded by the following upper bound:

$$(15) \quad R(F/\mathbb{F}_q) \leq \frac{1}{(q-1)^2} ((g+1)(q+1) - B_1(F/\mathbb{F}_q)).$$

The inequality (12) is obtained as follows:

$$R(F/\mathbb{F}_q) = \sum_{i=1}^g \frac{1}{(1 - \alpha_i)(1 - \bar{\alpha}_i)} = \sum_{i=1}^g \frac{1}{1 + q - (\alpha_i + \bar{\alpha}_i)}.$$

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

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

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

$$\sum_{i=1}^g (\alpha_i + \bar{\alpha}_i) = 1 + q - B_1(F/\mathbb{F}_q),$$

gives the inequality (12). The inequality (12) cannot be improved in the general case. Remark that in the same way we can prove that

$$(16) \quad R(F/\mathbb{F}_q) \geq \frac{1}{(q+1)^2} ((g+1)(q+1) - B_1(F/\mathbb{F}_q)).$$

□

Remark 3.10. Note that Bound (12) is better than Bound (10) because of the lower Weil bound. Indeed,

$$B_1(F/\mathbb{F}_q) \geq q + 1 - 2g\sqrt{q},$$

then

$$\begin{aligned} & \frac{1}{(q-1)^2} ((g+1)(q+1) - B_1(F/\mathbb{F}_q)) \\ & \leq \frac{1}{(q-1)^2} ((g+1)(q+1) - (q+1) + 2g\sqrt{q}). \end{aligned}$$

and we can conclude thanks to the following equality:

$$\frac{1}{(q-1)^2} ((g+1)(q+1) - (q+1) + 2g\sqrt{q}) = \frac{g}{(\sqrt{q}-1)^2}.$$

Moreover (13) is interesting when the number of places of degree one is unknown and $q + 1 - 2g\sqrt{q} < 0$. Indeed in this case (13) is better than (10). On the contrary, if $q + 1 - 2g\sqrt{q} > 0$ (10) is better than (13).

The following theorem gives upper bounds on $\frac{A_d}{h}$.

Theorem 3.11. *For any function field F/\mathbb{F}_q of genus g defined over \mathbb{F}_q and any degree n such that $1 \leq n \leq g-1$, the following holds:*

$$(17) \quad \begin{cases} \frac{A_n}{h} < \frac{1}{2q^{\frac{g-n-1}{2}}(\sqrt{q}-1)^2} & \text{if } n < g-1, \\ \frac{A_n}{h} < \frac{1}{(\sqrt{q}-1)^2} & \text{for } n = g-1. \end{cases}$$

$$(18) \quad \frac{A_n}{h} \leq \frac{g}{q^{g-n-1}(\sqrt{q}-1)^2}.$$

$$(19) \quad \frac{A_n}{h} \leq \frac{(g+1)(q+1)}{q^{g-n-1}(q-1)^2}.$$

Proof. Inequality (17) was obtained in the proof of [2, Theorem 3.3]. We prove here inequalities (18) and (19). Note that Inequality (18) was also proved by I. Cascudo, R. Cramer, C.Xing in [5, Proposition 3.4]. Let us denote by

$$L(t) = \prod_{j=1}^g (1 - \alpha_j t)(1 - \overline{\alpha_j} t)$$

the numerator of the zeta-function of F/\mathbb{F}_q . Then

$$h = L(1) = \prod_{j=1}^g |1 - \alpha_j|^2.$$

The Hecke formula (see [7]) implies

$$(20) \quad A_{g-1} + \sum_{d=0}^{g-2} A_d (1 + q^{g-1-d}) = h \sum_{j=1}^g \frac{1}{|1 - \alpha_j|^2}.$$

But by Formula (10)

$$\sum_{j=1}^g \frac{1}{|1 - \alpha_j|^2} \leq \frac{g}{(\sqrt{q} - 1)^2},$$

then

$$A_{g-1} + \sum_{d=0}^{g-2} A_d (1 + q^{g-1-d}) \leq \frac{gh}{(\sqrt{q} - 1)^2},$$

hence for any n such that $1 \leq n \leq g - 1$ the following holds:

$$A_n q^{g-1-n} \leq \frac{gh}{(\sqrt{q} - 1)^2}.$$

From this last inequality we get (18). Replacing Formula (10) by Formula (13) we obtain (19). \square

If $B_1 \geq 1$ inequalities (18) and (19) can be improved. by the following proposition:

Proposition 3.12. *Let F/\mathbb{F}_q be a function field of genus g defined over \mathbb{F}_q and n an integer such that $1 \leq n < g - 1$. Suppose that $B_1 \geq 1$. Then the following holds:*

$$(21) \quad \frac{A_n}{h} \leq \frac{1}{2(\sqrt{q} - 1)^2 \left(\frac{1}{2} + \sqrt{q} \frac{\sqrt{q^{g-n-1}-1}}{\sqrt{q}-1} \right)}.$$

$$(22) \quad \frac{A_n}{h} \leq \frac{(g+1)(q+1) - B_1}{(q-1)[(q-1)(g-n) + q(q^{g-n-1} - 1)]}.$$

Proof. In order to prove Formula (21) we use the following inequality established in [2, Formula (6)]:

$$2 \sum_{d=0}^{g-2} q^{(g-1-d)/2} A_d + A_{g-1} \leq \frac{h}{(\sqrt{q} - 1)^2}.$$

Then, as $B_1 \geq 1$, we know by Proposition 3.2 that $A_{n+1} \geq A_n$. Hence

$$2A_n \sum_{d=n}^{g-2} q^{(g-1-d)/2} + A_n \leq \frac{h}{(\sqrt{q} - 1)^2},$$

from which we deduce (21).

To prove Formula (22), first we can replace inequalities (10) and (13) by the better inequality (12). Next we know by Proposition 3.2 that $A_{n+1} \geq A_n$. Hence we can deduce from formula (20) the following ones:

$$A_n \left((g-n) + \sum_{d=n}^{g-2} q^{g-d-1} \right) \leq \frac{h}{(q-1)^2} ((g+1)(q+1) - B_1),$$

$$A_n \left((g-n) + \frac{q(q^{g-n-1} - 1)}{(q-1)} \right) \leq \frac{h}{(q-1)^2} ((g+1)(q+1) - B_1).$$

This last inequality leads to the result. \square

If we compare Inequalities (17), (18) and (19) we can see that each of them can be better than the other depending on the parameters. A complete study is done in Annexe A.

We can also obtain bounds concerning directly the quantity A_n from bounds on $\frac{A_n}{h}$ by using the Weil bounds [11] [12]:

$$(23) \quad (\sqrt{q} - 1)^{2g} \leq h \leq (\sqrt{q} + 1)^{2g}.$$

A better upper bound for h than the Weil bound, due to P. Lebacque and A. Zykin [8] can be used if we know upper bounds for the number of rational points of the curve $X(\mathbb{F}_{q^k})$ over the fields \mathbb{F}_{q^k} for $1 \leq k \leq N$ where N is an integer ≥ 1 :

$$(24) \quad h \leq q^g \exp \left(\sum_{k=1}^N \frac{1}{kq^k} |X(\mathbb{F}_{q^k})| - \sum_{k=1}^N \frac{1+q^{-k}}{k} + \frac{2g}{(\sqrt{q}-1)(N+1)q^{\frac{N}{2}}} \right).$$

Moreover, in the special case $n = g - 1$, the estimates for $\frac{A_{g-1}}{h}$ can be improved. Let us introduce

$$Q_{r,s} = \sum_{k=0}^s \frac{1}{q^{\frac{rk}{2}}} \binom{B_r + k - 1}{k}.$$

Lemma 3.13.

$$Q_{r,s} = \left(\frac{q^{\frac{r}{2}}}{q^{\frac{r}{2}} - 1} \right)^{B_r} - B_r \binom{B_r + s}{B_r} \int_0^{\frac{1}{q^{\frac{r}{2}}}} \frac{\left(\frac{1}{q^{\frac{r}{2}}} - t\right)^s}{(1-t)^{B_r+s+1}} dt.$$

Proof. Let us set

$$S_r(X) = \sum_{k=0}^{\infty} X^k \binom{B_r + k - 1}{k}, \quad T_r(X, s) = \sum_{k=0}^s X^k \binom{B_r + k - 1}{k},$$

$$\text{and } R_r(X, s) = \sum_{k=s+1}^{\infty} X^k \binom{B_r + k - 1}{k}.$$

Let us remark that

$$Q_{r,s} = T_r\left(\frac{1}{q^{\frac{r}{2}}}, s\right) \quad \text{and} \quad S_r(X) = \frac{1}{(1-X)^{B_r}}$$

which converges for $|X| < 1$ and moreover

$$S_r(X) = T_r(X, s) + R_r(X, s).$$

By the Taylor Formula, we get

$$R_r(X, s) = B_r \binom{B_r + s}{B_r} \int_0^X \frac{(X-t)^s}{(1-t)^{B_r+s+1}} dt.$$

Then

$$Q_{r,s} = \left(\frac{q^{\frac{r}{2}}}{q^{\frac{r}{2}} - 1} \right)^{B_r} - B_r \binom{B_r + s}{B_r} \int_0^{\frac{1}{q^{\frac{r}{2}}}} \frac{\left(\frac{1}{q^{\frac{r}{2}}} - t\right)^s}{(1-t)^{B_r+s+1}} dt.$$

□

Lemma 3.14. *Let F/\mathbb{F}_q be a function field of genus g defined over \mathbb{F}_q . Let let $m = (m_r)_{r \in \Delta}$ be a finite sequence of integers such that $m_r \geq 0$ and $\sum_{r \in \Delta} r m_r \leq g - 2$. Then the following inequality holds:*

$$\sum_{k=0}^{g-2} \frac{A_k}{q^{\frac{k}{2}}} \geq \prod_{r \in \Delta} Q_{r, m_r}.$$

Proof. By Proposition 3.1 we know that

$$A_k = \sum_{b \in U_k} \left[\prod_{i \in \Delta} \binom{B_i + b_i - 1}{b_i} \right].$$

If one set

$$V = \bigcup_{k=0}^{g-2} U_k = \left\{ b = (b_r)_{r \in \Delta} \mid b_r \geq 0 \text{ and } \sum_{r \in \Delta} r b_r \leq g - 2 \right\}$$

the following holds:

$$\sum_{k=0}^{g-2} \frac{A_k}{q^{\frac{k}{2}}} = \sum_{b \in V} \prod_{r \in \Delta} \frac{1}{q^{\frac{r b_r}{2}}} \binom{B_r + b_r - 1}{b_r}.$$

Let C be the subset of V defined by

$$C = \prod_{r \in \Delta} \{0, \dots, m_r\}.$$

Then

$$\begin{aligned} \sum_{k=0}^{g-2} \frac{A_k}{q^{\frac{k}{2}}} &\geq \sum_{b \in C} \prod_{r \in \Delta} \frac{1}{q^{\frac{r b_r}{2}}} \binom{B_r + b_r - 1}{b_r} = \\ &\prod_{r \in \Delta} \sum_{k=0}^{m_r} \frac{1}{q^{\frac{r k}{2}}} \binom{B_r + k - 1}{k} = \prod_{r \in \Delta} Q_{r, m_r}. \end{aligned}$$

□

Proposition 3.15. *Let F/\mathbb{F}_q be a function field of genus g defined over \mathbb{F}_q . Let $m = (m_r)_{r \in \Delta}$ be a finite sequence of integers such that $m_r \geq 0$ and $\sum_{r \in \Delta} r m_r \leq g - 2$.*

Then the following inequality holds:

$$(25) \quad A_{g-1} \leq \frac{h}{(\sqrt{q} - 1)^2} - 2q^{\frac{g-1}{2}} \prod_{r \in \Delta} Q_{r, m_r},$$

$$(26) \quad A_{g-1} \leq \frac{(\sqrt{q} + 1)^{2g}}{(\sqrt{q} - 1)^2} - 2q^{\frac{g-1}{2}} \prod_{r \in \Delta} Q_{r, m_r},$$

where for any $r \geq 1$ and $s \geq 0$ the following holds:

$$Q_{r, s} = \left(\frac{q^{\frac{r}{2}}}{q^{\frac{r}{2}} - 1} \right)^{B_r} - B_r \binom{B_r + s}{B_r} \int_0^{\frac{1}{q^{\frac{r}{2}}}} \frac{\left(\frac{1}{q^{\frac{r}{2}}} - t\right)^s}{(1-t)^{B_r + s + 1}} dt.$$

Proof. Let us recall the following inequality established in [2, Formula (6)]:

$$2q^{(g-1)/2} \sum_{d=0}^{g-2} \frac{A_d}{q^{d/2}} + A_{g-1} \leq \frac{h}{(\sqrt{q}-1)^2}.$$

We know by Proposition 3.14 that

$$\sum_{k=0}^{g-2} \frac{A_k}{q^{\frac{k}{2}}} \geq \prod_{r \in \Delta} Q_{r, m_r}.$$

Then the inequality (25) holds.

The inequality (26) directly follows from the inequality (25) and from the upper Weil bound.

Finally, Lemma 3.13 gives the last equality. \square

Remark 3.16. The inequality (26) can be improved by using, if possible, the upper bound (24).

Theorem 3.17. *For any curve X of genus g defined over \mathbb{F}_q . If $1 \leq d \leq g-1$ the following holds:*

$$(27) \quad A_d \leq \frac{g(\sqrt{q}+1)^{2g}}{q^{g-d-1}(\sqrt{q}-1)^2}.$$

Proof. From (18) and (23) we obtain (27). As previously remarked, if possible, we can use (24) instead of (23) and get the bound:

$$(28) \quad A_d \leq \frac{gq^g \exp\left(\sum_{k=1}^N \frac{1}{kq^k} |X(\mathbb{F}_{q^k})| - \sum_{k=1}^N \frac{1+q^{-k}}{k} + \frac{2g}{(\sqrt{q}-1)(N+1)q^{\frac{N}{2}}}\right)}{q^{g-d-1}(\sqrt{q}-1)^2}.$$

\square

4. ASYMPTOTICAL CASE

The study of the asymptotic behavior of certain quantities associated to curves or function fields can be done from many point of view depending on the parameter tending to infinity. The simpler cases are described by the two following situations:

- **Increasing the size of the definition function field of one fixed curve.** The first case corresponds to the situation of a unique fixed curve X_0 of genus g and a fixed degree d_0 . Let us remark that if the curve X_0 is defined on the finite field \mathbb{F}_{q_1} , it is also defined on any extension \mathbb{F}_q of \mathbb{F}_{q_1} , and then we can study the asymptotic behavior of quantities related to the curve X_0

when q is growing to infinity. In particular in section 4.1 we will study the asymptotic behaviour of

$$\frac{A_{d_0}(F_0/\mathbb{F}_q)}{h(F_0/\mathbb{F}_q)}$$

when q is growing to infinity, where d_0 is a fixed degree and F_0/\mathbb{F}_q , the function field over \mathbb{F}_q associated to the curve X_0 .

- **Case of a family of curves defined over the same finite field \mathbb{F}_q .** Let $(X_k)_{k \geq 1}$ be a family of curves defined over \mathbb{F}_q . We study the sequence of function fields $(F_k/\mathbb{F}_q)_k$. Let us denote by $g_k = g(X_k)$ the genus of the curve X_k . We will suppose in the following that the genus sequence $(g_k)_k$ is growing to infinity. In section 4.2 we will study the asymptotic behaviour of many interesting quantities when k (and then g_k) is growing to infinity, and when the degree d is linked to g_k by a relation. We will study in particular the case where d is a linear function of g_k .

Some asymptotic behaviours are deduced from absolute *formulae*, namely true for any value of the variables $(g(X), q, d)$. Many such *formulae* exist, each of them being mainly adapted to a particular asymptotic study. We can consider this point of view by using the results obtained in the section 3.

4.1. Case of a fixed curve and a fixed degree. In this section the curve X of genus g is fixed and d is a fixed integer such that $d \leq g - 1$. Let us recall that $A_d(F/\mathbb{F}_q)$ is the number of degree d effective divisors of F/\mathbb{F}_q and that $h(F/\mathbb{F}_q)$ is its class number. We give here the asymptotic behaviour of the quotient

$$\frac{A_d(F/\mathbb{F}_q)}{h(F/\mathbb{F}_q)}.$$

Theorem 4.1. *Let us suppose that $g \geq 1$ and $d \leq g - 1$. Then when q is growing to infinity, the following holds:*

$$\frac{A_d(F/\mathbb{F}_q)}{h(F/\mathbb{F}_q)} = \frac{1}{q^{g-d}} \left(1 + O\left(\frac{1}{q}\right) \right),$$

where the O Landau function depends upon X and d .

This theorem is a consequence of the two following *lemmata*. Let us denote by W_d^0 the following set:

$$W_d^0 = \{[D] \in \mathcal{P}ic_d(X) \mid \dim(D) > 0\}.$$

If $d \leq g - 1$, the elements of W_d^0 are special divisor classes.

$$|X(\mathbb{F}_q)| = q + 1 - \text{trace}(\pi).$$

Lemma 4.2. *If $g \geq 1$ and $d \leq g$ then when q tends to infinity*

$$|W_d^0(\mathbb{F}_q)| = q^d - q^{d-1} \text{trace}(\pi) + O(q^{d-1}).$$

Proof. The restriction of the projection

$$\Pi : \text{Div}_d(X) \rightarrow \text{Pic}_d(X)$$

gives a surjective morphism

$$\Pi : \text{Div}_d^+(X) \rightarrow W_d^0.$$

The scheme W_d^0 is a dimension d irreducible normal sub-variety of $\text{Pic}_d(X)$ defined over \mathbb{F}_q (see [1, p. 190], [9, Prop. 5.1, p. 182]). The Albanese variety of W_d^0 is $\mathcal{J}ac(X)$ (see [9, Prop. 5.3, p. 183]). We conclude by [6, Cor. 11.4]. \square

Lemma 4.3. *If $g \geq 1$ and $d \leq g - 1$ then when q tends to infinity*

$$A_d(F/\mathbb{F}_q) = |W_d^0(\mathbb{F}_q)| + O(q^{d-1}).$$

Proof. Recall that

$$A_d(F/\mathbb{F}_q) = \sum_{[D] \in \text{Pic}_d(\mathbb{F}_q)} \frac{q^{\dim(D)} - 1}{q - 1}.$$

The dimension of included varieties

$$W_d^r = \{[D] \in \text{Pic}_d(\mathbb{F}_q) \mid \dim(D) \geq r + 1\}$$

is the Brill-Noether number (see [1, p. 180])

$$\rho(r) = g - (r + 1)(g - d + r),$$

and $W_d^r = \emptyset$ if $r > d/2$ by the Clifford's theorem. When q is growing to infinity the following holds:

$$\begin{aligned} A_d(F/\mathbb{F}_q) &= \sum_{l=1}^{+\infty} \frac{q^l - 1}{q - 1} (|W_d^{l-1}(\mathbb{F}_q)| - |W_d^l(\mathbb{F}_q)|), \\ A_d(F/\mathbb{F}_q) &= \sum_{l=1}^{+\infty} \sum_{i=0}^{l-1} q^i (|W_d^{l-1}(\mathbb{F}_q)| - |W_d^l(\mathbb{F}_q)|), \\ A_d(F/\mathbb{F}_q) &= \sum_{l=0}^{+\infty} \sum_{i=0}^l q^i |W_d^l(\mathbb{F}_q)| - \sum_{l=1}^{+\infty} \sum_{i=0}^{l-1} q^i |W_d^l(\mathbb{F}_q)|, \\ A_d(F/\mathbb{F}_q) &= |W_d^0(\mathbb{F}_q)| + \sum_{l=1}^{+\infty} q^l |W_d^l(\mathbb{F}_q)|, \\ A_d(F/\mathbb{F}_q) &\leq |W_d^0(\mathbb{F}_q)| + \sum_{l=1}^{+\infty} q^{l+\rho(l)} (1 + O(q^{-1/2})), \end{aligned}$$

$$A_d(F/\mathbb{F}_q) \leq |W_d^0(\mathbb{F}_q)| + q^d \sum_{l=1}^{+\infty} q^{-l^2} q^{-(g-d)l} (1 + O(q^{-1/2})).$$

But when q tends to infinity

$$\sum_{l=1}^{+\infty} q^{-l^2} \sim q^{-1}$$

hence

$$A_d(F/\mathbb{F}_q) \leq |W_d^0(\mathbb{F}_q)| + O(q^{d-1}).$$

On the other hand $A_d(F/\mathbb{F}_q) \geq |W_d^0(\mathbb{F}_q)|$, then

$$A_d(F/\mathbb{F}_q) = |W_d^0(\mathbb{F}_q)| + O(q^{d-1}).$$

□

Proof of Theorem 4.1. Let us remark that $h(F/\mathbb{F}_q) = |\mathcal{P}ic_d(\mathbb{F}_q)| = q^g - q^{g-1} \text{trace}(\pi) + O(q^{g-1})$. Then we deduce the result from Lemma 4.2 and Lemma 4.3. □

4.2. Case of a fixed finite field.

4.2.1. *Introduction.* When, for a given finite ground field, the sequence of the genus of a sequence of algebraic function fields tends to infinity, there exist asymptotic *formulae* for different numerical invariants. In this section, we are interested by the asymptotic study with respect to the genus g of the number of effective divisors of certain degrees.

Let $(X_k)_k$ be a sequence of smooth irreducible curves defined over the finite field \mathbb{F}_q . We denote by $\mathcal{F}/\mathbb{F}_q = (F_k/\mathbb{F}_q)_k$ the corresponding sequence of algebraic function fields defined over \mathbb{F}_q . We denote by g_k the genus of X_k and we suppose that the sequence $(g_k)_k$ is growing to infinity. For any integer k , let d_k be an integer. We denote by $A_{d_k,k}$ the number $A_{d_k}(F_k/\mathbb{F}_q)$ of degree d_k effective divisors of F_k/\mathbb{F}_q and by h_k its class number.

M. Tsfasman and S. Vladut give in [10, Theorem 5.1], under some assumption on the behaviour of $\frac{d_k}{g_k}$ when k is growing to infinity, the following asymptotic estimate when the family $\mathcal{F}/\mathbb{F}_q = (F_k/\mathbb{F}_q)_k$ is an asymptotically exact family:

$$(29) \quad \frac{A_{d_k,k}}{h_k} \sim \frac{1}{q^{g_k-d_k}} \frac{q}{q-1}.$$

Remark 4.4. The assumption done in [10, Theorem 5.1] is made precise in [10, Lemma 5.1]. It turns out that it is verified if there is an $\epsilon > 0$ and an integer $k_0 \geq 1$ such that for all $k \geq k_0$ the inequality $\frac{d_k}{g_k} \geq 2\lambda + \epsilon$

holds, where λ is the unique root of the equation $H_{1+\frac{1}{\sqrt{q}}}(x) = 0$ on $[0, 1]$, $H_y(x)$ being the entropy function defined by

$$H_y(x) = x \log_y(y-1) - x \log_y(x) - (1-x) \log_y(1-x).$$

4.2.2. *General sequences.* In this section, we consider general sequences of algebraic function fields namely which are not necessarily asymptotically exact. Then, we obtain a result in two parts which respectively follows from *formulae* (17) and (18) of Section 3. For each case, we choose the formula giving the best result.

Theorem 4.5. *Let $(d_k)_k$ be a sequence of integers such that $1 \leq d_k \leq g_k - 1$. Let us set $d_k = g_k - \phi(g_k)$ where ϕ is a function with integer value. If there exists an integer k_0 such that for any integer k , the function ϕ is such that*

$$0 \leq \phi(g_k) \leq 2 \log_q(g_k) + 1$$

then

$$(30) \quad 0 \leq \limsup_{k \rightarrow +\infty} \frac{A_{d_k, k}}{h_k} \leq \limsup_{k \rightarrow +\infty} \frac{\sqrt{q}}{2(\sqrt{q}-1)^2} q^{-\frac{\phi(g_k)}{2}},$$

else, supposing that the following limit exists $\delta = \lim_{k \rightarrow +\infty} \frac{d_k}{g_k}$ and satisfies $0 \leq \delta \leq 1$, we have

$$(31) \quad \limsup_{k \rightarrow +\infty} \left(\frac{A_{d_k, k}}{h_k} \right)^{\frac{1}{g_k}} \leq \frac{1}{q^{1-\delta}}.$$

Proof. Note that for the borderline case $d_k = g_k - 1$, the estimate (17) is clearly better than the estimate (18). Now we suppose that $d_k < g_k - 1$. The inequality (17) implies the inequality (30) and the inequality (18) implies the inequality (31). Indeed, first let us compare the two estimates (17) and (18). The estimate (17) is better than (18) if and only if

$$\frac{1}{2q^{\frac{g_k - d_k - 1}{2}} (\sqrt{q} - 1)^2} \leq \frac{g_k}{q^{g_k - d_k - 1} (\sqrt{q} - 1)^2}$$

namely,

$$\phi(g_k) \leq 2 \log_q(g_k) + 1 + 2 \log_q(2).$$

Then if there exists an integer k_0 such that for any integer $k \geq k_0$, $\phi(g_k) \leq 2 \log_q(g_k) + 1$, we obtain the formula (30) else, if the limit $\delta = \lim_{k \rightarrow +\infty} \frac{d_k}{g_k}$ exists and satisfies $0 \leq \delta \leq 1$, we obtain the estimate (31). \square

Corollary 4.6. *Let us set $d_k = g_k - \phi(g_k)$ where ϕ is a function with integer value. If for any integer k , the function ϕ is such that*

$$0 \leq \phi(g_k) \leq 2 \log_q(g_k) + 1$$

and if $\lim_{k \rightarrow +\infty} \phi(g_k) = +\infty$, then we have

$$(32) \quad \lim_{k \rightarrow +\infty} \frac{A_{d_k, k}}{h_k} = 0.$$

Proof. The result is a straightforward consequence of formula (30). \square

APPENDIX A

A.1. Comparison of bounds. Let us denote by K_{17} , K_{18} and K_{19} the respective second members of the inequalities (17), (18) and (19). In Remark 3.10 we proved that $K_{18} \leq K_{19}$ if and only if $g \leq \frac{1}{2} \left(\sqrt{q} + \frac{1}{\sqrt{q}} \right)$. In the following we compare K_{17} to K_{18} and to K_{19} .

(1) Case $d = g - 1$.

$$K_{17} = \frac{1}{(\sqrt{q} - 1)^2}, K_{18} = \frac{g}{(\sqrt{q} - 1)^2}, K_{19} = \frac{(g + 1)(q + 1)}{(q - 1)^2}.$$

We remark that in this case $K_{17} \leq K_{18}$.

(a) For $g \leq \frac{1}{2} \left(\sqrt{q} + \frac{1}{\sqrt{q}} \right)$: from the previous results the following inequalities hold:

$$K_{17} \leq K_{18} \leq K_{19}.$$

(b) For $g \geq \frac{1}{2} \left(\sqrt{q} + \frac{1}{\sqrt{q}} \right)$:

$$\frac{K_{17}}{K_{19}} = \frac{(\sqrt{q} + 1)^2}{(g + 1)(q + 1)}.$$

But

$$(g + 1)(q + 1) - (\sqrt{q} + 1)^2 = gq - 2\sqrt{q} + g.$$

The last right member is a quadratic polynomial in \sqrt{q} which has a discriminant ≤ 0 . The sign is constant and ≥ 0 . We conclude that:

$$K_{17} \leq K_{19} \leq K_{18}.$$

(2) Case $d = g - 2$. In this case

$$K_{17} = \frac{1}{2\sqrt{q}(\sqrt{q} - 1)^2}, K_{18} = \frac{g}{q(\sqrt{q} - 1)^2},$$

$$K_{19} = \frac{(g + 1)(q + 1)}{q(q - 1)^2}.$$

(a) For $g \leq \frac{1}{2} \left(\sqrt{q} + \frac{1}{\sqrt{q}} \right)$:

$$\frac{K_{17}}{K_{18}} = \frac{\sqrt{q}}{2g}.$$

(i) If $\frac{1}{2}\sqrt{q} \leq g \leq \frac{1}{2} \left(\sqrt{q} + \frac{1}{\sqrt{q}} \right)$, then the following inequalities hold:

$$K_{17} \leq K_{18} \leq K_{19}.$$

(ii) If $g \leq \frac{1}{2}\sqrt{q}$ then

$$\frac{K_{17}}{K_{19}} = \frac{\sqrt{q}(\sqrt{q}+1)^2}{2(g+1)(q+1)}.$$

But as $g \leq \frac{1}{2}\sqrt{q}$, the following holds:

$$\begin{aligned} \sqrt{q}(\sqrt{q}+1)^2 - 2(g+1)(q+1) &\geq \\ 2gq + 2q + 2g - (2gq + 2g + 2q + 2) &\geq \end{aligned}$$

and

$$\sqrt{q}(\sqrt{q}+1)^2 - 2(g+1)(q+1) \geq 2.$$

Hence $K_{19} \leq K_{17}$ and

$$K_{18} \leq K_{19} \leq K_{17}.$$

(b) For $g \geq \frac{1}{2} \left(\sqrt{q} + \frac{1}{\sqrt{q}} \right)$:

$$\begin{aligned} 2(g+1)(q+1) - \sqrt{q}(\sqrt{q}+1)^2 &\geq \\ \left(\sqrt{q} + \frac{1}{\sqrt{q}} \right) (q+1) + 2(q+1) - \sqrt{q}(\sqrt{q}+1)^2 &= \\ &(\sqrt{q}+1)^2. \end{aligned}$$

Then $K_{17} \leq K_{19}$ and

$$K_{17} \leq K_{19} \leq K_{18}.$$

(3) Case $d \leq g - 3$.

(a) The case $q = 2$ and $d = g - 3$ ($g \geq 3$) is the only case such that

$$\left(\sqrt{q} + \frac{1}{\sqrt{q}} \right) > q^{\frac{g-d-1}{2}}.$$

By a simple computation we obtain:

$$K_{17} \leq K_{19} \leq K_{18}.$$

(b) For $q \neq 2$ or $d < g - 3$ we have

$$\frac{K_{17}}{K_{19}} = \frac{q^{\frac{g-d-1}{2}}}{2g}.$$

(i) If we have the following inequalities

$$\frac{1}{2} \left(\sqrt{q} + \frac{1}{\sqrt{q}} \right) \leq g \leq \frac{1}{2} q^{\frac{g-d-1}{2}}$$

then

$$K_{19} \leq K_{18} \leq K_{17}.$$

(ii) If

$$g \leq \frac{1}{2} \left(\sqrt{q} + \frac{1}{\sqrt{q}} \right),$$

then $K_{18} \leq K_{17}$, $K_{18} \leq K_{19}$ and

$$\frac{K_{17}}{K_{19}} = \frac{q^{\frac{g-d-1}{2}} (\sqrt{q} + 1)^2}{2(g+1)(q+1)}.$$

But

$$\begin{aligned} & q^{\frac{g-d-1}{2}} (\sqrt{q} + 1)^2 - 2(g+1)(q+1) \geq \\ & q^{\frac{g-d}{2}} (q + 2\sqrt{q} + 1) - (q+1 + 2\sqrt{q})(q+1) = \\ & (q + 2\sqrt{q} + 1) \left(q^{\frac{g-d}{2}} - (q+1) \right). \end{aligned}$$

(A) If $q = 2$ and $g - d \geq 4$ then

$$q^{\frac{g-d}{2}} - (q+1) \geq q^2 - q - 1 > 0.$$

(B) If $q \geq 3$ (and $g - d \geq 3$) then

$$q^{\frac{g-d}{2}} - (q+1) \geq q^{\frac{3}{2}} - (q+1) > 0.$$

In any cases $K_{19} \leq K_{17}$. Hence

$$K_{18} \leq K_{19} \leq K_{17}.$$

(iii) If

$$g \geq \frac{1}{2} q^{\frac{g-d-1}{2}},$$

then $K_{17} \leq K_{18}$, $K_{19} \leq K_{18}$ and

$$\frac{K_{17}}{K_{19}} = \frac{q^{\frac{g-d-1}{2}} (\sqrt{q} + 1)^2}{2(g+1)(q+1)}.$$

Let us set

$$g = \frac{1}{2} q^{\frac{g-d-1}{2}} + a$$

where $a \geq 0$. Then the sign of $K_{17} - K_{19}$ is the sign of

$$2(g-a)(\sqrt{q}+1)^2 - 2(g+1)(q+1),$$

namely the sign of

$$2g\sqrt{q} - (q+1) - a(\sqrt{q}+1)^2.$$

Remark that $2g\sqrt{q} - (q+1)$ is ≥ 0 . Hence:

(A) if

$$a \leq \frac{2g\sqrt{q} - (q+1)}{(\sqrt{q}+1)^2}$$

then $K_{19} \leq K_{17}$ and

$$K_{19} \leq K_{17} \leq K_{18}.$$

(B) else if

$$a \geq \frac{2g\sqrt{q} - (q+1)}{(\sqrt{q}+1)^2}$$

then $K_{19} \geq K_{17}$ and

$$K_{17} \leq K_{19} \leq K_{18}.$$

A.2. Examples. Let us give some examples where we compare bounds K_{17} , K_{18} , and K_{19} :

(1) g and $d < g - 1$ are fixed, q large enough, then Bound K_{18} is the best of the three bounds: we are in cases (2) (a) (ii) or (3) (b) (ii);

(2) g is fixed and $d = g - 1$, for any q , Bound K_{17} is the best one: we are in case (1);

(3) q and d are fixed, g large enough, then Bound K_{19} is the best one: we are in the case (3) (b) (i);

(4) q fixed, g and d large:

(a) $d = g - c$ where c is a constant, then Bound K_{17} is the best one; for $c = 1$ we are in the case (1), for $c = 2$ we are in the case (2) (b) and for $c < 2$, we are in the case (3) (a) or in the case (3) (b) (iii) (B);

(b) $d = g(1 - \epsilon)$ where ϵ is a constant, then Bound K_{19} is the best one; we are in the case (3) (b) (i);

(c) $d = g - \alpha \log(g) - 1$, then

$$\frac{g-d-1}{2} = \frac{\alpha}{2} \log(g) \quad \text{and} \quad q^{\frac{g-d-1}{2}} = g^{\frac{\alpha}{2} \log(g)}.$$

(i) if $\alpha > \frac{2}{\log(q)}$ then we are in the case (3) (b) (i), hence the best bound is (19).

(ii) if $\alpha \leq \frac{2}{\log(q)}$ then we are in the case (3) (b) (iii) (B), hence the best bound is (17).

The following example is an example of the case (3) (b) (iii) (A). Set $q = 4$, $g = 520$ and $d = 509$. Hence $(g - d - 1)/2 = 5$. Then

$$\frac{1}{2}q^{\frac{g-d-1}{2}} = 512 < g.$$

We can compute

$$a = g - \frac{1}{2}q^{\frac{g-d-1}{2}} = 8.$$

Now

$$\frac{2g\sqrt{q} - (q + 1)}{(\sqrt{q} + 1)^2} = \frac{2075}{9}.$$

Hence

$$a \leq \frac{2g\sqrt{q} - (q + 1)}{(\sqrt{q} + 1)^2}.$$

Here the best bound is K_{19} .

REFERENCES

- [1] Enrico Arbarello, Maurizio Cornalba, Philip Griffiths, and Joe Harris. *Geometry of Algebraic Curves*, volume I. Springer, 1985.
- [2] Stéphane Ballet, Christophe Ritzenthaler, and Robert Rolland. On the existence of dimension zero divisors in algebraic function fields defined over \mathbb{F}_q . *Acta Arithmetica*, 143(4):377–392, 2010.
- [3] Stéphane Ballet and Robert Rolland. Lower bounds on the class number of algebraic function fields defined over any finite field. *Journal de théorie des nombres de Bordeaux*, 24(3):505–540, 2012.
- [4] Stéphane Ballet, Robert Rolland, and Seher Tutdere. Lower bounds on the number of rational points of Jacobians over finite fields and application to algebraic function fields in towers. *Moscow Mathematical Journal*, 15(3):425–433, 2015.
- [5] Ignacio Cascudo, Ronald Cramer, and Chaoping Xing. Torsion limits and Riemann-Roch Systems for Function Fields and Applications. *Transactions on Information Theory*, 60(7):3871–3888, 2014.
- [6] Sudhir Ghorpade and Gilles Lachaud. Etale cohomology, Lefschetz theorems and number of points of singular varieties over finite fields. *Moscow Mathematical Journal*, 2(3):589–631, 2002.
- [7] Gilles Lachaud and Mireille Martin-Deschamps. Nombre de points des jacobiniennes sur un corps fini. *Acta Arithmetica*, 56(4):329–340, 1990.
- [8] Philippe Lebacque and Alexey Zykin. On the number of rational points of jacobians over finite fields. *Acta Arithmetica*, 169:373–384, 2015.
- [9] James Milne. Jacobian varieties. In Michael Artin, Gary Cornell, and Joseph Silverman, editors, *Arithmetic geometry*, pages 167–212. Springer, New-York, 1986. Proceedings of a conference held July 30 through August 10, 1984 at the University of Connecticut at Storrs.
- [10] Michael Tsfasman and Serguei Vlăduț. Asymptotic properties of zeta-functions. *Journal of Mathematical Sciences*, 84(5):1445–1467, 1997.

- [11] 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.
- [12] André Weil. *Basic Number Theory*. Springer, 1967.

STÉPHANE BALLET, AIX MARSEILLE UNIV, CNRS, CENTRALE MARSEILLE,
I2M, MARSEILLE, FRANCE, CASE 907 13288 MARSEILLE CEDEX 9, FRANCE
E-mail address: `ballet@iml.univ-mrs.fr`

GILLES LACHAUD, AIX MARSEILLE UNIV, CNRS, CENTRALE MARSEILLE,
I2M, MARSEILLE, FRANCE, CASE 907 13288 MARSEILLE CEDEX 9, FRANCE

ROBERT ROLLAND AIX MARSEILLE UNIV, CNRS, CENTRALE MARSEILLE,
I2M, MARSEILLE, FRANCE, CASE 907 13288 MARSEILLE CEDEX 9, FRANCE
E-mail address: `robert.rolland@acrypta.fr`