ACTA ARITHMETICA
143.4 (2010)

On the existence of dimension zero divisors in algebraic function fields defined over $\mathbb{F}_q$

by

S. Ballet, C. Ritzenthaler and R. Rolland (Marseille)

1. Introduction. Let $\mathbf{F}/\mathbb{F}_q$ be an algebraic function field of one variable defined over a finite field $\mathbb{F}_q$. We will always suppose that the full constant field of $\mathbf{F}/\mathbb{F}_q$ is $\mathbb{F}_q$ and denote by g the genus of $\mathbf{F}/\mathbb{F}_q$. If D is a (rational) divisor we recall that the $\mathbb{F}_q$-*Riemann–Roch vector space* associated to D is the following subspace of rational functions:

$$\mathcal{L}(D) = \{x \in \mathbf{F}/\mathbb{F}_q \mid (x) \geq -D\} \cup \{0\}. \tag{1}$$

By the Riemann–Roch theorem, the dimension of this vector space, denoted by $\dim(D)$, is related to the genus of $\mathbf{F}/\mathbb{F}_q$ and the degree of D by

$$\dim(D) = \deg(D) - g + 1 + \dim(\kappa - D), \tag{2}$$

where κ denotes a canonical divisor of $\mathbf{F}/\mathbb{F}_q$ of degree $2g-2$. In this relation, the complementary term $i(D) = \dim(\kappa - D)$ is called the *index of speciality* and is not easy to compute in general. Note that we always have $i(D) \geq 0$. In particular, a divisor D is called *non-special* when $i(D)$ is zero, and *special* if $i(D) > 0$. Many deep results on such divisors have been obtained in the dual language of curves when the field of definition is algebraically closed. See for instance [1] for a beautiful survey over $\mathbb{C}$. On the contrary, few results are known when the rationality of the divisor is taken into account, as in our context where we require the divisor D to be defined over $\mathbb{F}_q$. We refer to [4] for known results on the existence of non-special divisors of degree g and $g-1$.

In the present article, we study a natural generalization of certain results obtained in [4] by looking at *dimension zero divisors*, i.e. such that $\dim(D) = 0$. Clearly, such a divisor has degree less than or equal to $g-1$. The non-special divisors of degree $g-1$ form the borderline case. In Corollary 3.4 we prove that for $g \geq 1$, $q \geq 4$ (resp. $q = 3$, resp. $q = 2$) and $k \geq 1$ (resp.

2010 *Mathematics Subject Classification*: Primary 14H05; Secondary 12E20.
Key words and phrases: finite field, function field, non-special divisor.

DOI: 10.4064/aa143-4-4

$k \geq 2$, resp. $k \geq 5$) there always exists a dimension zero divisor of degree $g-k$. When $q \leq 3$, it is not known whether there exist infinitely many function fields without non-special degree $g-1$ divisors (see [4, Rem. 12] for examples with $g \leq 3$). For $q = p \leq 3$, we slightly clarify the situation by showing that when the Jacobian of $\mathbf{F}/\mathbb{F}_q$ is ordinary, there always exists a non-special divisor of degree $g-1$ (Proposition 4.3). More generally, we show the existence of a dimension zero divisor of degree $\gamma - 1$ where γ is the so called p-rank of $\mathbf{F}/\mathbb{F}_q$. Also, if $\mathbf{F}/\mathbb{F}_2$ has at least three degree one places, then one can replace $k \geq 5$ by $k \geq 2$ in Corollary 3.4.

If the zeta function of $\mathbf{F}/\mathbb{F}_q$ is known, we give a sufficient condition on its coefficients to have a dimension zero divisor of degree $g-k$ (Theorem 3.7). In general (Remark 3.10) the knowledge of the zeta function is not sufficient to distinguish between function fields with or without dimension zero divisor of a certain degree. However, if $\mathbf{F}/\mathbb{F}_q$ is hyperelliptic, using results from [11], we can give a necessary and sufficient condition (Theorem 3.9).

Many inequalities and techniques we use are refinements of the ones developed in [4]. More specifically, most results are derived from the inequality $A_m < h$ where A_m is the number of effective divisors of degree m and h is the divisor class number (see Lemma 3.1). To the best of our knowledge, the use of the p-rank and the hyperelliptic case are new.

Apart from theoretical interest, our study is motivated by the appearance of such divisors in many applications (see [13] and [3]). Hence we prove not only existence results but also density results in order to justify the good behavior of certain algorithms.

Here is an overview of the paper. In Section 2, we recall the basic definitions and notation for algebraic function fields, and elementary and known results on dimension zero divisors. In Section 3, we give our main results concerning the existence of dimension zero divisors. In Section 4, we study the special cases $q = 2, 3$ under various hypotheses. In Section 5, we prove that a random draw of a divisor of degree $g-k$ gives with high probability a dimension zero divisor. Then we compare the results obtained in Section 3 with the ones obtained in [16] and [13] which can be deduced directly from the known asymptotical properties of the zeta functions.

2. Preliminaries

2.1. Notation. Let us recall the usual notation (for the basic notions related to an algebraic function field $\mathbf{F}/\mathbb{F}_q$ see [14]). Let $\mathbf{F}/\mathbb{F}_q$ be a function field of genus g. For any integer $k \geq 1$ we denote by $\mathsf{P}_k(\mathbf{F}/\mathbb{F}_q)$ the set of places of degree k and by $B_k(\mathbf{F}/\mathbb{F}_q)$ the cardinality of this set. We define $\mathsf{P}(\mathbf{F}/\mathbb{F}_q) = \bigcup_k \mathsf{P}_k(\mathbf{F}/\mathbb{F}_q)$. The divisor group of $\mathbf{F}/\mathbb{F}_q$ is denoted by $\mathsf{D}(\mathbf{F}/\mathbb{F}_q)$.

If a divisor $D \in \mathsf{D}(\mathbf{F}/\mathbb{F}_q)$ is such that

$$D = \sum_{P \in \mathsf{P}(\mathbf{F}/\mathbb{F}_q)} n_P P,$$

the *support* of D is the finite set

$$\mathrm{supp}(D) = \{P \in \mathsf{P}(\mathbf{F}/\mathbb{F}_q) \mid n_P \neq 0\}$$

and its *degree* is

$$\deg(D) = \sum_{P \in \mathsf{P}(\mathbf{F}/\mathbb{F}_q)} n_P \deg(P).$$

We denote by $\mathsf{D}_n(\mathbf{F}/\mathbb{F}_q)$ the set of divisors of degree n. We say that the divisor D is *effective* if $n_P \geq 0$ for each $P \in \mathrm{supp}(D)$; we denote by $\mathsf{D}_n^+(\mathbf{F}/\mathbb{F}_q)$ the set of effective divisors of degree n and write $A_n = \#\mathsf{D}_n^+(\mathbf{F}/\mathbb{F}_q)$.

The *dimension* of a divisor D, denoted by $\dim(D)$, is the dimension of the vector space $\mathcal{L}(D)$ defined by (1).

Let $x \in \mathbf{F}/\mathbb{F}_q$. We denote by (x) the divisor associated to the rational function x, that is,

$$(x) = \sum_{P \in \mathsf{P}(\mathbf{F}/\mathbb{F}_q)} v_P(x) P,$$

where v_P is the valuation at the place P. A divisor of the form (x) is called a *principal divisor*, and the set of principal divisors is a subgroup of $\mathsf{D}_0(\mathbf{F}/\mathbb{F}_q)$ denoted by $\mathsf{Princ}(\mathbf{F}/\mathbb{F}_q)$. The factor group

$$\mathcal{C}(\mathbf{F}/\mathbb{F}_q) = \mathsf{D}(\mathbf{F}_q)/\mathsf{Princ}(\mathbf{F}/\mathbb{F}_q)$$

is called the *divisor class group*. If D_1 and D_2 are in the same class, i.e. the divisor $D_1 - D_2$ is principal, we write $D_1 \sim D_2$. We denote by $[D]$ the class of the divisor D.

If $D_1 \sim D_2$, then

$$\deg(D_1) = \deg(D_2), \quad \dim(D_1) = \dim(D_2),$$

so that we can define the degree $\deg([D])$ and the dimension $\dim([D])$ of a class. Since the degree of a principal divisor is zero, we can define the subgroup $\mathcal{C}(\mathbf{F}/\mathbb{F}_q)^0$ of classes of degree zero divisors in $\mathcal{C}(\mathbf{F}/\mathbb{F}_q)$. It is a finite group and we denote by h its order, called the *class number* of $\mathbf{F}/\mathbb{F}_q$. Moreover if

$$L(t) = \sum_{i=0}^{2g} a_i t^i = \prod_{i=1}^{g} [(1 - \pi_i t)(1 - \overline{\pi}_i t)]$$

with $|\pi_i| = \sqrt{q}$ is the numerator of the zeta function of $\mathbf{F}/\mathbb{F}_q$, we have $h = L(1)$. Finally we denote by $h_{n,k}$ the number of classes of divisors of degree n and of dimension k.

In the following, we may simultaneously use the dual language of (smooth, absolutely irreducible, projective) curves by associating to $\mathbf{F}/\mathbb{F}_q$ a unique ($\mathbb{F}_q$-isomorphism class of a) curve $\mathbf{C}/\mathbb{F}_q$ of genus g and conversely to such a curve its function field. Because, by F. K. Schmidt's theorem (cf. [14, Corollary V.1.11]) there always exists a rational divisor of degree 1, the group $\mathcal{C}(\mathbf{F}/\mathbb{F}_q)^0$ is isomorphic to the group of $\mathbb{F}_q$-rational points on the Jacobian of $\mathbf{C}$, denoted $\mathcal{J}\mathrm{ac}(\mathbf{C})$. In particular $h(\mathbf{F}/\mathbb{F}_q) = \#\mathcal{J}\mathrm{ac}(\mathbf{C})(\mathbb{F}_q)$.

2.2. Elementary results on dimension zero divisors. Let $\mathbf{F}/\mathbb{F}_q$ be a function field of genus $g > 0$. We are interested in dimension zero divisors. From the Riemann–Roch theorem, they are the divisors D such that $[D]$ does not contain an effective divisor. If $\deg(D) < 0$ then D is automatically a dimension zero divisor. Therefore, in what follows we assume that $\deg(D) \geq 0$. Note that the divisor with empty support exists and is effective. So, if $\deg(D) = 0$, then D is a dimension zero divisor if and only if D is not principal. Finally, as said in the introduction, since $i(D) \geq 0$, it follows easily from the Riemann–Roch theorem that a dimension zero divisor is necessarily of degree less than g. The following lemma shows that among them, the degree $g-1$ dimension zero divisors represent the extreme case.

LEMMA 2.1. *Let $D \in \mathsf{D}_{g-1}(\mathbf{F}/\mathbb{F}_q)$ be a dimension zero divisor of degree $g-1$. If $B_1(\mathbf{F}/\mathbb{F}_q) > 0$ then for all $k > 0$, there exists a dimension zero divisor of degree $g-k$.*

Proof. Let $P \in \mathsf{P}_1(\mathbf{F}/\mathbb{F}_q)$. Suppose that $D - kP$ is not a dimension zero divisor. Then by the Riemann–Roch theorem, there exists a function $x \in \mathbf{F}$ such that $(x) + D - kP$ is an effective divisor. But then $(x) + D$ is also effective and D is not a dimension zero divisor, a contradiction. ∎

Note that if degree D is $g-1$, then D is a dimension zero divisor if and only if $i(D) = 0$. Such divisors are particular cases of non-special divisors. Over an algebraically closed field, it is easy to prove the existence of a non-special divisor of degree $g-1$ for any function field $\mathbf{F}$. However, if we impose the rationality of such a divisor then the question is more subtle and has been studied in [4] and [2]. Among other results proved there, the following are interesting for our purpose.

PROPOSITION 2.2. *If $B_1(\mathbf{F}/\mathbb{F}_q) \geq g+1$, then there is a non-special divisor such that* $\deg(D) = g-1$ *and* $\mathrm{supp}(D) \subset \mathsf{P}_1(\mathbf{F}/\mathbb{F}_q)$.

REMARK 2.3. Assume that $D \in \mathsf{D}_g(\mathbf{F}/\mathbb{F}_q)$ is an effective non-special divisor of degree $g \geq 1$. If there exists a degree one place P such that $P \notin \mathrm{supp}(D)$, then $D - P$ is a non-special divisor of degree $g-1$.

Using Lemma 2.1, we know that we get in these cases dimension zero divisors of degree $g-k$ for all $k>0$.

Theorem 2.4. *Let $\mathbf{F}/\mathbb{F}_q$ be a function field of genus $g(\mathbf{F})\geq 2$. If $q\geq 4$, then there is a non-special divisor of degree $g(\mathbf{F})-1$.*

Finally, in order to get rid of the small genus cases, we give the following proposition.

Proposition 2.5. *Let $\mathbf{F}/\mathbb{F}_q$ be a function field of genus $g(\mathbf{F})\leq 2$. There is always a dimension zero divisor of degree zero except in the following cases:*

(i) *$g=1$ and $\mathbf{F}/\mathbb{F}_q$ is given by*

$$\begin{cases} y^2+y=x^5+x^3+1, & q=2,\\ y^2=x^3+2x+2, & q=3,\\ y^2+y=x^3+a, & q=4 \text{ with } a^2+a+1=0; \end{cases}$$

(ii) *$g=2$, $q=2$ and $\mathbf{F}/\mathbb{F}_2$ is given by*

$$y^2+y=x^5+x^3+1 \quad \text{or} \quad y^2+(x^3+x+1)y=x^6+x^5+x^4+x^3+x^2+x+1.$$

Let $\mathbf{F}/\mathbb{F}_q$ be a function field of genus $g(\mathbf{F})=2$. There is always a dimension zero divisor of degree 1 except if $\mathbf{F}/\mathbb{F}_q=\mathbb{F}_2(x,y)/\mathbb{F}_2$ with

$$y^2+y=x^5+x^3+1 \quad \text{or} \quad y^2+y=(x^4+x+1)/x.$$

Proof. As said, a degree zero divisor is zero-dimensional if and only if it is not principal. Hence, a function field $\mathbf{F}/\mathbb{F}_q$ has no dimension zero divisor of degree zero if and only if $h(\mathbf{F}/\mathbb{F}_q)=1$. When $g=1$, it is well known that the only cases are the ones indicated in the proposition. For $g=2$, this was proved in [8] and [7]. For the degree 1 case, this has been studied in [4, Th. 11]. ■

In the following, we assume that $g(\mathbf{F})>2$.

3. On the existence of dimension zero divisors. In this section we establish our main results on the existence of divisors of degree $g-k$ and dimension zero for an algebraic function field $\mathbf{F}/\mathbb{F}_q$ of genus g defined over $\mathbb{F}_q$.

3.1. Relation with the Jacobian. First, let us give a key lemma for proving the existence of divisors of dimension zero.

Lemma 3.1. *Let n be an integer and assume that $A_n=\#\mathsf{D}_n^+(\mathbf{F}/\mathbb{F}_q)<h$, where h is the class number of $\mathbf{F}/\mathbb{F}_q$. Then there exists a divisor of degree n and dimension zero. More precisely, the number of classes of divisors of degree n and dimension zero, denoted $h_{n,0}$, is greater than or equal to $h-A_n$.*

Proof. We know by F. K. Schmidt's theorem (cf. [14, Corollary V.1.11]) that there always exists a divisor of degree 1, say $D_0 \in \mathsf{D}_1(\mathbf{F}/\mathbb{F}_q)$. For all n, we denote by ψ the map from $\mathsf{D}_n(\mathbf{F}/\mathbb{F}_q)$ into the Jacobian of $\mathbf{F}/\mathbb{F}_q$ given by

$$\psi(D) = [D - nD_0].$$

Since we assumed that $A_n < h$, we have

$$\#\psi(\mathsf{D}_n^+(\mathbf{F}/\mathbb{F}_q)) \le A_n < h,$$

so the restriction of ψ to $\mathsf{D}_n^+(F/\mathbb{F}_q)$ is not surjective. If $[D']$ is a class of degree 0 not in the image of ψ, then $[D' + nD_0]$ does not contain an effective divisor, hence $D' + nD_0$ is a dimension zero divisor of degree n. The number of classes $[D]$ of degree n where D is not equivalent to a positive divisor is $h_{n,0} \ge h - A_n$. ∎

Remark 3.2. We can give examples where a counterpart of the first claim in Lemma 3.1 does not hold: for instance the function field $\mathbf{F}_1/\mathbb{F}_2$: $y^2 + (x^4 + x^3 + x)y = x^{10} + x^6 + 1$ (resp. $\mathbf{F}_2/\mathbb{F}_2 : y^2 + (x^4 + x^3 + x^2)y = x^{10} + x^7 + x^3$) is of genus 3 (resp. 4) with class number 8 (resp. 10) and $A_2 = 9$ (resp. $A_3 = 13$). However $\mathbf{F}_1/\mathbb{F}_2$ (resp. $\mathbf{F}_2/\mathbb{F}_2$) is ordinary and one can apply Proposition 4.1 below to show that there is a dimension zero divisor of degree 2 (resp. 3) in $\mathsf{D}(\mathbf{F}_1/\mathbb{F}_2)$ (resp. in $\mathsf{D}(\mathbf{F}_2/\mathbb{F}_2)$).

3.2. Main results. Some applications (cf. [13] and [3]) require many linearly independent divisors of dimension zero. Then we are interested not only in the existence of such a divisor, but also in their number.

Let k be a positive integer. Let us set the following notation:

$$C_q = \begin{cases} 2(\sqrt{q}-1)^2/\sqrt{q} & \text{if } k \ge 2, \\ (\sqrt{q}-1)^2/\sqrt{q} & \text{if } k = 1, \end{cases}$$

$$l_q(k) = C_q q^{k/2},$$

$$\Delta_q = \begin{cases} q^{(g-k)/2} & \text{if } k \ge 2, \\ 2q^{(g-1)/2} & \text{if } k = 1. \end{cases}$$

Then the following result holds:

Theorem 3.3. *Assume that k is a positive integer such that*

$$-2\log_q(C_q) \le k. \tag{3}$$

Then there is at least one dimension zero divisor of degree $g-k$ in the set $\mathsf{D}_{g-k}(\mathbf{F}/\mathbb{F}_q)$. Moreover, the number $h_{n,0}$ of (classes of) linearly independent divisors of degree $n = g-k$ and dimension zero satisfies

$$h_{n,0} \ge h\left(1 - \frac{1}{l_q(k)}\right) + \Delta_q. \tag{4}$$

Proof. Note that

$$\log_q(l_q(k)) = \log_q(C_q) + k/2 \geq 0,$$

so $l_q(k) \geq 1$. From the functional equation of the zeta function, it can be deduced (see [10, Lemma 3(i)]) that, for $g \geq 1$, one has

$$A_n = q^{n+1-g} A_{2g-2-n} + h\,\frac{q^{n+1-g}-1}{q-1} \quad \text{for all } 0 \leq n \leq 2g-2. \tag{5}$$

For $g \geq 2$, it follows from (5) (see [6] or [10, Lemma 3 and proof of Lemma 6]) that

$$\sum_{n=0}^{g-2} A_n t^n + \sum_{n=0}^{g-1} q^{g-1-n} A_n t^{2g-2-n} = \frac{L(t) - ht^g}{(1-t)(1-qt)}.$$

Substituting $t = q^{-1/2}$ in the last identity, we obtain

$$2\sum_{n=0}^{g-2} q^{-n/2} A_n + q^{-(g-1)/2} A_{g-1} = \frac{h - q^{g/2} L(q^{-1/2})}{(q^{1/2}-1)^2 q^{(g-1)/2}}.$$

For $j = 1, \ldots, g$ write $\pi_j = q^{1/2} e^{i\theta_j}$. Since

$$L(q^{-1/2}) = \prod_{j=1}^{g} [(1 - \pi_j q^{-1/2})(1 - \overline{\pi}_j q^{-1/2})] = 2^{2g} \cdot \prod_{j=1}^{g} \sin^2(\theta_j/2) \geq 0,$$

we have

$$2\sum_{n=0}^{g-2} q^{(g-1-n)/2} A_n + A_{g-1} \leq \frac{h}{(\sqrt{q}-1)^2}. \tag{6}$$

Note that $A_0 = 1$ and $A_i \geq 0$ for all $i > 0$. Hence (6) implies, for $k \geq 2$,

$$A_{g-k} \leq \frac{h}{2q^{(k-1)/2}(\sqrt{q}-1)^2} - q^{(g-k)/2}.$$

In the same way we get

$$A_{g-1} \leq \frac{h}{(\sqrt{q}-1)^2} - 2q^{(g-1)/2}.$$

In any case

$$A_{g-k} \leq \frac{h}{l_q(k)} - \Delta_q < h.$$

Then there exist $h_{n,0} \geq h - A_{g-k}$ linearly independent divisors of degree $g-k$ and dimension zero and so (4) holds. ∎

Corollary 3.4. *There exists a dimension zero divisor of degree $g-k$ in $\mathsf{D}_{g-k}(\mathbf{F}/\mathbb{F}_q)$ as soon as*

- *for $q = 2$, $k \geq 5$;*
- *for $q = 3$, $k \geq 2$;*
- *for $q \geq 4$, $k \geq 1$.*

Hence, for $q \geq 4$ the situation is optimal. This can be seen as a generalization of Theorem 2.4.

Remark 3.5. However, the bound on $h_{n,0}$ is not optimal. For instance, we have already noticed that every degree 0 divisor which is not principal is zero-dimensional. Hence $h_{g,0} = h - 1$. From [6], one knows that for any field $\mathbf{F}/\mathbb{F}_q$ of genus g,

$$h \geq \left\lceil q^{g-1} \frac{(q-1)^2}{(q+1)(g+1)} \right\rceil.$$

A simple computation shows that for any q,

$$h - 1 > h\left(1 - \frac{1}{l_q(g)}\right) + \Delta_q \quad \text{for } g > 20.$$

If more is known about the zeta function of $\mathbf{F}/\mathbb{F}_q$, other estimates can be deduced. In the following lemma, we give the value of A_{g-k} in terms of the coefficients of the polynomial $L(t)$.

Lemma 3.6. *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. Then*

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

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 $i = 0, \ldots, g$, we get

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

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. ∎

Theorem 3.7. *Let $k \geq 1$ be a fixed integer. If $\mathbf{F}/\mathbb{F}_q$ is an algebraic function field such that $q \geq 3$ and $q^{-k+1}\sum_{i=0}^{g+k-1} a_i + \sum_{i=0}^{g-k} a_i \geq 0$ (resp. $q = 2$ and $q^{-k+1}\sum_{i=0}^{g+k-1} a_i + \sum_{i=0}^{g-k} a_i > 0$), then there exists a dimension zero divisor of degree $n = g - k$. Moreover, the number $h_{n,0}$ of linearly independent divisors of degree $n = g - k$ and dimension zero is such that*

$$h_{n,0} \geq h - \frac{1}{q-1}\Big[q^{-k+1}\Big(h - \sum_{i=0}^{g+k-1} a_i\Big) - \sum_{i=0}^{g-k} a_i\Big]. \tag{7}$$

Proof. By Lemma 3.6, we have the inequality $A_{g-k} < h$. The result follows by using Lemma 3.1. ∎

Example 3.8. We can apply the previous theorem to classical types of algebraic function fields, in particular a maximal function field $\mathbf{F}/\mathbb{F}_{q^2}$ over $\mathbb{F}_{q^2}$ or its descent over $\mathbb{F}_q$ if it exists. In the first case, one has $L(t) = (1+qt)^{2g}$ and

$$h_{n,0} \geq h - \frac{1}{q^2-1}\Big[q^{-2k+2}\Big(h - \sum_{i=0}^{g+k-1}\binom{2g}{i}q^i\Big) - \sum_{i=0}^{g-k}\binom{2g}{i}q^i\Big].$$

In the latter, $L(t) = (1 + qt^2)^g$ and

$$h_{n,0} \geq h - \frac{1}{q-1}\Big[q^{-k+1}\Big(h - \sum_{i=0}^{\lfloor (g+k-1)/2\rfloor}\binom{g}{i}q^i\Big) - \sum_{i=0}^{\lfloor (g-k)/2\rfloor}\binom{g}{i}q^i\Big].$$

For instance, for the descent of the (maximal) genus 3 hermitian field over $\mathbb{F}_3$, one gets $h_{2,0} \geq 42$ and $h_{1,0} \geq 60$ (compare with $h_{1,0} \geq 12$ obtained from formula (4) of Theorem 3.3).

In the particular case where $\mathbf{F}/\mathbb{F}_q$ is hyperelliptic, one can give a necessary and sufficient condition in terms of the coefficients of L to obtain a dimension zero divisor of degree $g - k$.

Theorem 3.9. *If $\mathbf{F}/\mathbb{F}_q$ is a hyperelliptic algebraic function field of genus $g > 2$, the number $h_{g-k,0}$ of linearly independent divisors of degree $g-k$ and dimension zero is*

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

Proof. We use results from [11, Sec. 4]. Let $h_{n,i}$ be the number of classes of divisors of degree n and of dimension $i \geq 0$ of $\mathbf{F}/\mathbb{F}_q$. By [11, Prop. 4.3], for $0 \leq n \leq 2g-2$ and $i > 0$, one has

$$h_{n,i} = A_{n-2i+2} - (q+1)A_{n-2i} + qA_{n-2i-2}.$$

Now for any n,

$$h = \sum_{i=0}^{\infty} h_{n,i}$$

so

$$h_{n,0} = h - \sum_{i=1}^{\infty} h_{n,i}.$$

By the expression of $h_{n,i}$ for $i > 0$ above and the fact that $A_i = 0$ if $i < 0$ we get

$$h_{g-k,0} = h - (A_{g-k} - qA_{g-k-2}).$$

Using the expressions of A_{g-k} from Lemma 3.6 and

$$h = \sum_{i=0}^{g} a_i + \sum_{i=0}^{g-1} q^{g-i} a_i$$

after some simplifications we get the desired equality. ∎

Remark 3.10. However, in general, the knowledge of the zeta function is not sufficient to characterize the existence of a dimension zero divisor. For instance the genus 3 function field $\mathbf{F}_1/\mathbb{F}_2 : y^2 + y = x^7 + x^6 + 1$ has the same L-polynomial $L(t) = 8t^6 - 8t^5 + 4t^4 - 2t^3 + 2t^2 - 2t + 1$ as $\mathbf{F}_2/\mathbb{F}_2$: $y^3 + x^2y^2 + (x^3+1)y = x^4 + x^3 + 1$. Now from [4, Rem. 12], $\mathbf{F}_2/\mathbb{F}_2$ has no degree 2 divisor of dimension zero whereas $\mathbf{F}_1/\mathbb{F}_2$ (which is hyperelliptic) has by Theorem 3.9.

4. Particular cases: the cases of $\mathbb{F}_2$ and $\mathbb{F}_3$

4.1. Assumption on the p-rank. Let $\mathbf{C}/k$ be a genus g (smooth, projective, absolutely irreducible) curve over a finite field $k = \mathbb{F}_{p^n}$. Classically, one defines the *p-rank* γ of this curve as the integer $0 \leq \gamma \leq g$ such that $\#\mathcal{J}\mathrm{ac}(\mathbf{C})[p](\overline{k}) = p^\gamma$. In particular $\mathbf{C}$ is said to be *ordinary* if $\gamma = g$. There is another equivalent characterization in terms of the L-polynomial, namely $\gamma = \deg(L(t) \pmod{p})$ (see [9]). In particular, $\mathbf{C}$ is ordinary if and only if p does not divide a_g.

Proposition 4.1. *Let $\mathbf{C}$ be an ordinary curve of genus $g > 0$ over a finite field k of characteristic 2. There is always a degree $g-1$ dimension zero divisor on $\mathbf{C}$.*

Proof. Let $f \in k(\mathbf{C})$ with $df \neq 0$. Developing f in power series at any point of $\mathbf{C}$, we see that df has only zeros and poles of even multiplicity. Hence there exists a rational divisor of degree $(2g-2)/2 = g-1$ such that $(df) = 2D_0$. It is easy to show that the class of this divisor does not depend on the choice of f and it is called the *canonical theta characteristic divisor.*

In [15, Prop. 3.1], it is shown that there is a bijection between $\mathcal{L}(D_0)$ and the space of exact regular differentials (i.e. the regular differentials ω such that $\omega = df$ for $f \in k(\mathbf{C})$). Now by [12, Prop. 8], a regular differential ω is exact if and only if $\mathcal{C}(\omega) = 0$ where $\mathcal{C}$ is the Cartier operator. Moreover by [12, Prop. 10], $\mathcal{J}\mathrm{ac}(\mathbf{C})$ is ordinary if and only if $\mathcal{C}$ is bijective. So the only exact regular differential is 0 and $\dim(D_0) = 0$. Hence D_0 is the divisor we were looking for. ∎

Corollary 4.2. *Let $\mathbf{C}/\mathbb{F}_2$ be an ordinary curve of genus $g > 0$. Assume that $\#\mathbf{C}(\mathbb{F}_2) > 0$. Then for all $k > 0$, there exists a dimension zero divisor of degree $g - k$.*

Note that the previous proof gives a way to explicitly construct a degree $g - 1$ divisor of dimension zero. We will now generalize Proposition 4.1 but without such an explicit construction.

Proposition 4.3. *Let $\mathbf{C}$ be a curve of genus $g > 0$ over a finite field $\mathbb{F}_q$ of characteristic p and of p-rank γ. There is always a degree $\gamma - 1$ dimension zero divisor on $\mathbf{C}$.*

Proof. On one hand, we have already pointed out in the proof of Lemma 3.6 that for all $0 \le m \le 2g$,

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

Reducing modulo p, we get

$$A_m \equiv \sum_{i=0}^{m} a_i \pmod{p}.$$

On the other hand, with the same notation as in the proof of Theorem 3.9,

$$A_m = \sum_{i=1}^{\infty} \frac{q^i - 1}{q - 1} h_{m,i}.$$

Reducing modulo p, we get

$$A_m \equiv \sum_{i=1}^{\infty} h_{m,i} \pmod{p}.$$

Now,

$$h = \sum_{i=0}^{\infty} h_{m,i} \quad \text{and} \quad h \equiv \sum_{i=0}^{\gamma} a_i \pmod{p}.$$

Hence, for $m = \gamma - 1$,

$$h_{m,0} = h - \sum_{i=1}^{\infty} h_{m,i} \equiv h - A_m \equiv \sum_{i=0}^{\gamma} a_i - \sum_{i=0}^{\gamma-1} a_i \equiv a_\gamma \not\equiv 0 \pmod{p}.$$

Thus, $h_{\gamma-1,0}$ is not zero and hence is positive. ∎

Remark 4.4. Note that this proposition is interesting only in the case where $q = 2$ and $\gamma = g - k$ with $k \leq 3$, or $q = 3$ and $\gamma = g$. Indeed, Corollary 3.4 gives a better result for the other values of q and k.

4.2. Assumption on the number of rational points. As we have seen in Proposition 2.2, if we know that there are many ($> g$) degree one places then there is always a dimension zero divisor of degree $g - k$ for all $k > 0$. We want to relax the hypothesis in the case of $q = 2$ for $k > 1$. To do so, we need the following lemma which can be found in [10].

Lemma 4.5. *If $B_1(\mathbf{F}/\mathbb{F}_q) \geq m \geq 1$, then for all $n \geq 2$ one has*

$$A_n \geq mA_{n-1} - \frac{m(m-1)}{2} A_{n-2}.$$

Then the following result improves Proposition 2.2.

Theorem 4.6. *If $q = 2$ ($g \geq 3$) and $B_1(\mathbf{F}/\mathbb{F}_2) \geq 3$ then*

$$A_{g-k} < h(\mathbf{F}/\mathbb{F}_2)$$

for any integer $k \geq 2$. Therefore there exists a divisor of degree $g - k$ and dimension zero for any $k \geq 2$.

Proof. From the inequality (6), we obtain

$$4A_{g-3} + 2\sqrt{2}\, A_{g-2} + A_{g-1} \leq \frac{h}{(\sqrt{2}-1)^2} = (3 + 2\sqrt{2})h. \tag{8}$$

Assume that $B_1(\mathbf{F}/\mathbb{F}_2) \geq m = 3$. Then by Lemma 4.5 applied with $n = g-1$, we have $A_{g-1} + 3A_{g-3} \geq 3A_{g-2}$. Hence, using (8), we obtain

$$A_{g-3} + (3 + 2\sqrt{2})A_{g-2} \leq (3 + 2\sqrt{2})h.$$

Moreover, it is clear that $A_{g-3} \geq 1$ because if $g = 3$ then $A_{g-3} = A_0 = 1$, and if $g > 3$ then $A_{g-3} \geq B_1(\mathbf{F}/\mathbb{F}_2) = m = 3$. Hence, we deduce that if $B_1(\mathbf{F}/\mathbb{F}_2) \geq 3$ and $g \geq 3$, then $A_{g-2} < h$. We can apply Lemma 2.1 to get the result. ∎

5. Density of dimension zero divisors

5.1. General result. In many situations, divisors of dimension zero are needed. The bilinear multiplication algorithm of D. Chudnovsky and G. Chudnovsky (see [5]), for instance, requires the random choice of good divisors to set up the algorithmic infrastructure. In this context, we draw at random a divisor until we obtain a divisor having the needed properties. From an algorithmic point of view, one can ask what the expected complexity is to construct the required divisors. Until now, it is not at all clear that this construction is practical (cf. [13, Rem. 5]). However, the experiments show that in each particular case, this random draw quickly gives us a solution. The following result explains why this method works.

PROPOSITION 5.1. *Let* $\mathsf{D}_n(\mathbf{F}/\mathbb{F}_q)$ *be the set of divisors of degree* $n = g-k$ *with* $k \geq 1$, *provided with the equiprobability distribution. If* $k \geq -2\log_q(C_q)$ *then the probability to draw a degree* $g-k$ *divisor of dimension zero is greater than or equal to* $1 - 1/l_q(k)$ *where*

$$l_q(k) = C_q q^{k/2}$$

and

$$C_q = \begin{cases} 2(\sqrt{q}-1)^2/\sqrt{q} & \text{if } k \geq 2, \\ (\sqrt{q}-1)^2/\sqrt{q} & \text{if } k = 1. \end{cases}$$

Proof. For any integer n, the probability to draw a dimension zero divisor among the divisors of degree n is equal to the probability to draw a divisor class of dimension zero among the classes of degree n. We have seen in Theorem 3.3 that the number of classes of linearly independent divisors of degree $n = g - k$ and dimension zero is

$$h_{n,0} \geq h\left(1 - \frac{1}{l_q(k)}\right) + \Delta_q > h\left(1 - \frac{1}{l_q(k)}\right).$$

Since the number of classes of degree n is equal to h, we get the result. ∎

Note that this probability does not depend upon the value of g and tends to 1 as $k \to \infty$. In particular g and k can grow simultaneously to infinity. For example we can take $k = \lfloor \log_q(g) \rfloor$ which satisfies the inequality (3) and which tends to infinity as $g \to \infty$.

For practical cases, using Proposition 5.1, we see that it is not necessary to take a very large k to obtain a probability very close to 1. For example if $q = 16$ and $k = 3$, which is a rather small value, the probability to draw a divisor of degree $g-3$ and dimension zero is $\geq 287/288 \simeq 0.996$. If $q = 256$ and $k = 1$ the probability to draw a non-special divisor of degree $g-1$ is $\geq 224/225 \simeq 0.995$.

5.2. Comparison with asymptotical results. In this section, we compare the previous results with those obtained under asymptotical assumptions on the zeta functions by M. Tsfasman [16], M. Tsfasman and S. Vladut [17] and I. Shparlinski, M. Tsfasman and S. Vladut [13]. First, let us recall the notion of asymptotically exact sequence of algebraic function fields introduced in [16].

DEFINITION 5.2. Consider a sequence $\mathcal{F}/\mathbb{F}_q = (\mathbf{F}_k/\mathbb{F}_q)_{k\geq 1}$ of algebraic function fields $\mathbf{F}_k/\mathbb{F}_q$ defined over $\mathbb{F}_q$ of genus g_k. We suppose that the sequence of genus g_k is an increasing sequence growing to infinity. The sequence $\mathcal{F}/\mathbb{F}_q$ is called *asymptotically exact* if for all $m \geq 1$ the following limit exists:

$$\beta_m(\mathcal{F}/\mathbb{F}_q) = \lim_{g_k \to \infty} \frac{B_m(\mathbf{F}_k/\mathbb{F}_q)}{g_k}$$

where $B_m(\mathbf{F}_k/\mathbb{F}_q)$ is the number of places of degree m on $\mathbf{F}_k/\mathbb{F}_q$.

Now, let us recall two results used by I. Shparlinski, M. Tsfasman and S. Vladut in [13]. These results follow easily from Corollary 2 and Theorem 6 of [16]. Note that the proof of Theorem 6 of [16] can be found in [17].

Lemma 5.3. *Let $\mathcal{F}/\mathbb{F}_q = (\mathbf{F}_k/\mathbb{F}_q)_{k\geq 1}$ be an asymptotically exact sequence of algebraic function fields defined over $\mathbb{F}_q$ and h_k be the class number of $\mathbf{F}_k/\mathbb{F}_q$. Then*

$$\log_q(h_k) = g_k\left(1 + \sum_{m=1}^{\infty} \beta_m \log_q\left(\frac{q^m}{q^m - 1}\right)\right) + o(g_k).$$

Lemma 5.4. *Let A_{d_k} be the number of effective divisors of degree d_k on $\mathbf{F}_k/\mathbb{F}_q$. If*

$$d_k \geq g_k\left(\sum_{m=1}^{\infty} \frac{m\beta_m}{q^m - 1}\right) + o(g_k)$$

then

$$\log_q(A_{d_k}) = d_k + g_k \sum_{m=1}^{\infty} \beta_m \log_q\left(\frac{q^m}{q^m - 1}\right) + o(g_k).$$

These asymptotical properties were established in [16] and [17] in order to estimate the class number h of algebraic function fields of genus g defined over $\mathbb{F}_q$ and also in order to estimate their number of classes of effective divisors of degree $m \leq g - 1$. Namely, I. Shparlinski, M. Tsfasman and S. Vladut used in [13] the inequality $2A_{\lceil g_k(1-\epsilon)\rceil} < h_k$ where $0 < \epsilon < 1/2$ and k is large enough, under the hypothesis of Lemma 5.3. In the same spirit, we generalize their result in the following proposition and corollary.

Proposition 5.5. *Let $\mathcal{F}/\mathbb{F}_q = (\mathbf{F}_k/\mathbb{F}_q)_{k\geq 1}$ be an asymptotically exact sequence of algebraic function fields defined over $\mathbb{F}_q$. Let ϵ and l be real numbers such that $0 < \epsilon < 1/2$ and $l \geq 1$. Then there exists an integer k_0 such that for any integer $k \geq k_0$,*

$$lA_{\lceil g_k(1-\epsilon)\rceil} < h_k.$$

Proof. The total number of linear equivalence classes of an arbitrary degree equals the divisor class number h_k of $\mathbf{F}_k/\mathbb{F}_q$, which is given by Lemma 5.3. Moreover, for g_k sufficiently large, we have

$$\sum_{m=1}^{\infty} \frac{m\beta_m}{q^m - 1} \leq \frac{1}{\sqrt{q}+1} \sum_{m=1}^{\infty} \frac{m\beta_m}{q^{m/2} - 1} < \frac{1}{2}$$

since $q \geq 2$ and $\sum_{m=1}^{\infty} \frac{m\beta_m}{q^{m/2}-1} \leq 1$ by Corollary 1 of [16]. As $\epsilon < 1/2$, one has

$$\lceil g_k(1-\epsilon)\rceil \geq g_k(1-\epsilon) \geq g_k\left(\sum_{m=1}^{\infty} \frac{m\beta_m}{q^m-1}\right) + o(g_k)$$

for k large enough.

Therefore, we can apply Lemma 5.4 and compare $\log_q(lA_{\lceil g_k(1-\epsilon)\rceil})$ with $\log_q(h_k)$ given by Lemma 5.3. Hence, there exists an integer k_0 such that $lA_{\lceil g_k(1-\epsilon)\rceil} < h_k$ for $k \geq k_0$. ∎

Corollary 5.6. *Let $\mathcal{F}/\mathbb{F}_q = (\mathbf{F}_k/\mathbb{F}_q)_{k\geq 1}$ be an asymptotically exact sequence of algebraic function fields defined over $\mathbb{F}_q$. Let ϵ be a real number such that $0 < \epsilon < 1/2$ and $\phi = o(g_k)$ a function such that $g_k(1-\epsilon)+\phi(g_k)$ is an integer. Then there exists an integer k_0 such that for any integer $k \geq k_0$, there is a divisor of degree $g_k(1-\epsilon)+\phi(g_k)$ and dimension zero in $\mathsf{D}(\mathbf{F}_k/\mathbb{F}_q)$.*

Proof. The corollary is a consequence of Proposition 5.5 applied with $l = 1$ and Lemma 3.1. ∎

On the other hand Theorem 3.3 implies the following result.

Proposition 5.7. *Let q be a prime power and $l \geq 1$ be a real number. Then for any algebraic function field $\mathbf{F}/\mathbb{F}_q$ of genus g and any strictly positive integer k such that*

$$2\log_q(l) - 2\log_q(C_q) \leq k$$

we have

$$A_{g-k} < h/l.$$

If we compare this proposition to Proposition 5.5, and thus to Tsfasman and Vladut's inequality, we see that the "asymptotical exact sequence" hypothesis is no longer necessary. Moreover, the range covered by the divisor order $g-k$ is now larger than the one covered by $g(1-\epsilon)$. In particular, we can now take a constant k or k growing slowly to infinity, for example $k = \log_q(g)$, which was not possible in Proposition 5.5.

Acknowledgments. The second author was partially supported by grant MTM2006-1139 from the Spanish MEC.

References

[1] E. Arbarello, M. Cornalba, P. Griffiths, and J. Harris, *Geometry of Algebraic Curves*, Vol. I, Springer, 1985.

[2] S. Ballet, *Curves with many points and multiplication complexity in any extension of* $\mathbb{F}_q$, Finite Fields Appl. 5 (1999), 364–377.

[3] —, *On the tensor rank of the multiplication in the finite fields*, J. Number Theory 128 (2008), 1795–1806.

[4] S. Ballet and D. Le Brigand, *On the existence of non-special divisors of degree g and $g-1$ in algebraic function fields over $\mathbb{F}_q$*, ibid. 116 (2006), 293–310.

[5] D. V. Chudnovsky and G. V. Chudnovsky, *Algebraic complexities and algebraic curves over finite fields*, J. Complexity 4 (1988), 285–316.

[6] G. Lachaud et M. Martin-Deschamps, *Nombre de points des jacobiennes sur un corps fini*, Acta Arith. 56 (1990), 329–340.

[7] J. Leitzel, M. Madan, and C. Queen, *Algebraic function fields with small class number*, J. Number Theory 7 (1975), 11–27.

[8] M. Madan and C. Queen, *Algebraic function fields of class number one*, Acta Arith. 20 (1972), 423–432.

[9] Y. Manin, *The Hasse–Witt matrix of an algebraic curve*, Izv. Akad. Nauk SSSR Ser. Mat. 25 (1961), 153–172 (in Russian).

[10] H. Niederreiter and C. Xing, *Low-discrepancy sequences and global function fields with many rational places*, Finite Fields Appl. 2 (1996), 241–273.

[11] R. Pellikaan, *On special divisors and the two variable zeta function on algebraic curves over finite fields*, in: R. Pellikaan et al. (eds.), Arithmetic, Geometry and Coding Theory (Luminy, 1993), de Gruyter, Berlin, 1996, 175–184.

[12] J.-P. Serre, *Sur la topologie des variétés algébriques en caractéristique p*, in: Symposium Internacional de Topología Algebrica, Univ. Nacional Autónoma de México, 1958, 24–53; see also: Oeuvres, Vol. I, Springer, 1986, 501–530.

[13] I. Shparlinski, M. Tsfasman, and S. Vladut, *Curves with many points and multiplication in finite fields*, in: H. Stichtenoth and M. A. Tsfasman (eds.), Coding Theory and Algebraic Geometry (Luminy, 1991), Lecture Notes in Math. 1518, Springer, Berlin, 1992, 145–169.

[14] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, 1993.

[15] K.-O. Stöhr and J. Voloch, *A formula for the Cartier operator on plane algebraic curves*, J. Reine Angew. Math. 377 (1987), 49–64.

[16] M. Tsfasman, *Some remarks on the asymptotic number of points*, in: H. Stichtenoth and M. A. Tsfasman (eds.), Coding Theory and Algebraic Geometry (Luminy, 1991), Lecture Notes in Math. 1518, Springer, Berlin, 1992, 178–192.

[17] M. Tsfasman and S. Vladut, *Asymptotic properties of zeta-functions*, J. Math. Sci. 84 (1997), 1445–1467.

S. Ballet, C. Ritzenthaler, R. Rolland
Institut de Mathématiques de Luminy
Case 930
F-13288 Marseille Cedex 9, France
E-mail: ballet@iml.univ-mrs.fr
ritzenth@iml.univ-mrs.fr
robert.rolland@acrypta.fr

Received on 16.6.2009
and in revised form on 4.11.2009 (6059)