C. R. Acad. Sci. Paris, Ser. I 349 (2011) 709–712

Contents lists available at ScienceDirect

C. R. Acad. Sci. Paris, Ser. I

www.sciencedirect.com

Théorie des nombres/Géométrie algébrique

Minorations du nombre de classes des corps de fonctions algébriques définis sur un corps fini

Lower bound for the class number of an algebraic function field over a finite field

Stéphane Ballet, Robert Rolland

Institut de mathématiques de Luminy, case 930, 13288 Marseille cedex 9, France

INFO ARTICLE

Historique de l'article :
Reçu le 21 juin 2010
Accepté après révision le 15 juin 2011
Disponible sur Internet le 13 juillet 2011

Présenté par Jean-Pierre Serre

RÉSUMÉ

On donne des minorations du nombre de diviseurs effectifs de degré $\leqslant g-1$ d'un corps de fonctions algébriques en une variable de genre $g \geqslant 2$ défini sur un corps fini $\mathbb{F}_q$. On en déduit alors des minorations du nombre de classes, dépendant essentiellement du nombre de places d'un certain degré r, qui améliorent les meilleures bornes inférieures connues dans de nombreux cas. De plus, nous montrons que toutes les familles de corps de fonctions algébriques en une variable ayant asymptotiquement (relativement au genre) un grand nombre de places d'un certain degré $r \geqslant 1$, possèdent un nombre de classe asymptotiquement grand dont nous donnons une estimation.

ABSTRACT

We give lower bounds for the number of effective divisors of degree $\leqslant g-1$ of an algebraic function field of one variable of genus $g \geqslant 2$ defined over a finite field. We deduce lower bounds for the class number, depending mainly on the number of places of a certain degree, which improve the best known lower bounds in many cases. Moreover, we prove that any family of algebraic function fields having asymptotically (with respect to the genus) a large number of places of a certain degree $r \geqslant 1$, have a large asymptotical class number for which we give an estimate.

1. Introduction

Soient A_n le nombre de diviseurs effectifs de degré n d'un corps de fonctions algébriques $F/\mathbb{F}_q$ défini sur $\mathbb{F}_q$ de genre $g \geqslant 2$ et $h = h(F/\mathbb{F}_q)$ le nombre de classes de $F/\mathbb{F}_q$. Soit $B_n(F/\mathbb{F}_q)$ le nombre de places de degré n de $F/\mathbb{F}_q$ que l'on notera B_n s'il n'y a aucune ambiguïté.

Posons

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

Adresses e-mail : stephane.ballet@univmed.fr (S. Ballet), robert.rolland@acrypta.fr (R. Rolland).

1631-073X/$ – see front matter
doi:10.1016/j.crma.2011.06.016

où $(\pi_i, \overline{\pi_i})_{1\leqslant i\leqslant g}$ est la suite des couples des racines inverses du numérateur de la fonction zêta $Z(F/\mathbb{F}_q, T)$ de $F/\mathbb{F}_q$. D'après un résultat de G. Lachaud et M. Martin-Deschamps [4], on a : $S(F/\mathbb{F}_q) = hR(F/\mathbb{F}_q)$.

En conséquence, pour trouver de bonnes minorations de h, il est suffisant de déterminer une bonne minoration de $S(F/\mathbb{F}_q)$ ainsi qu'une bonne majoration de $R(F/\mathbb{F}_q)$. D'après [4] on a l'inégalité :

$$R(F/\mathbb{F}_q) \leqslant \frac{1}{(q-1)^2}\big((g+1)(q+1) - B_1(F/\mathbb{F}_q)\big),$$

qui ne peut être améliorée dans le cas général.

Dans cette Note, nous nous proposons d'étudier des minorations de $S(F/\mathbb{F}_q)$. Pour ce faire, nous déterminons des minorations du nombre de diviseurs effectifs de degré $n \leqslant g-1$ obtenues à partir du nombre de diviseurs effectifs de degré $n \leqslant g-1$ contenant dans leur support un maximum de places d'un degré $r \geqslant 1$ fixé. Nous en déduisons des minorations du nombre de classes.

2. Minorations du nombre de diviseurs effectifs

Grâce à des minorations du nombre de diviseurs effectifs de degré $\leqslant g-1$, on obtient des minorations de $S(F/\mathbb{F}_q)$. Soit $B_r(F/\mathbb{F}_q)$ le nombre de places de degré r. On sait que si $B_i \geqslant 1$ et $b_i \geqslant 0$ le nombre de solutions de l'équation

$$n_1 + n_2 + \cdots + n_{B_i} = b_i$$

en nombres entiers $\geqslant 0$ est :

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

On en déduit des minorations du nombre de diviseurs effectifs de degré $n \leqslant g-1$ à partir du nombre de diviseurs effectifs contenant dans leur support un maximum de places d'un certain degré $r \geqslant 1$ qu'on complète par des places de degré 1 jusqu'à obtenir le degré n voulu.

Proposition 2.1. *Soient r et n deux entiers strictement positifs. Supposons que B_1 et B_r ne soient pas nuls. Alors :*

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

où $m_r(n)$ et $s_r(n)$ sont respectivement le quotient et le reste de la division euclidienne de n par r.

En minorant de cette façon chaque terme A_n, puis en regroupant les r indices n ayant le même $m_r(n)$ on obtient :

$$\sum_{n=0}^{g-1} A_n \geqslant \sum_{m=0}^{m_r(g-1)} \left(\sum_{i=0}^{r-1}\binom{B_1 + i - 1}{B_1 - 1}\right)\binom{B_r + m - 1}{B_r - 1},$$

ce qui donne le lemme suivant :

Lemme 2.2. *Supposons que $B_1 > 0$ et $B_r > 0$, alors on a la minoration suivante de la somme $\Sigma_1 = \sum_{n=0}^{g-1} A_n$:*

$$\Sigma_1 \geqslant K_1(r-1, B_1)\binom{B_r + m_r(g-1) - 1}{B_r} + K_1\big(s_r(g-1), B_1\big)\binom{B_r + m_r(g-1) - 1}{B_r - 1} \tag{2}$$

où

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

Étudions maintenant la deuxième somme : $\Sigma_2 = q^{g-1}\sum_{n=0}^{g-2}\frac{A_n}{q^n}$. On a alors :

$$\begin{aligned}\Sigma_2 \geqslant\ & q^{g-1}\left(\sum_{i=0}^{r-1}\frac{1}{q^i}\binom{B_1 + i - 1}{B_1 - 1}\right)\sum_{m=0}^{m_r(g-2)-1}\frac{1}{q^{mr}}\binom{B_r + m - 1}{B_r - 1} \\ &+ q^{s_r(g-2)+1}\binom{B_r + m_r(g-2) - 1}{B_r - 1}\sum_{i=0}^{s_r(g-2)}\frac{1}{q^i}\binom{B_1 + i - 1}{B_1 - 1}.\end{aligned} \tag{3}$$

Notons f_r le nombre suivant :

$$f_r = \begin{cases} 0 & \text{si } \frac{g-1}{2} < r \leqslant g-1; \\ 1 & \text{si } r \leqslant \frac{g-1}{2} \text{ and } B_r < q^r; \\ \min\bigl(\lfloor \frac{B_r - q^r}{q^r - 1} \rfloor + 1, m_r(g-2) - 1\bigr) & \text{if } r \leqslant \frac{g-1}{2} \text{ and } B_r \geqslant q^r. \end{cases}$$

Nous obtenons alors :

Lemme 2.3. *Soit q et r deux entiers > 0 et soit $g \geqslant 2$ un entier. Soit Q_r la somme définie par :*

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

où $m_r(n)$ est le quotient de la division Euclidienne de n par r. Alors

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

et

$$\Sigma_2 \geqslant K_2(q, r-1, B_1) q^{g-1} \left(\frac{q^{rm_r(g-2)} - 1}{q^{r(m_r(g-2)-1)}(q^r - 1)} + \frac{(B_r - 1)}{q^r} f_r \right) + q K_2\bigl(q, s_r(g-2), B_1\bigr) \binom{B_r + m_r(g-2) - 1}{B_r - 1},$$

où

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

et $s_r(n)$ est le reste de n par r.

Remarque 1. Notons que dans les deux lemmes précédents, les quantités $K_1(i, B)$ et $K_2(q, j, B)$ sont plus grandes que 1.

3. Minorations du nombre de classes

Dans cette section, on obtient des minorations du nombre de classes $h = h(F/\mathbb{F}_q)$ d'un corps de fonctions $F/\mathbb{F}_q$ en utilisant les minorations obtenues dans le paragraphe précédent. Soit $B_r = B_r(F/\mathbb{F}_q)$ le nombre de place de degré r.

Théorème 3.1. *Soit $F/\mathbb{F}_q$ un corps de fonctions algébriques défini sur $\mathbb{F}_q$ de genre $g \geqslant 2$ et h le nombre de classes de $F/\mathbb{F}_q$. Supposons que $B_1 > 0$ et $B_r > 0$. Alors, on a l'inégalité suivante :*

$$h \geqslant \frac{(q-1)^2}{(g+1)(q+1) - B_1} q^{g-1} \left(\frac{q^{rm_r(g-2)} - 1}{q^{r(m_r(g-2)-1)}(q^r - 1)} + \frac{(B_r - 1)}{q^r} f_r \right). \tag{4}$$

Remarque 2. Si on note

$$L_1 = q^{g-1} \frac{(q-1)^2}{(q+1)(g+1) - B_1}$$

qui correspond quand $B_1 = 0$ au premier minorant de h donné dans [4, Théorème 2] et L'_r la borne (4), alors :

$$L'_r > \left(\frac{q^{rm_r(g-2)} - 1}{q^{r(m_r(g-2)-1)}(q^r - 1)} + \frac{(B_r - 1)}{q^r} f_r \right) L_1.$$

Remarque 3. Des bornes sur h ont aussi été obtenues par Perret dans [5]. Ces bornes qui ne font intervenir que les points rationnels sont moins bonnes que L'_r dès lors que le nombre de points rationnels est petit alors qu'il existe beaucoup de points d'un degré supérieur.

4. Étude asymptotique quand g tend vers l'infini

Soit $\mathcal{F}/\mathbb{F}_q = (F_k/\mathbb{F}_q)_k$ une suite de corps de fonctions en une variable définis sur un corps fini $\mathbb{F}_q$. Soit $\mathcal{G}/\mathbb{F}_{q^r} = (G_k/\mathbb{F}_{q^r})_k$ la suite d'extensions du corps des constantes de degré r de $\mathcal{F}/\mathbb{F}_q$, à savoir pour tout k on a $G_k/\mathbb{F}_{q^r} = F_k \otimes_{\mathbb{F}_q} \mathbb{F}_{q^r}$. Notons g_k le genre de F_k et G_k, $h(F_k/\mathbb{F}_q)$ le nombre de classe de $F_k/\mathbb{F}_q$ et $B_i(F_k/\mathbb{F}_q)$ le nombre de places de degré i de $F_k/\mathbb{F}_q$. Supposons que pour tout k on a $B_1(F_k/\mathbb{F}_q) \geqslant 1$. Nous donnons des bornes asymptotiques du nombre de classes $h(F_k/\mathbb{F}_q)$ lorsque k tend vers l'infini et lorsqu'il existe un entier r tel que l'une des limites suivantes

$$\mu_r(\mathcal{F}/\mathbb{F}_q) = \liminf_{k\to+\infty} \frac{B_r(F_k/\mathbb{F}_{q_k})}{g(F_k)} \quad \text{ou} \quad \mu_1(\mathcal{G}/\mathbb{F}_{q^r}) = \liminf_{k\to\infty} \sum_{i|r} \frac{iB_i(F_k/\mathbb{F}_q)}{g_k}$$

existe et est strictement positive (par exemple lorsque la borne de Drinfeld–Vladut généralisée est atteinte [1]).

Théorème 4.1. *Soit $\alpha > 0$ un nombre réel. S'il existe un entier $r \geqslant 1$ tel que*

$$\mu_r(\mathcal{F}/\mathbb{F}_q) > \alpha \quad \textit{ou} \quad \frac{1}{r}\mu_1(\mathcal{G}/\mathbb{F}_{q^r}) > \alpha.$$

Alors

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

où $C > 0$ est une constante indépendante de k.

Remarque 4. A partir des tours de Garcia–Stichtenoth [2,3], on peut construire de nombreux exemples de tours de corps de fonctions algébriques vérifiant la condition (1) ainsi que des exemples vérifiant la condition (2) de ce théorème (cf. par exemple [1]).

Références

[1] Stéphane Ballet, Robert Rolland, Families of curves over any finite field attaining the generalized Drinfeld–Vladut bound, Publ. Math. Univ. Franche-Comté Besançon Algèbr. Theor. 5–18 (2011).
[2] Arnaldo Garcia, Henning Stichtenoth, On tame towers over finite felds of Artin–Schreier extensions of function fields attaining the Drinfeld–Vladut bound, Journal fur die Reine und Angewandte Mathematik 557 (2003) 53–80.
[3] Arnaldo Garcia, Henning Stichtenoth, Hans-Georg Rück, A tower of Artin–Schreier extensions of function fields attaining the Drinfeld–Vladut bound, Inventiones Mathematicae 121 (1995) 211–222.
[4] Gilles Lachaud, Mireille Martin-Deschamps, Nombre de points des jacobiennes sur un corps finis, Acta Arithmetica 56 (4) (1990) 329–340.
[5] Marc Perret, Number of points of Prym varieties over finite fields, Glasg. Math. J. 48 (2) (2006) 275–280.