Finite Fields and Their Applications **8,** 207–215 (2002)
doi:10.1006/ffta.2000.0336, available online at http://www.idealibrary.com on IDEAL®

A Note on Tamely Ramified Towers of Global Function Fields

Bruno Angles

Laboratoire de Mathématiques E. Picard, Université Toulouse III, 118 route de Narbonne, 31062 Toulouse Cédex 4, France
E-mail: angles@picard.ups-tlse.fr

and

Christian Maire

Laboratoire A2X, Universite Bordeaux I, 351 cours de la Libération, 33400 Talence, France
E-mail: maire@math.u-bordeaux.fr

Communicated by Harald Niederreiter

Received June 15, 1999; revised May 23, 2000; published online January 30, 2002

By using ramified Hilbert Class Field Towers we improve lower asymptotic bounds of the number of rational points of smooth algebraic curves over $\mathbb{F}_3$ and $\mathbb{F}_5$. © 2002 Elsevier Science (USA)

0. INTRODUCTION

For a function field F over $\mathbb{F}_q$, it is natural to compare the number $N(F)$ of places of degree one of F with its genus. To do this, Ihara introduced the quantity $A(q)$. Let's recall its definition. Let

$N_q(g) = \max\{N(F), F$ is a function field with constant field $\mathbb{F}_q$ of genus $g\}$, and define

$$A(q) = \limsup_{g \to \infty} \frac{N_q(g)}{g}.$$

By the well-known Hasse–Weil bound $N_q(g) \leq q + 1 + 2g\sqrt{q}$, one has immediately $A(q) \leq 2\sqrt{q}$. In 1981–1982, Ihara [5] showed by using modular curves that $A(q) \geq \sqrt{q} - 1$ if q is a square (in Tsfasman *et al.* [12] proved the same lower bound only if q is a second or fourth power of a prime number).

In 1983, Drinfeld and Vladut [2] improved the lower bound by showing that for all q,

$$A(q) \leq \sqrt{q} - 1,$$

and so $A(q) = \sqrt{q} - 1$ for q a square. For other values of q the problem of determining $A(q)$ is open. We may view the problem has having two directions: (1) What happens for large q? (2) What happens for small values of q, especially for $q = 2$, 3, 5? Much work has been done in the first direction: Serre [10] proved that there is an absolute constant c such that $A(q) > c \log q$. In this paper we are interested in $A(q)$ for $q = 3$ and $q = 5$.

A method for obtaining lower bounds for $A(q)$ is to construct towers of function fields with restricted ramification and to use the Riemann–Hurwitz formula. We should mention that by using explicit equations for such towers, Garcia and Stichtenocth [3] found again that the bound of Drinfeld–Vladut is optimal for q a square. Subsequently, Elkies has shown that the towers constructed by Garcia and Stichtenocth are modular.

Recently Niederreiter and Xing [6] provided lower bounds for $A(2)$, $A(3)$, and $A(5)$. They obtained $A(2) \geq 81/317$ (the previous best lower bound was $A(2) \geq 2/9$ due to Serre [10] and Schoof [9]); $A(3) \geq 62/163 \approx 0.38$; $A(5) \geq 2/3$. Their method was to construct unramified Hilbert Class field towers with decomposition.

Here by constructing class field towers with *ramification* and decomposition, we obtain with simple examples that $A(3) \geq 8/17 \approx 0.47$ and $A(5) \geq 8/11 \approx 0.72$. Note that the key Theorem (Theorem 6) is a special case of a conjecture of Perret [7, Conjecture 1'].

In the number fields setting, the analogous problem is to determine the minimal asymptotic rate of growth of discriminants. For over 20 years, the best known bound in this case has been that of Martinet. The idea of considering ramified class field towers has allowed Hajir and the second author to improve Martinet's bound [4].

We first recall some results from class field theory. In the second part, we give relation between tamely ramified extensions and $A(q)$, and then improve lower bounds for $A(3)$ and $A(5)$.

1. PRELIMINARIES

Let $\mathbb{F}_q(X)$ be a rational function field over $\mathbb{F}_q$; let F be a finite separable geometric extension of $\mathbb{F}_q(X)$ ($\mathbb{F}_q$ is the constant field of F). Let S and T be two finite sets of places of F (S is not empty) such that $S \cap T = \emptyset$. We then define:

- $\mathcal{O}(S) = \{x \in F, v(x) \geq 0, \forall v \notin S\}$ the ring of S-integers of F;
- $I(S)$ the group of fractional ideals of $\mathcal{O}(S)$;
- $I(S, T)$ the sub-group of $I(S)$ consisting of ideals prime to T;
- $m = \prod_{\mathcal{P} \in T} \mathcal{P}$;
- $P_m = \{(x) \in I(S, T), x \in F, x \equiv 1 (mod\, m)\}$;
- $E(S) = \{x \in \mathcal{O}_F(S), v(x) = 0, \forall v \notin S\}$ the group of S-units of F;
- $E(S, m) = \{x \in E(S), x \equiv 1 (mod\, m)\}$;
- and finally the following ray class group:

$$Cl(S, T) = \frac{I(S, T)}{P_m}.$$

If T is empty, $Cl(S) = Cl(S, \emptyset)$ is the class group of $\mathcal{O}(S)$.

Definition 1. Let ℓ be a prime. For a group A, we denote the dimension over $\mathbb{F}_\ell$ of $A/A^\ell[A, A]$ by $d_\ell A$.

Proposition 2. *By the approximation Theorem, $Cl(S)$ is quotient of $Cl(S, T)$, and then one has $d_\ell Cl(S, T) \geq d_\ell Cl(S)$.*

1.1. *Dirichlet's Unit Theorem.* Here we give the structure of $E(S, m)$ as $\mathbb{Z}$-module:

Proposition 3. *If T is not empty, then $E(S, m) \simeq \mathbb{Z}^{|S|-1}$.*

Proof. Thanks to Dirichlet's Unit Theorem, one gets $E(S) \simeq \mathbb{F}_q^\times . \mathbb{Z}^{|S|-1}$. Now, if T is not empty then the torsion of $E(S, m)$ is trivial and the proposition follows. ■

1.2. *Artin's Map.* We now recall how $Cl(S, T)$ classifies extensions of F in which S splits and ramified places are restricted to T. For a place $\mathcal{P}$ of F, we denote by $F_{\mathcal{P}}$ the completion of F at $\mathcal{P}$, $U_{\mathcal{P}}$ the unit group of $F_{\mathcal{P}}$ and $U_{\mathcal{P}}^1$ the group of principal units. Let

$$U_F(S, T) = \prod_{\mathcal{P} \in S} F_{\mathcal{P}}^\times \prod_{\mathcal{P} \notin T \cup S} U_{\mathcal{P}} \prod_{\mathcal{P} \in T} U_{\mathcal{P}}^1.$$

Definition 4. We define $F(S, T)$ to be the abelian extension of F associated to $U_F(S, T)$ by class field theory.

The following proposition is then immediate:

Proposition 5. (1) *$F(S, T)$ is the maximal abelian extension of F such that:*

- *all places of S are decomposed,*
- *all places outside T are unramified,*
- *the ramification for $\mathcal{P} \in T$ is tame.*

(2) *The Artin map induces the following isomorphism*:

$$Cl(S, T) \simeq Gal(F(S, T)/F).$$

1.3. *The T-Tamely Ramified and S-Decomposed Hilbert Tower.* Define by induction $(F_i)_i$ a sequence of Galois extensions of F: $F_0 = F$ and $F_{i+1} = F_i(S_i, T_i)$ where S_i (resp. T_i) is the set of places of F_i above S (resp. T). Put $F_\infty(S, T) = \bigcup_i F_i$.

Definition 6. $F_\infty(S, T)$ is called the T-S-Hilbert tower of F. For a prime ℓ, $F_\infty(S, T)(\ell)$ is the maximal ℓ-extension of F included in $F_\infty(S, T)$. It is the T-S-Hilbert ℓ-tower of F.

We now make two observations:

(1) if $\ell | q$, *then* $F(S, T)(\ell) = F(S, \emptyset)(\ell)$;

(2) if $(q, \ell) = 1$, then the ramification in ℓ-extension is always tame.

We work with the ℓ-tower as opposed to the bigger extension because we know a criterion for $F_\infty(S, T)(\ell)/F$ to be infinite, namely the Theorem of Golod–Shafarevich.

1.4. *Theorem of Golod–Shafarevich.* We now give the key theorem:

Theorem 7. *Let F be a geometric extension of $\mathbb{F}_q(X)$ and S and T two finite sets of places of F, $S \neq \emptyset$. Let ℓ be a prime with $(q, \ell) = 1$. Denote by $F_\infty(S, T)(\ell)$ the maximal ℓ-extension of F, S-decomposed and unramified outside T.*

If $F_\infty(S, T)(\ell)/F$ is finite then

$$d_\ell Cl(S, T) < 2 + 2\sqrt{d_\ell E(S, m) + 1}.$$

In particular if T is not empty, one gets (*thanks to Proposition* 2)

$$d_\ell Cl(S, T) < 2 + 2\sqrt{|S|}.$$

Remark. There are two benefits in the introduction of tame ramification:

(1) As $d_\ell Cl(S, T) \geq d_\ell Cl(S)$, the inequality in Theorem 6 may be true for $Cl(S)$ but false for $Cl(S, T)$; as a consequence we may not be able to determine what's happening for $F_\infty(S)/F$, in many cases where we can prove $F_\infty(S, T)/F$ to be infinite.

(2) If $\ell | (q - 1)$ then $d_\ell E(S, m) = d_\ell E(S) + 1$, and so the result of Theorem 6 is better for T not empty than for T empty. For this reason, we will try to find examples with $\ell | (q - 1)$.

Proof. Denote by $L = F_\infty(S, T)(\ell)$ and G the Galois group of L/F; G is a pro-ℓ group. As we have defined $U(S, T)$, $E(S, m)$, etc., for F, we define

$U_L(S_L, T_L)$, $E_L(S_L, m_L)$, etc., for L where the S_L (resp. T_L) are the places of L above S (resp. T). The following proposition is the crucial point of the proof of Theorem 7:

PROPOSITION 8. *For all $i \in \mathbb{Z}$, $\hat{H}^i(G, U_L(S_L, T_L)) = 1$.*

Thanks to Shapiro's lemma [1], one has

$$\hat{H}^i(G, U_L(S_L, T_L)) = \prod_{\mathscr{P} \in S} \hat{H}^i(G_{\mathscr{P}}, F_{\mathscr{P}}{}^{\times}) \prod_{\mathscr{P} \notin S \cup T} \hat{H}^i(G_{\mathscr{P}}, U_{\mathscr{P}}) \prod_{\mathscr{P} \in T} \hat{H}^i(G_{\mathscr{P}}, U^1_{\mathscr{P}}),$$

where $G_{\mathscr{P}}$ is the decomposition group of $\mathscr{P}$ in L/F. Now for $\mathscr{P} \in S$,

$$\hat{H}^i(G_{\mathscr{P}}, F_{\mathscr{P}}{}^{\times}) = 1$$

because $G_{\mathscr{P}}$ is trivial. For other $\mathscr{P}$ we have the following lemma:

LEMMA 9. *Let k be a complete field with respect to a discrete valuation. Let F be the residue field of k. Assume that F is finite; $char(F) = p > 0$. Let K/k be a finite Galois extension; $G = Gal(K/k)$. Denote by U the group of units of K and by U^1 the group of principal units of K. Then:*

(1) *If K/k is unramified, $\hat{H}^i(G, U) = 1$, $\forall i \in \mathbb{Z}$;*
(2) *If K/k is tamely ramified, $\hat{H}^i(G, U^1) = 1$, $\forall i \in \mathbb{Z}$.*

Proof. The first point is a well-known result [1, p. 131]. Using a criteria of trivial cohomology (see [1, p. 113]) to prove (2) it suffices to show that for all prime ℓ and for one ℓ-sylow G_ℓ of G, one has

$$\hat{H}^i(G_\ell, U^1) = 1, \qquad \forall i \geq 1. \tag{1}$$

First suppose $(p, \ell) = 1$. Then for $j \geq 1$,

$$\hat{H}^i(G_\ell, U^j/U^{j+1}) = 1,$$

because U^j/U^{j+1} is a finite p-group. Using the fact that $U^1 = \varprojlim_j U^j/U^{j+1}$ and that U^j is a decreasing sequence of G_ℓ-modules then a result of Serre (see [1, p. 132]) implies (1).

Now suppose $p = \ell$. Let $k_p = K^{G_p}$. As K/k_p is a tamely ramified p-extension then K/k_p is unramified and so $\hat{H}^i(G_p, U) = 1$ by first point. Moreover $\hat{H}^i(G_p, U/U^1)$ is trivial because U/U^1 is prime to p. So these remarks with the following exact sequence of G_p-modules

$$1 \to U^1 \to U \to U/U^1 \to 1,$$

show (1). ■

The proof of Theorem 6 is then classical. One has two exact sequences,

$$1 \to E_L(S_L, m_L) \to U_L(S_L, T_L) \to \frac{U_L(S_L, T_L)}{E_L(S_L, m_L)} \to 1, \tag{2}$$

$$1 \to \frac{U_L(S_L, T_L)}{E_L(S_L, m_L)} \to \frac{J_L}{L^\times} \to Cl(S_L, T_L) \to 1, \tag{3}$$

where J_L is the group of ideles of L. The second sequence comes from the Approximation Theorem. Next, remark that, since the tower ends at L, the order of $Cl_L(S_L, T_L)$ is not divisible by ℓ, and so $\hat{H}^i(G, Cl_L(S_L, T_L)) = 1$. Also by Proposition 8, $\hat{H}^{-1}(G, U_L(S_L, T_L)/E_L(S_L, m_L))$ is isomorphic to $\hat{H}^0(G, E(S_L, m_L))$ which is isomorphic to $\hat{H}^{-1}(G, J_L/L^\times)$, which is isomorphic to $H_2(G, \mathbb{Z})$ (cf. [1]). But the Theorem of Golod–Shafarevich [8] says that

$$\frac{1}{4} d_\ell G^2 - d_\ell G \leq d_\ell H_2(G, \mathbb{Z})$$

and this establishes the theorem. ■

1.5. *Genus Theory.* Using classical result about genus theory, we give a lower bound of the ℓ-rank of $Cl_F(S, T)$:

Theorem 10. *Let F/k be a cyclic Galois extension of degree ℓ of geometric function fields over $\mathbb{F}_q$; let S_k be a finite set of places of k (not empty) and let S be the set of places of F above S_k. Denote by ρ the number of places of k which are ramified in F/k. Then*

$$d_\ell Cl_F(S, T) \geq \rho - |S_k| - \delta,$$

where $\delta = 1$ if $\ell \mid (q-1)$ and 0 otherwise.

Proof. We use the remark of Theorem 7 and a result of Schoof [9] ■

The following corollary is a consequence of Theorems 7 and 10.

Corollary 11. *Let F/k be a cyclic Galois extension of degree ℓ of geometric function fields over $\mathbb{F}_q$; assume that $\ell \mid (q-1)$. Let S_k be a finite set of places of k (not empty) and S the set of places of F above S_k. Denote by ρ the number of places of k which are ramified in F/k. If $\rho \geq 3 + |S_k| + 2\sqrt{|S|}$, then for all non-empty sets T of places of F, $F_\infty(S, T)(\ell)/F$ is infinite.*

2. MAIN RESULT

We now show how an infinite tamely ramified extension gives a lower bound for $A(q)$.

2.1. *The Riemann–Hurwitz Formula*

PROPOSITION 12. *Let F be a function field with constant field $\mathbb{F}_q$. Let S be a set of places of F of degree one; assume that S is not empty. Let T be a finite set of places of F with $S \cap T = \emptyset$. Assume now that $F_\infty(S, T)/F$ is infinite. Then*

$$A(q) \geq \frac{|S|}{g - 1 + (1/2)\sum_{\mathscr{P} \in T} deg\, \mathscr{P}},$$

where g is the genus of F.

Proof. We use the notation of Section 1.3. Let g_i be the genus of F_i. Remark first that the constant field of F_i is $\mathbb{F}_q$ because F_i/F is S-decomposed. Denote by N_i the number of places of F_i of degree one. Then

$$N_i \geq |S|[F_i\colon F].$$

But one has, thanks to the Hasse–Weil Theorem,

$$N_i \leq q + 1 + 2g_i\sqrt{q},$$

so g_i tends to infinity because $F_\infty(S, T)/F$ is infinite. Let i be large enough so that $g_i \geq 2$. Using the Riemann–Hurwitz formula with the fact that the ramification is tame, one gets

$$2g_i - 2 = [F_i\colon F](2g - 2) + \sum_{\mathscr{P} \in T} (e_i(\mathscr{P}) - 1) f_i(\mathscr{P}) deg\, \mathscr{P},$$

where $e_i(\mathscr{P})$ (resp. $f_i(\mathscr{P})$) is the ramification index (resp. residue degree) of $\mathscr{P}$ in F_i/F. So

$$2g_i - 2 \geq \frac{|S_i|}{|S|}\left(2g - 2 + \sum_{\mathscr{P} \in T} deg\, \mathscr{P}\right),$$

and

$$\frac{g_i - 1}{|S_i|} \leq \frac{g - 1 + (1/2)\sum_{\mathscr{P} \in T} deg\, \mathscr{P}}{|S|}.$$

Remark that $g - 1 + \sum_{\mathscr{P} \in T} deg\,\mathscr{P} > 0$. So one gets

$$\frac{|S_i|}{g_i - 1} \geq \frac{|S|}{g - 1 + (1/2)\sum_{\mathscr{P} \in T} deg\,\mathscr{P}},$$

and finally

$$A(q) \geq \liminf_i \frac{N_i}{g_i} \geq \frac{|S|}{g - 1 + (1/2)\sum_{\mathscr{P} \in T} deg\,\mathscr{P}}. \qquad \blacksquare$$

2.2. *Quadratic Case.* Let $q \neq 2$, and $F = \mathbb{F}_q(X, Y)$ with Y satisfying $Y^2 = D(X)$, $D(X) \in \mathbb{F}_q[X]$ square free. We want to use Corollary 11 with $\ell = 2$, $k = \mathbb{F}_q(X)$, $(q, 2) = 1$, $|S_k| = 2$, $|S| = 4$, and $T = \{\mathscr{P}\}$. The places of S_k should be decomposed in F/k. Moreover we want that $\mathscr{P}$ is a place of degree one which is ramified in F/k. Let ρ be the number of places of k ramified in F. With these conditions using Proposition 12, we obtain:

Proposition 13. *With the above assumptions, if $\rho \geq 9$ then*

$$A(q) \geq \frac{4}{g - 1/2}.$$

Proposition 14. *We have*:

- $A(3) \geq \dfrac{8}{17}$;
- $A(5) \geq \dfrac{8}{11}$.

Proof. We apply Proposition 13, with $S_k = \{X; 1/X\}$.

For $q = 3$, we take $D(X) = (X - 1)(X - 2)(X^2 + 1)(X^2 + X + 2)(X^2 + 2X + 2)(X^3 + 2X + 1)(X^3 + 2X + 2)(X^3 + X^2 + 2)(X^3 + X^2 + X + 2)$, and $\mathscr{P}$ the place of F above $X - 1$. Then $g = 9$.

For $q = 5$, we take $D(X) = (X - 1)(X - 2)(X - 3)(X - 4)(X^2 + X + 1)(X^2 + 3)(X^2 + 2)(X^2 + X + 2)(X^2 + 2X + 3)$, and $\mathscr{P}$ the place of F above $X - 1$. Then $g = 6$. $\blacksquare$

ACKNOWLEDGMENTS

We thank F. Hajir and anonymous referees for this comments.

REFERENCES

1. J. W. S. Cassels and A. Fröhlich, “Algebraic Number Theory,” London, 1967.
2. V. G. Drinfeld and S. G. Vladut, Number of points of an algebraic curve, *Funct. Anal.* **17** (1983), 53–54.
3. A. Garcia and H. Stichtenoch, A tower of Artin–Schreier extensions of function fields attaining the Drinfeld–Vladut bound, *Invent. Math.* **121** (1995), 211–222.
4. F. Hajir and C. Maire, Tamely ramified towers and discriminant bounds for number fields, *Compositio Math.*, to appear.
5. Y. Ihara, Some remarks on the number of rational points of algebraic curves over finite fields, *J. Fac. Sci. Tokyo* **28** (1981), 721–724.
6. H. Niederreiter and C. Xing, Towers of global function fields with asymptotically many rational places and an improvement on the Gilbert–Varshamov bound, *Math. Nachr.* **195** (1998), 171–186.
7. M. Perret, Tours ramifiées infinies de corps de classes, *J. Number Theory* **38** (1991), 300–322.
8. P. Roquette, On class field towers, *in* “Algebraic Number Theory” (J. Cassels and A. Fröhlich, Eds.), Academic Press, San Diego, 1980.
9. R. Schoof, Algebraic curves over $\mathbb{F}_2$ with many rational points, *J. Number Theory* **41** (1992), 6–14.
10. J.-P. Serre, Rational points on curves over finite fields, lecture notes, Harvard University, 1985.
11. H. Stichtenoch, “Algebraic Function Fields and Codes,” Springer-Verlag, Berlin, 1993.
12. M. A. Tsfasman, S. G. Vladut, and T. Zink, Modular curves, Shimura curves and Goppa codes better than the Varshamov–Gilbert bound, *Math. Nachr.* **109** (1982), 21–28.