EVERYWHERE RAMIFIED TOWERS OF GLOBAL FUNCTION FIELDS

IWAN DUURSMA, BJORN POONEN, AND MICHAEL ZIEVE

ABSTRACT. We construct a tower of function fields $F_0 \subset F_1 \subset \dots$ over a finite field such that every place of every F_i ramifies in the tower and $\lim \operatorname{genus}(F_i)/[F_i : F_0] < \infty$. We also construct a tower in which every place ramifies and $\lim N_{F_i}/[F_i : F_0] > 0$, where N_{F_i} is the number of degree-1 places of F_i. These towers answer questions posed by Stichtenoth at Fq7.

1. Introduction

Let q be a prime power, and let $\mathbb{F}_q$ be a finite field of size q. By a *function field over* $\mathbb{F}_q$, we mean a finitely generated extension $K/\mathbb{F}_q$ of transcendence degree 1 in which $\mathbb{F}_q$ is algebraically closed. By an *extension of function fields* K'/K, we mean a finite separable extension such that K and K' are function fields over the same $\mathbb{F}_q$. Let g_K be the genus of K. Let N_K be the number of degree-1 places of K (the number of $\mathbb{F}_q$-rational points on the corresponding curve). A *tower* of function fields over $\mathbb{F}_q$ is a sequence of extensions of such function fields

$$K_0 \subset K_1 \subset K_2 \subset \dots$$

such that $g_i := g_{K_i} \to \infty$ as $i \to \infty$. Define $N_i = N_{K_i}$, and $d_i = [K_i : K_0]$. Since N_i/d_i is decreasing while $(g_i - 1)/d_i$ is increasing (Hurwitz), $\lim N_i/d_i$ and $\lim g_i/d_i$ exist. (The latter can be ∞.)

The Weil bound $N_K \leq q + 1 + 2g_K\sqrt{q}$ implies

$$\lim N_i/g_i \leq 2\sqrt{q}.$$

This was improved by Drinfeld and Vladut [4] (following Ihara [19]) to

$$\lim N_i/g_i \leq \sqrt{q} - 1.$$

Ihara also showed that, for any square q, there are towers of Shimura curves with $\lim N_i/g_i = \sqrt{q} - 1$ [15–19]. Subsequent authors have given further constructions of 'asymptotically good' towers, i.e., towers with $\lim N_i/g_i > 0$ [1–3, 5–14, 20–31, 33–36].

Every known asymptotically good tower has two special properties: there is some place of some K_i which splits completely in the tower, and there are only finitely many places of K_0 which ramify in the tower. (We say that a place of K_i *splits completely in the tower* if it splits completely in K_j/K_i for every $j \geq i$. We say that a place of K_0 *ramifies in the tower* if there exists i such that it ramifies in K_i/K_0.) But it is difficult to study asymptotically good towers directly since one must control both the genus and the number of rational places. With this as motivation, Stichtenoth posed the following two questions in his talk at Fq7 (the Seventh International Conference on Finite Fields and Their Applications):

Date: July 16, 2003.

2000 *Mathematics Subject Classification.* Primary 11G20; Secondary 14G05, 14G15.

The second author was supported in part by NSF grant DMS-0301280 and a Packard Fellowship.

Question 1.1. If $\lim N_i/d_i > 0$, must some K_i have a place that splits completely in the tower?

Question 1.2. If $\lim g_i/d_i < \infty$, must only finitely many places of K_0 ramify in the tower?

Our Theorems 1.3 and 1.4 imply negative answers to these two questions. Call a tower $K_0 \subset K_1 \subset \dots$ of function fields over $\mathbb{F}_q$ *everywhere ramified* if for each place P of each K_i, there exists $j > i$ such that P ramifies in K_j/K_i.

Theorem 1.3. *Given a function field K_0 over $\mathbb{F}_q$ with a rational place, there exists an everywhere ramified tower $K_0 \subset K_1 \subset \dots$ such that $\lim N_i/d_i > 0$.*

Theorem 1.4. *Given a function field K_0 over $\mathbb{F}_q$, there exists an everywhere ramified tower $K_0 \subset K_1 \subset \dots$ such that $\lim g_i/d_i < \infty$.*

2. Proof of Theorem 1.3

Lemma 2.1. *Let K be a function field over $\mathbb{F}_q$. Then there is a nontrivial extension K'/K in which all rational places of K split completely.*

Proof. Weak approximation (or Riemann-Roch) gives $f \in K^*$ having a zero at each rational place of K and a simple pole at some other place of K. Adjoin a root of $y^q - y = f$ to obtain K'. Then K'/K is totally ramified above the simple pole of f, so K' is another function field over $\mathbb{F}_q$ and $[K' : K] = q > 1$. □

Lemma 2.2. *Let K be a function field over $\mathbb{F}_q$ with $N_K > 0$, and let P be a place of K. For any $\varepsilon > 0$, there is an extension L/K such that $N_L/N_K > (1-\varepsilon)[L : K]$ and P ramifies in L/K.*

Proof. We first reduce to the case where $1/N_K < \varepsilon$. Repeated application of Lemma 2.1 yields K'/K such that $1/([K' : K]N_K) < \varepsilon$ and all rational places of K split completely. Then $N_{K'} = [K' : K]N_K$. Pick a place P' of K' above P. If we could find L/K' satisfying the conditions of the lemma for (K', P'), then

$$\frac{N_L}{N_K} = \frac{N_L}{N_{K'}}\frac{N_{K'}}{N_K} > (1-\varepsilon)[L : K'][K' : K] = (1-\varepsilon)[L : K],$$

so L/K would work for (K, P). Thus, renaming K' as K, we may assume $1/N_K < \varepsilon$.

Weak approximation gives $f \in K^*$ having a simple pole at P and zeros at all rational places not equal to P. Adjoin a root of $y^q - y = f$ to obtain L. Then P ramifies in L/K, but all other rational places of K split completely, so $N_L \geq (N_K - 1)q$. Thus $N_L/N_K \geq q(1 - 1/N_K) > [L : K](1-\varepsilon)$. □

Proof of Theorem 1.3. Fix a sequence of positive numbers $\varepsilon_m \to 0$ such that $\prod_{m=1}^{\infty}(1-\varepsilon_m)$ converges to a positive number. In our proof we will apply Lemma 2.2 infinitely often, using ε_1 in the first application, ε_2 in the second application, and so on.

Let $P_0, P_1, \dots$ be an enumeration of the places of K_0 (of all degrees). Given K_i, we construct K_{i+1} in stages so that all places of K_i lying above $P_0, \dots, P_i$ ramify in K_{i+1}/K_i. Namely, if $Q_1, \dots, Q_I$ are all the places of K_i lying above $P_0, \dots, P_i$, we set $K_{i,0} = K_i$ and then for $j = 1, \dots, I$ in turn, apply Lemma 2.2 with the first unused ε_m to find $K_{i,j}/K_{i,j-1}$ in which some place of $K_{i,j-1}$ above Q_j ramifies and $N_{K_{i,j}}/N_{K_{i,j-1}} > (1-\varepsilon_m)[K_{i,j} : K_{i,j-1}]$. Finally, set $K_{i+1} = K_{i,I}$.

If R is a place of some K_r, then R lies over some P_j of K_0. By construction, for all $i \geq \max\{j, r\}$, all places of K_i above R ramify in K_{i+1}/K_i. Thus R is ramified in K_{i+1}/K_r.

The inequality in Lemma 2.2 guarantees that the value of N/d for $K_{i,j}$ is at least $1-\varepsilon_m$ times the value of N/d for $K_{i,j-1}$. Thus N_i/d_i is at least $\left(\prod_{m\le M}(1-\varepsilon_m)\right) N_0/d_0$, if M is the number of applications of Lemma 2.2 used in the construction up to K_i. Since $N_0/d_0>0$ and $\prod_{m=1}^{\infty}(1-\varepsilon_m)$ converges, the decreasing sequence N_i/d_i is bounded below by

$$\left(\prod_{m=1}^{\infty}(1-\varepsilon_m)\right) N_0/d_0,$$

which is positive. So N_i/d_i has a positive limit. Finally, $N_i\to\infty$ implies $g_i\to\infty$. □

Remark 2.3. A slight modification of the argument shows that, given K_0, we can construct an everywhere ramified tower in which N_i/d_i converges to any prescribed value less than N_0. This is because weak approximation lets us prescribe the ramification and splitting of any finite number of places at each step.

3. Proof of Theorem 1.4

Let p be the characteristic of $\mathbb{F}_q$.

Lemma 3.1. *Let K be a function field over $\mathbb{F}_q$ of genus >1, and let P be a place of K. Then there exist unramified extensions K'/K of arbitrarily high genus such that for some place Q of K' lying over P, the residue field extension for Q/P is trivial.*

Proof. Let C be the smooth, projective, geometrically integral curve with function field K. Let J be the Jacobian of C. There exists a degree-1 divisor D on C [32, V.1.11]. Use D to identify C with a closed subvariety of J.

The place P corresponds to a Galois conjugacy class of points in $C(\mathbb{F}_{q^f})$, where $\mathbb{F}_{q^f}$ is the residue field. Choose P_0 in this conjugacy class. Choose $n\in\mathbb{Z}_{>0}$ such that $n\equiv 1 \pmod{p\cdot \#J(\mathbb{F}_{q^f})}$. Then the multiplication-by-n map $[n]\colon J\to J$ is étale, and maps P_0 to itself. Let $C'=[n]^{-1}C$, so C' is an étale cover of C. Then C' corresponds to a function field K' that is unramified over K. Also $P_0\in C'(\mathbb{F}_{q^f})$ represents a place Q of K' lying over P, having the same residue field as P. By choosing n large, we can make $g_{K'}$ as large as desired, by the Hurwitz formula. □

Lemma 3.2. *Let K be a function field over $\mathbb{F}_q$ of genus >1, let P be a place of K, and let $\varepsilon>0$. Then there exists an extension L/K with $(g_L-1)/(g_K-1)<(1+\varepsilon)[L:K]$ such that P ramifies in L/K.*

Proof. Let f be the degree of P over $\mathbb{F}_q$. For an unramified extension K'/K, we have $(g_{K'}-1)/(g_K-1)=[K':K]$ by Hurwitz. By applying Lemma 3.1, we may replace (K,P) by some (K',Q) in order to assume that g_K is arbitrarily large, without changing f.

When g_K is sufficiently large, an easy estimate (e.g. cf. [32, V.2.10]) based on the Weil bounds implies there exist places Q,Q' of K of degrees $d, d+f$ respectively, where d is the smallest integer $>\sqrt{g_K}$ and not equal to f. Choose a prime $\ell\nmid p\cdot\#G$, where G is the group of degree-zero divisor classes of K. Then every element of G, and in particular $[Q'-Q-P]$, is divisible by ℓ. Thus, there exists a divisor D of degree 0 and an element h of K such that $(h)=Q'-Q-P-\ell D$. Let $L=K(h^{1/\ell})$, so $[L:K]=\ell$. Hurwitz gives

$$2g_L-2=\ell(2g_K-2)+(\ell-1)((d+f)+d+f),$$

so

$$\frac{g_L - 1}{[L:K](g_K - 1)} \quad = \quad 1 + \frac{\ell - 1}{\ell}\left(\frac{d+f}{g_K - 1}\right) \quad = \quad 1 + O(g_K^{-1/2}).$$

The $O(g_K^{-1/2})$ term will be $< \varepsilon$ if g_K is sufficiently large. □

Proof of Theorem 1.4. Given K_0, let K_1/K_0 be an extension with $g_1 > 1$. Just as Lemma 2.2 let us prove Theorem 1.3, Lemma 3.2 now lets us construct an everywhere ramified tower $K_1 \subset K_2 \subset \dots$ such that at the i^{th} step the value of $(g_i - 1)/d_i$ increases by a factor at most $1 + \varepsilon_i$ for a prescribed $\varepsilon_i > 0$. By choosing ε_i so that $\prod(1 + \varepsilon_i)$ converges, we obtain such a tower with $\lim(g_i - 1)/d_i < \infty$. Since $d_i \to \infty$, this limit equals $\lim g_i/d_i$. □

4. Question

Can one combine Theorems 1.3 and 1.4? In particular, does there exist an everywhere ramified tower in which both $\lim N_i/d_i > 0$ and $\lim g_i/d_i < \infty$?

References

[1] B. Angles and C. Maire, *A note on tamely ramified towers of global function fields*, Finite Fields Appl. **8** (2002), 207–215.

[2] P. Beelen, *Graphs and recursively defined towers of function fields*, preprint.

[3] J. Bezerra and A. Garcia, *A tower with non-Galois steps which attains the Drinfeld-Vladut bound*, preprint.

[4] V.G. Drinfeld and S.G. Vladut, *The number of points of an algebraic curve*, Funktsional. Anal. i Prilozhen. **17** (1983), 68–69. [Funct. Anal. Appl. **17** (1983), 53–54.]

[5] N. D. Elkies, *Explicit modular towers*, in: Proceedings of the Thirty-Fifth [1997] Annual Allerton Conference on Communication, Control and Computing, (T. Başar and A. Vardy, eds.), Univ. of Illinois at Urbana-Champaign, 1998, 23–32.

[6] N. D. Elkies, *Explicit towers of Drinfeld modular curves*, in: European Congress of Mathematics (Barcelona, 2000), Vol. II (C. Casacuberta et al., eds.), Birkhauser, Basel, 2001, 189–198. arXiv:math.NT/0005140 (2000).

[7] G. Frey, E. Kani, and H. Völklein, *Curves with infinite K-rational geometric fundamental group*, in: Aspects of Galois Theory [Florida, 1996] (H. Völklein et al., eds.), Cambridge University Press, Cambridge, 1999, 85–118.

[8] G. Frey, M. Perret, and H. Stichtenoth, *On the different of abelian extensions of global fields*, in: Coding Theory and Algebraic Geometry, (H. Stichtenoth and M.A. Tsfasman, eds.), Springer-Verlag, New York, 1992, 26–32.

[9] A. Garcia and H. Stichtenoth, *A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound*, Invent. Math. **121** (1995), 211–222.

[10] A. Garcia and H. Stichtenoth, *On the asymptotic behavior of some towers of function fields over finite fields*, J. Number Theory **61** (1996), 248–273.

[11] A. Garcia and H. Stichtenoth, *On tame towers over finite fields*, J. Reine Angew. Math. **557** (2003), 53–80.

[12] A. Garcia, H. Stichtenoth, and M. Thomas, *On towers and composita of towers of function fields over finite fields*, Finite Fields Appl. **3** (1997), 257–274.

[13] G. van der Geer and M. van der Vlugt, *An asymptotically good tower of curves over the field with eight elements*, Bull. London Math. Soc. **34** (2002), 291–300.

[14] F. Hajir and C. Maire, *Asymptotically good towers of global fields*, in: European Congress of Mathematics (Barcelona, 2000), Vol. II (C. Casacuberta et al., eds.), Birkhauser, Basel, 2001, 207–218.

[15] Y. Ihara, *Algebraic curves mod $\mathfrak{p}$ and arithmetic groups*, in: Algebraic Groups and Discontinuous Subgroups (A. Borel and G. D. Mostow, eds.), American Mathematical Society, Providence, 1966, 265–271.

[16] Y. Ihara, On Congruence Monodromy Problems. Vol. 2, Department of Mathematics, University of Tokyo, 1969.

[17] Y. Ihara, *On modular curves over finite fields*, in: Discrete Subgroups of Lie Groups and Applications to Moduli (Internat. Colloq., Bombay, 1973), Oxford Univ. Press, Bombay, 1975, 161–202.

[18] Y. Ihara, *Congruence relations and Shimūra curves*, in: Automorphic Forms, Representations, and L-functions. Part 2 (A. Borel and W. Casselman, eds.), American Mathematical Society, Providence, 1979, 291–311.

[19] Y. Ihara, *Some remarks on the number of rational points of algebraic curves over finite fields*, J. Fac. Sci. Univ. Tokyo **28** (1981), 721–724.

[20] W.-C. W. Li and H. Maharaj, *Coverings of curves with asymptotically many rational points*, J. Number Theory **96** (2002), 232–256. arXiv:math.NT/9908152

[21] W.-C. W. Li, H. Maharaj and H. Stichtenoth, *New optimal towers over finite fields*, in: Algorithmic Number Theory [Sydney, 2002] (C. Fieker and D. Kohel, eds.), 372–389.

[22] Y.I. Manin and S.G. Vladut, *Linear codes and modular curves*, Itogi Nauki i Tekhniki **25** (1984), 209–257. [J. Soviet Math. **30** (1985), 2611–2643.]

[23] 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.

[24] H. Niederreiter and C. Xing, *Curve sequences with asymptotically many rational points*, in: Applications of Curves over Finite Fields [Seattle, 1997] (M. Fried, ed.), 3–14.

[25] H. Niederreiter and C. Xing, *Global function fields with many rational places and their applications*, in: Finite Fields: Theory, Applications, and Algorithms [Waterloo, 1997] (R. Mullin and G. Mullen, eds.), 87–111.

[26] H. Niederreiter and C. Xing, *Rational points on curves over finite fields: theory and applications*, Cambridge Univ. Press, Cambridge, 2001.

[27] M. Perret, *Tours ramifiées infinies de corps de classes*, J. Number Theory **38** (1991), 300–322.

[28] R. Schoof, *Algebraic curves over* $\mathbb{F}_2$ *with many rational points*, J. Number Theory **41** (1992), 6–14.

[29] J.-P. Serre, *Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini*, C. R. Acad. Sci. Paris **296** (1983), 397–402; = Œuvres [128].

[30] J.-P. Serre, *Rational points on curves over finite fields*, unpublished lecture notes by F. Q. Gouvêa, Harvard University, 1985.

[31] H. Stichtenoth, *Explicit constructions of towers of function fields with many rational places*, in: European Congress of Mathematics (Barcelona, 2000), Vol. II (C. Casacuberta et al., eds.), Birkhauser, Basel, 2001, 219–224.

[32] H. Stichtenoth, Algebraic Function Fields and Codes, Springer Verlag, Berlin, 1993.

[33] A. Temkine, *Hilbert class field towers of function fields over finite fields and lower bounds for* $A(q)$, J. Number Theory **87** (2001), 189–210.

[34] J. Wulftange, *Zahme Türme algebraischer Funktionenkörper*, Ph.D. thesis (Essen, 2003).

[35] C. Xing, *The number of rational points of algebraic curves over finite fields*, Acta Math. Sinica **37** (1994), 584–589.

[36] Th. Zink, *Degeneration of Shimura surfaces and a problem in coding theory*, in: Fundamentals of Computation Theory [Cottbus] (L. Budach, ed.), Springer-Verlag, New York, 1985, 503–511.

Department of Mathematics, University of Illinois, Urbana, IL 61801–2975, USA
E-mail address: `duursma@math.uiuc.edu`
URL: `http://www.math.uiuc.edu/~duursma`

Department of Mathematics, University of California, Berkeley, CA 94720–3840, USA
E-mail address: `poonen@math.berkeley.edu`
URL: `http://math.berkeley.edu/~poonen`

Center for Communications Research, 805 Bunn Drive, Princeton, NJ, 08540, USA
E-mail address: `zieve@idaccr.org`