



Good recursive towers over prime fields exist

Alp Bassa, Christophe Ritzenthaler

► To cite this version:

Alp Bassa, Christophe Ritzenthaler. Good recursive towers over prime fields exist. *Mathematische Annalen*, 2020, 378 (1-2), pp.599-604. 10.1007/s00208-020-02039-9 . hal-01856435

HAL Id: hal-01856435

<https://hal.science/hal-01856435>

Submitted on 9 Jan 2024

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.

GOOD RECURSIVE TOWERS OVER PRIME FIELDS EXIST

ALP BASSA AND CHRISTOPHE RITZENTHALER

ABSTRACT. We give a construction and equations for good recursive towers over any finite field \mathbf{F}_q with $q \neq 2$ and 3 .

1. INTRODUCTION

Let \mathbf{F}_q be a finite field with $q = p^n$ elements, where p is a prime and $n \geq 1$ an integer. A central quantity in the theory of curves over finite fields of large genus is the Ihara constant $A(q)$, which is defined as

$$A(q) := \limsup_{g \rightarrow \infty} \frac{N_q(g)}{g},$$

where $N_q(g) = \max \#X(\mathbf{F}_q)$ with X running over all smooth projective absolutely irreducible curves defined over \mathbf{F}_q of genus $g(X) = g > 0$. Drinfel'd–Vlăduț [VD83] obtained the inequality

$$A(q) \leq \sqrt{q} - 1, \quad (1.1)$$

which is still the only known upper bound.

When the exponent n is even, Ihara [Iha81] used reductions of Shimura curves to show that equality holds in (1.1). This result was also obtained by Tsfasman–Vlăduț–Zink [TVZ82] for $n = 2$ and 4 using reductions of elliptic modular curves. For any q , using class field theory, Serre [Ser83] showed that $A(q) > c \log(q)$ for some constant $c > 0$ independent of q (one can take for instance $c = \frac{1}{96}$ [NX01, Theorem 5.2.9]). In particular $A(q) > 0$ for all q . The exact value of $A(q)$ is however unknown when q is not a square.

Garcia and Stichtenoth [GS95] marked a major turning-point in the theory by introducing the notion of recursive towers $\mathcal{T} = (X_m)_{m \in \mathbf{N}}$. These towers are described by two morphisms $f, g : C_0 \rightrightarrows C_{-1}$ where C_0 and C_{-1} are curves defined over \mathbf{F}_q . This defines recursively $(C_m)_{m \geq 0}$ by the fiber product

$$\begin{array}{ccc} C_{m+1} & \xrightarrow{\quad} & C_0 \\ \pi_m \downarrow & & \downarrow g \\ C_m & \xrightarrow{f_m} & C_{-1} \end{array}$$

where $f_m(P_0, \dots, P_m) = f(P_m)$ and $\pi_m(P_0, \dots, P_{m+1}) = (P_0, \dots, P_m)$. In other terms one has

$$C_m = \{(P_0, \dots, P_m) \in C_0^{m+1} : g(P_i) = f(P_{i-1}), 1 \leq i \leq m\}.$$

One then considers the normalization X_m of C_m and we will still denote by $\pi_m : X_{m+1} \rightarrow X_m$ the induced cover. Although the curves X_m are smooth, it is not automatic that they are absolutely irreducible or that their genus goes to infinity. If it is so, $\mathcal{T} = (X_m)_{m \in \mathbf{N}}$ with the morphisms π_m is called a *tower*. It is a *good tower* if the *limit of the tower*

$$\lambda(\mathcal{T}) := \limsup \frac{\#X_m(\mathbf{F}_q)}{g(X_m)}$$

is positive and an *optimal tower* if it reaches the Drinfel'd–Vlăduț bound.

Date: July 17, 2018.

2010 Mathematics Subject Classification. 11G20, 11T71, 14H25, 14G05, 14G15.

Key words and phrases. recursive tower ; explicit ; prime field ; correspondences ; Singer subgroup.

The authors acknowledge support by the PHC Bosphorus 39652NB - TŮBĚTAK 117F274 and thank the Nesin Mathematical Village for its inspiring environment.

For n even, Garcia and Stichtenoth exhibited explicit examples of optimal towers. Compared to constructions using class field towers or modular curves, recursive towers have the advantage of being more elementary and explicit, which is crucial for potential applications in coding theory and cryptography. This approach resulted subsequently in the discovery of many good recursive towers when $n = 2$ (see [GS96, GSR03], among others), $n = 3$ (see [vdGvdV02, BGS05], among others) and $n > 1$ (see [BBGS15]). The last one gives, under a unified construction, the best known lower bounds. The morphisms f and g resulting in good towers seem to be very special and in fact almost all have been proven to have a modular interpretation of various types (see [Elk98, Elk01, ABB17] among others).

Still, when $n = 1$, among the several approaches mentioned above, only class field theory has produced positive lower bounds for the Ihara constant $A(q)$. Despite several decades of attempts, no good modular towers or recursive towers were obtained and their existence has even been questioned.

The present article breaks this barrier by exhibiting a good recursive tower $\mathcal{T} = (X_m)_{m \in \mathbf{N}}$ over any field \mathbf{F}_q with $q > 3$ such that $\lambda(\mathcal{T}) \geq \frac{2}{q-2}$. The structure of the tower is surprisingly simple. Starting from a good choice of cover $f : C_0 \rightarrow C_{-1}$, one constructs the morphism g by choosing carefully an automorphism ψ (resp. φ) of C_0 (resp. C_{-1}) and defines $g = \varphi \circ f \circ \psi$. More precisely, let us denote by \mathcal{R} a subset of $C_0(\overline{\mathbf{F}}_q)$ containing the ramification points of f and $\mathcal{S} \subset C_0(\mathbf{F}_q)$ the inverse image under f of a set of totally split points of f . Let us assume that there exist an automorphism ψ of C_0 (resp. φ of C_{-1}) preserving \mathcal{R} and \mathcal{S} (resp. $f(\mathcal{R})$ and $f(\mathcal{S})$). If we can ensure that f, g define a tower $\mathcal{T} = (X_m)_{m \in \mathbf{N}}$, then \mathcal{R} (resp. \mathcal{S}) contains the ramification locus (resp. splitting locus) of the tower as defined in [Sti09]. The general formula of [Sti09, Corollary 7.2.11.] then gives that $\lambda(\mathcal{T}) \geq \frac{2\#\mathcal{S}}{\#\mathcal{R}-2}$.

We choose a particular cyclic Galois cover $f : \mathbf{P}^1 \rightarrow \mathbf{P}^1$ of degree $q+1$. The ramification points Q, \overline{Q} of f are defined over \mathbf{F}_{q^2} whereas the point at infinity is totally split, i.e. $f^{-1}(\infty) = \mathbf{P}^1(\mathbf{F}_q)$. We let $\mathcal{R} = \mathbf{P}^1(\mathbf{F}_{q^2}) \setminus \mathbf{P}^1(\mathbf{F}_q)$ and $\mathcal{S} = \mathbf{P}^1(\mathbf{F}_q)$ and prove that there exist automorphisms ψ and φ preserving these sets and their image by f . Moreover, when $q > 3$, we can impose that $g(Q) = Q$ and Q, \overline{Q} are not ramification points of g . This implies that the curves X_m are absolutely irreducible and of growing genus hence \mathcal{T} is a good tower.

Our construction does not work over \mathbf{F}_2 and \mathbf{F}_3 and does not improve any of the known lower bounds on $A(q)$. It does, however, provide an elementary proof for $A(q) > 0$ in case $q > 3$. The simple framework we suggest makes it tempting to improve the limit by changing the cover $f : C_0 \rightarrow C_{-1}$. Using the map μ in the proof of Lemma 2.1, it is also possible to recover the tower as a twist of a good tower over a quadratic field extension. It might be possible to generalize this principle to other good towers. A further interesting question is to give (if possible) a modular interpretation for this tower. Our construction gives a first example of recursive towers over prime fields and we hope that it will stimulate the quest for better ones.

2. MAIN RESULT

Let $q = p^n$ be a prime power and for $x \in \mathbf{F}_{q^2}$ denote \overline{x} its Galois conjugate over \mathbf{F}_q . Let $Q = (\theta : 1) \in \mathbf{P}^1(\mathbf{F}_{q^2}) \setminus \mathbf{P}^1(\mathbf{F}_q)$. The automorphism group of \mathbf{P}^1 over \mathbf{F}_q is $\mathrm{PGL}_2(\mathbf{F}_q)$ and the isotropy group G of Q is a cyclic subgroup of $\mathrm{PGL}_2(\mathbf{F}_q)$ of order $q+1$. The conjugate point $\overline{Q} = (\overline{\theta} : 1)$ has the same isotropy group G and all cyclic subgroups of $\mathrm{PGL}_2(\mathbf{F}_q)$ of order $q+1$ appear as isotropy subgroups of such Q . Because of the transitive action of $\mathrm{PGL}_2(\mathbf{F}_q)$ on $\mathbf{P}^1(\mathbf{F}_{q^2}) \setminus \mathbf{P}^1(\mathbf{F}_q)$, they are all conjugated (see for instance [VM80, Th.2]). Seen as a subgroup of $\mathrm{GL}_2(\mathbf{F}_q)$, these subgroups are called *Singer subgroups* and have been well studied.

The group G defines a tame Galois cover $f : \mathbf{P}^1 \rightarrow \mathbf{P}^1$ of degree $q+1$, where Q and \overline{Q} are totally ramified and, by Riemann-Hurwitz formula, the only ramified points. As a consequence, since the order of G is $q+1$, it acts transitively on $\mathbf{P}^1(\mathbf{F}_q)$. We choose coordinates $(x : z)$ on \mathbf{P}^1 such that $f(Q) = Q$, $f(\overline{Q}) = \overline{Q}$ and $f(\infty) = \infty$ where $\infty = (0 : 1)$. We then have that $f^{-1}(\infty) = \mathbf{P}^1(\mathbf{F}_p)$. Therefore ∞ is totally split whereas Q and \overline{Q} are the two branched points. As mentioned in the introduction, we denote $\mathcal{R} = \mathbf{P}^1(\mathbf{F}_{q^2}) \setminus \mathbf{P}^1(\mathbf{F}_q)$ and $\mathcal{S} = \mathbf{P}^1(\mathbf{F}_q)$.

Lemma 2.1. *We have $f(\mathcal{R}) = \{(\gamma : 1) : \gamma \in \mathbf{F}_{q^2} \text{ with } \text{Tr}_{\mathbf{F}_{q^2}/\mathbf{F}_q}(\gamma) = \text{Tr}_{\mathbf{F}_{q^2}/\mathbf{F}_q}(\theta)\}$.*

Proof. Let $\mu : x \mapsto (x - \theta)/(x - \bar{\theta})$ and consider $\tilde{f} = \mu \circ f \circ \mu^{-1} : \mathbf{P}^1 \rightarrow \mathbf{P}^1$. It defines a Galois cover of degree $q + 1$ with fixed points $(0 : 1)$ and ∞ . Hence \tilde{f} corresponds to the rational map $x \mapsto cN(x)$, with $N(x) = x^{q+1}$ for some constant $c \in \mathbf{F}_{q^2}$. Actually $c = 1$, since

$$\tilde{f}((\theta/\bar{\theta} : 1)) = (c : 1) = \mu \circ f((0 : 1)) = \mu(\infty) = (1 : 1).$$

If $u \in \mathbf{F}_q$ then $(u - \theta)/(u - \bar{\theta}) = (u - \theta)/\overline{(u - \theta)}$ hence $N \circ \mu(P) = (1 : 1)$ for all $P \in \mathbf{P}^1(\mathbf{F}_q)$. The surjectivity of the norm map from \mathbf{F}_{q^2} to \mathbf{F}_q implies that

$$N(\mu(\mathcal{R})) = \mathbf{P}^1(\mathbf{F}_q) \setminus \{(1 : 1)\}.$$

It is immediate to verify that

$$f(\mathcal{R}) = \mu^{-1}(\mathbf{P}^1(\mathbf{F}_q) \setminus \{(1 : 1)\}) = \{(\gamma : 1) : \gamma \in \mathbf{F}_{q^2} \text{ with } \text{Tr}_{\mathbf{F}_{q^2}/\mathbf{F}_q}(\gamma) = \text{Tr}_{\mathbf{F}_{q^2}/\mathbf{F}_q}(\theta)\}. \quad \square$$

Looking for automorphisms φ, ψ of \mathbf{P}^1 such that ψ preserves \mathcal{R}, \mathcal{S} and φ their image under f , we see that it is necessary and sufficient for ψ to be defined over \mathbf{F}_q to preserve \mathcal{R} and \mathcal{S} and hence φ is also defined over \mathbf{F}_q in order for g to be defined over \mathbf{F}_q . Moreover, since $f(\mathcal{S}) = \infty$, we need φ to be of the form $(x : z) \mapsto (cx + dz : z)$.

Proposition 2.2. *An automorphism $\varphi : \mathbf{P}^1 \rightarrow \mathbf{P}^1$ of the form $(x : z) \mapsto (cx + dz : z)$ and defined over \mathbf{F}_q preserves $f(\mathcal{R})$ if and only if $(1 - c)a = 2d$ with $c \neq 0$ and $a = \text{Tr}_{\mathbf{F}_{q^2}/\mathbf{F}_q}(\theta)$.*

Proof. An automorphism $(x : z) \mapsto (cx + dz : z)$ preserves

$$f(\mathcal{R}) = \{(\gamma : 1) : \gamma \in \mathbf{F}_{q^2} \text{ with } \text{Tr}_{\mathbf{F}_{q^2}/\mathbf{F}_q}(\gamma) = a\}$$

if and only if $\text{Tr}_{\mathbf{F}_{q^2}/\mathbf{F}_q}(c\gamma + d) = a$ i.e. $(1 - c)a = 2d$. \square

Theorem 2.3. *Assume that $q > 3$. There exists an explicit recursive tower $\mathcal{T} = (X_m)_{m \in \mathbf{N}}$ over \mathbf{F}_q with limit*

$$\lambda(\mathcal{T}) \geq \frac{2}{q-2}.$$

Proof. Let $g = \varphi \circ f \circ \psi$ for a choice of an automorphism ψ (resp. φ) defined over \mathbf{F}_q and preserving \mathcal{R} and \mathcal{S} (resp. $f(\mathcal{R})$ and $f(\mathcal{S})$). Consider the correspondence $f, g : \mathbf{P}^1 \rightrightarrows \mathbf{P}^1$ and the curves $(X_m)_{m \in \mathbf{N}}$ they define. For $\mathcal{T} = (X_m)_{m \in \mathbf{N}}$ to be a tower, it is enough to show that all the separable morphisms $\pi_{m+1} : X_{m+1} \rightarrow X_m$ are ramified. To ensure this, it is enough that $g(Q) = Q$ and that Q is not a ramification point for g , i.e. $\varphi(Q) \notin \{Q, \bar{Q}\}$. For $q > 3$, there always exists $c, d \in \mathbf{F}_q$ with $c \neq 0$ and $(1 - c)a = 2d$ (as in Proposition 2.2) such that $\varphi(x) = cx + d$ does not map Q on itself ($c = 1, d = 0$) or on \bar{Q} ($c = -1, d = a$). Let us pick such (c, d) and corresponding φ . Let us now consider $S = \varphi^{-1}(Q)$. Since φ stabilizes $f(\mathcal{R})$ and $Q \in f(\mathcal{R})$, we see that the points of $f^{-1}(S) = \{T_1, \bar{T}_1, \dots, T_{(q+1)/2}, \bar{T}_{(q+1)/2}\}$ are in \mathcal{R} . One then picks an automorphism ψ defined over \mathbf{F}_q such that $\psi(Q) = T_i$ for $1 \leq i \leq \frac{q+1}{2}$. For such a choice, one has $g(Q) = Q$. The general formula of [Sti09, Corollary 7.2.11.] then gives that

$$\lambda(\mathcal{T}) \geq \frac{2\#\mathcal{S}}{\#\mathcal{R} - 2} = \frac{2}{q-2}. \quad \square$$

Lastly, we derive in odd characteristic explicit equations for the maps f and g above. Let $\chi(X) = X^2 - aX + b$ be the minimal polynomial of θ . Requiring that $f(Q) = Q, f(\bar{Q}) = \bar{Q}$ and $f(\infty) = \infty$ with Q and \bar{Q} totally ramified and ∞ totally split implies that

$$f(x) = \frac{x^{q+1} - ax + b}{x^q - x}.$$

Let us now consider one of the ψ from above and denote $R = (\rho : 1) = \psi^{-1}(Q) \notin \{Q, \bar{Q}\}$ and $(\nu : 1) = g(R) = \varphi(Q)$. Let $X^2 - tX + n$ be the minimal polynomial of ρ . The fact that g is defined over \mathbf{F}_q , R is totally ramified for g and $g^{-1}(\infty) = \mathbf{P}^1(\mathbf{F}_q)$ means that

$$g(x) = \frac{x^{q+1} + c_q x^q + c_1 x + c_0}{c(x^q - x)}$$

where

$$c_0 = n, \quad c_q - c\nu = -\rho, \quad c_1 + c\nu = -\bar{\rho}$$

from which we derive $c_q + c_1 = -t$ and $c_q - c_1 = c \operatorname{Tr}_{\mathbf{F}_{q^2}/\mathbf{F}_q}(\nu)$. Imposing that $g(Q) = Q$ we get that

$$c = \frac{2b + 2n + ta}{4b - a^2} \neq 0, \quad c_q - c_1 = ca.$$

Since $\operatorname{Tr}_{\mathbf{F}_{q^2}/\mathbf{F}_q}(\nu) = (c_q - c_1)/c = a = \operatorname{Tr}_{\mathbf{F}_{q^2}/\mathbf{F}_q}(\theta)$, the map φ satisfies the condition of Proposition 2.2 and we can choose $\rho \in \mathbf{F}_{q^2} \setminus \mathbf{F}_q$ arbitrarily as long as $\rho \neq \theta, \bar{\theta}$ and $2b + 2t + ta \neq 0$. Taking conveniently $a = 0$ and $t = 0$ and $-n, -b \in \mathbf{F}_q^\times$ two non-squares with $n \neq \pm b$ (hence $q > 5$), we get for instance

$$f(x) = \frac{x^{q+1} + b}{x^q - x} \quad \text{and} \quad g(x) = \frac{2b(x^{q+1} + n)}{(b + n)(x^q - x)}.$$

For $q = 5$ one can check that with θ a root of $\chi(X) = X^2 + X + 2$, the automorphisms $\varphi(x) = 2x + 3$ and $\psi(x) = 1/x$ satisfy the requirements of the theorem. Hence we obtain as possible maps $f(x) = (x^6 + x + 2)/(x^5 - x)$ and $g(x) = (x^6 + x^5 + 2x + 3)/(x^5 - x)$.

REFERENCES

- [ABB17] Nurdagül Anbar, Alp Bassa, and Peter Beelen. A modular interpretation of various cubic towers. *J. Number Theory*, 171:341–357, 2017.
- [BBGS15] Alp Bassa, Peter Beelen, Arnaldo Garcia, and Henning Stichtenoth. Towers of function fields over non-prime finite fields. *Mosc. Math. J.*, 15(1):1–29, 181, 2015.
- [BGS05] Juscelino Bezerra, Arnaldo Garcia, and Henning Stichtenoth. An explicit tower of function fields over cubic finite fields and Zink’s lower bound. *J. Reine Angew. Math.*, 589:159–199, 2005.
- [Elk98] Noam D. Elkies. Explicit modular towers. In *Proceedings of the 35th annual Allerton conference on communication, control and computing, (Urbana, 1997)*, pages 23–32. 1998.
- [Elk01] Noam D. Elkies. Explicit towers of Drinfeld modular curves. In *European Congress of Mathematics, Vol. II (Barcelona, 2000)*, volume 202 of *Progr. Math.*, pages 189–198. Birkhäuser, Basel, 2001.
- [GS95] Arnaldo Garcia and Henning Stichtenoth. A tower of Artin-Schreier extensions of function fields attaining the Drinfel’d-Vlăduț bound. *Invent. Math.*, 121(1):211–222, 1995.
- [GS96] Arnaldo Garcia and Henning Stichtenoth. On the asymptotic behaviour of some towers of function fields over finite fields. *J. Number Theory*, 61(2):248–273, 1996.
- [GSR03] Arnaldo Garcia, Henning Stichtenoth, and Hans-Georg Rück. On tame towers over finite fields. *J. Reine Angew. Math.*, 557:53–80, 2003.
- [Iha81] Yasutaka Ihara. Some remarks on the number of rational points of algebraic curves over finite fields. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 28(3):721–724 (1982), 1981.
- [NX01] Harald Niederreiter and Chaoping Xing. *Rational points on curves over finite fields: theory and applications*, volume 285 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2001.
- [Ser83] Jean-Pierre Serre. Sur le nombre des points rationnels d’une courbe algébrique sur un corps fini. *C. R. Acad. Sci. Paris Sér. I Math.*, 296(9):397–402, 1983.
- [Sti09] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.
- [TVZ82] M. A. Tsfasman, S. G. Vladut, and Th. Zink. Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound. *Math. Nachr.*, 109:21–28, 1982.
- [VD83] S. G. Vlăduț and V. G. Drinfel’d. The number of points of an algebraic curve. *Funktsional. Anal. i Prilozhen.*, 17(1):68–69, 1983.
- [vdGvdV02] Gerard van der Geer and Marcel van der Vlugt. An asymptotically good tower of curves over the field with eight elements. *Bull. London Math. Soc.*, 34(3):291–300, 2002.
- [VM80] Robert C. Valentini and Manohar L. Madan. A Hauptsatz of L. E. Dickson and Artin-Schreier extensions. *J. Reine Angew. Math.*, 318:156–177, 1980.

BOĞAZIÇI UNIVERSITY, DEPARMENT OF MATHEMATICS, 34342 BEBEK, ISTANBUL, TURKEY
E-mail address: alp.bassa@boun.edu.tr

INSTITUT DE RECHERCHE MATHÉMATIQUE DE RENNES, UNIVERSITÉ DE RENNES 1, CAMPUS DE BEAULIEU, 35042 RENNES, FRANCE.
E-mail address: christophe.ritzenthaler@univ-rennes1.fr