ON THE GALOIS CLOSURE OF TOWERS

ARNALDO GARCIA AND HENNING STICHTENOTH

Abstract. We show that the Galois closures over F_0 of certain towers $\mathcal{F} = (F_0, F_1, F_2, \dots)$ also have good limits. We apply our method to the towers $\mathcal{F}$ considered in [4], [5], [7] and [8] (see Remark 2.4 and Theorems 2.5 and 2.7).

0. Introduction

Much interest on precise information about the number of rational places of function fields over finite fields comes from applications to Coding Theory. For an $\mathbb{F}_q$-function field F (we assume that the finite field $\mathbb{F}_q$ is algebraically closed in the field F), we have the so-called *Hasse-Weil bound* (see [13] and [10])

$$N(F) \le q + 1 + 2\sqrt{q} \cdot g(F),$$

where $N(F)$ is the number of $\mathbb{F}_q$-rational places of the field F and $g(F)$ is its genus.

Ihara (see [9]) was the first to notice that the Hasse-Weil bound can be significantly improved if one fixes the finite field $\mathbb{F}_q$ and lets $g(F) \to \infty$. In this context it is natural to consider the following concept:

A *tower* $\mathcal{F}$ over a finite field $\mathbb{F}_q$ (or an $\mathbb{F}_q$-*tower*) is an infinite sequence

$$\mathcal{F} = (F_0, F_1, F_2, \dots)$$

such that:

a) Each F_n is an $\mathbb{F}_q$-function field and $\mathbb{F}_q$ is algebraically closed in F_n.
b) For all n, we have inclusions $F_n \subseteq F_{n+1}$ and the field extensions F_{n+1}/F_n are separable.
c) We have $g(F_n) \to \infty$ as $n \to \infty$.

The following limit exists (see [5]) and it is called the *limit of the tower*:

$$\lambda(\mathcal{F}) = \lim_{n\to\infty} N(F_n)/g(F_n).$$

The tower $\mathcal{F}$ is said to be *asymptotically good* when it has a positive limit; i.e., when $\lambda(\mathcal{F}) > 0$. An interesting special class of towers is the so-called *recursive tower* $\mathcal{F} = (F_0, F_1, F_2, \dots)$. This means that there exist a polynomial $f(X,Y) \in \mathbb{F}_q[X,Y]$ and functions $x_n \in F_n$ for all n, such that

$$F_0 = \mathbb{F}_q(x_0) \quad \text{and} \quad F_{n+1} = F_n(x_{n+1}) \quad \text{with} \quad f(x_n, x_{n+1}) = 0.$$

This work was written while the first author was visiting Sabanci University - Istanbul-Turkey in May-June 2005. The first author was also partially supported by CNPq-Brazil (PRONEX).

The upper bound below is called the *Drinfeld-Vladut bound* (see [2] and [10]):

$$\lambda(\mathcal{F}) \leq \sqrt{q} - 1, \quad \forall\, \mathbb{F}_q - \text{tower } \mathcal{F}.$$

When the cardinality q of the finite field is a square, there exist $\mathbb{F}_q$-towers $\mathcal{F}_1$ attaining the Drinfeld-Vladut bound (see [9] and [12]), and such towers $\mathcal{F}_1$ are called *optimal towers*. Again here much interest on the construction of optimal towers comes from applications to Coding Theory. For instance, Tsfasman-Vladut-Zink have used optimal towers to show the existence of infinite sequences of linear codes with increasing lengths having limit parameters above the so-called Gilbert-Varshamov bound (see [12]). For practical applications it is highly desirable to construct *explicit towers* with limits as big as possible (by an explicit tower we mean a tower $\mathcal{F}$ where each field F_n is described explicitely by algebraic equations). For examples of explicit optimal towers of function fields we refer to [4], [5], [7] and [3].

For $q = p^3$ with p a prime number, Zink (see [15]) has shown the existence of $\mathbb{F}_q$-towers $\mathcal{F}_2$ with limits satisfying

$$\lambda(\mathcal{F}_2) \geq \frac{2(p^2-1)}{p+2}.$$

The first explicit tower $\mathcal{F}_2$ attaining the Zink bound above was obtained for the case $p = 2$ by van der Geer-van der Vlugt; i.e., their tower $\mathcal{F}_2$ is an $\mathbb{F}_8$-tower satisfying the equality (see [8]):

$$\lambda(\mathcal{F}_2) = \frac{2 \cdot (2^2-1)}{2+2} = \frac{3}{2}.$$

For a generalization of both results above (the Zink bound and the van der Geer-van der Vlugt tower) we refer to [1].

Let $\mathcal{F} = (F_0, F_1, F_2, \dots)$ be an $\mathbb{F}_q$-tower. We are going to consider places P of the field F_0. The place P *splits in the tower* $\mathcal{F}$ if it is $\mathbb{F}_q$-rational and it splits completely in all extensions F_n/F_0. If a place P is ramified in some extension F_n/F_0, we say that it *ramifies in the tower* $\mathcal{F}$. The *splitting locus* of $\mathcal{F}$ *over* F_0 is defined as:

$$Z(\mathcal{F}/F_0) = \{P \mid P \text{ splits in } \mathcal{F}\}.$$

The *ramification locus* of $\mathcal{F}$ *over* F_0 is defined as:

$$V(\mathcal{F}/F_0) = \{P \mid P \text{ ramifies in } \mathcal{F}\}.$$

If the tower $\mathcal{F}$ is of *finite ramification type* (i.e., $V(\mathcal{F}/F_0)$ is a finite set), we then define

$$\deg V(\mathcal{F}/F_0) = \sum_{P \in V(\mathcal{F}/F_0)} \deg P.$$

We will be interested in the asymptotic behaviour of the sequence of fields below

$$\mathcal{E} := (E_0, E_1, E_2, \dots, E_n, \dots),$$

where E_n denotes the Galois closure of the extension F_n/F_0.

Our results here are: Proposition 2.1 gives a simple condition implying that $\mathcal{E}$ is also an $\mathbb{F}_q$-tower. Using the concept of 2-bounded towers (see Definition 1.3), we then prove in Theorem 2.2 a lower bound for the limit $\lambda(\mathcal{E})$ in some cases where the tower $\mathcal{F}$ is such that each extension F_{n+1}/F_n is a 2-bounded Galois p-extension. This gives a unified proof (see Theorems 2.5 and 2.7) for the limits of the Galois closures of the towers considered in [5], [8] and [4]. The Galois closure of the tame tower in [7] is considered here in Remark 2.4.

We will need at a crucial point (see the proof of Proposition 1.10) the following lemma from [6], where p denotes the characteristic of $\mathbb{F}_q$.

Lemma 0.1. *Let E_1/F and E_2/F be Artin-Schreier extensions of degree p of an $\mathbb{F}_q$-function field F, and let $E = E_1 \cdot E_2$ be the composite field. For a place Q of the field E, denote by Q_1, Q_2 and P its restrictions to the fields E_1, E_2 and F. Suppose that the different exponents $d(Q_i|P)$, for $i = 1$ and $i = 2$, satisfy*

$$d(Q_i|P) \in \{0, 2(p-1)\}.$$

Then the different exponents $d(Q|Q_i)$, for $i = 1$ and $i = 2$, also satisfy

$$d(Q|Q_i) \in \{0, 2(p-1)\}.$$

Remark 0.1. Lemma 0.1 was used in [6] for a simplification of the proofs of the limits of the towers considered in [5] and in [8].

1. B-BOUNDED TOWERS

We start with a definition.

Definition 1.1. Let $B \in \mathbb{R}$ be a real constant. A finite and separable field extension H_2/H_1 of $\mathbb{F}_q$-function fields is said *B-bounded* if for all places Q_2 of H_2 we have the inequality

$$d(Q_2|Q_1) \le B \cdot (e(Q_2|Q_1) - 1),$$

where $Q_1 := Q_2 \cap H_1$ denotes the restriction of the place Q_2 to the subfield H_1.

We will need the following simple result:

Proposition 1.2. *Let H_3/H_1 be a finite and separable extension of $\mathbb{F}_q$-function fields, and let H_2 be an intermediate field. If the extensions H_3/H_2 and H_2/H_1 are both B-bounded, then the extension H_3/H_1 is also B-bounded.*

Proof. Let Q_3 be a place of H_3 and denote $Q_2 := Q_3 \cap H_2$ and $Q_1 := Q_3 \cap H_1$. From the transitity of different exponents, we have

$$d(Q_3|Q_1) = e(Q_3|Q_2) \cdot d(Q_2|Q_1) + d(Q_3|Q_2).$$

Using that H_3/H_2 and H_2/H_1 are both B-bounded, we get

$$d(Q_3|Q_1) \le e(Q_3|Q_2) \cdot B \cdot (e(Q_2|Q_1) - 1) + B \cdot (e(Q_3|Q_2) - 1) = B \cdot (e(Q_3|Q_1) - 1).$$

□

Next we introduce this concept of B-boundedness to towers.

Definition 1.3. An $\mathbb{F}_q$-tower $\mathcal{F} = (F_0, F_1, \dots)$ is called *B-bounded* if all the extensions F_i/F_0 are B-bounded, for $i = 1, 2, \dots$.

Repeated applications of Proposition 1.2 gives us easily:

Proposition 1.4. *Let B be a real constant and let $\mathcal{F} = (F_0, F_1, F_2, \dots)$ be an $\mathbb{F}_q$-tower such that all the extensions F_{i+1}/F_i are B-bounded, for $i = 1, 2, \dots$. Then the tower $\mathcal{F}$ is B-bounded.*

In other words, Proposition 1.4 is saying that an $\mathbb{F}_q$-tower which is "stepwise" B-bounded is "globally" B-bounded. The importance of this concept is apparent from the next proposition, where the genus $\gamma(\mathcal{F})$ of a tower is defined as

$$\gamma(\mathcal{F}) := \lim_{n\to\infty} \frac{g(F_n)}{[F_n : F_0]}.$$

Proposition 1.5. *Let B be a real constant and suppose that a tower of function fields $\mathcal{F} = (F_0, F_1, \dots)$ is B-bounded and of finite ramification type. Then the genus $\gamma(\mathcal{F})$ satisfies the following inequality:*

$$\gamma(\mathcal{F}) \le g(F_0) - 1 + \frac{B}{2} \cdot \deg V(\mathcal{F}/F_0).$$

Proof. Since we are considering the genus, we can extend $\mathbb{F}_q$ to the algebraic closure $\overline{\mathbb{F}}_q$. In particular, $\deg V(\mathcal{F}/F_0)$ is the number of places of $F_0 \cdot \overline{\mathbb{F}}_q$ that ramify in $F_n \cdot \overline{\mathbb{F}}_q$, for some n. Since the extension F_i/F_0 is B-bounded we have

$$\deg \operatorname{Diff}(F_i/F_0) \le B \cdot [F_i : F_0] \cdot \deg V(\mathcal{F}/F_0).$$

We have used in the inequality above the so-called fundamental equality; i.e., that for a place P_0 of F_0 it holds

$$\sum_{j=1}^{r} e(P_j|P_0) = [F_i : F_0],$$

where $P_1, P_2, \dots, P_r$ are the distinct places of the field F_i above the place P_0. Note that since we are working over the algebraic closure $\overline{\mathbb{F}}_q$, there is no inertia and all places P_j are of degree one. The Hurwitz genus formula gives then

$$\begin{aligned} 2g(F_i) - 2 &= [F_i : F_0](2g(F_0) - 2) + \deg \operatorname{Diff}(F_i/F_0) \\ &\le [F_i : F_0](2g(F_0) - 2 + B \cdot \deg V(\mathcal{F}/F_0)). \end{aligned}$$

Dividing by $2[F_i : F_0]$ and letting $i \to \infty$, we get the desired inequality. □

Remark 1.6. Clearly we have that tame towers $\mathcal{F}$ are 1-bounded. One can show that the optimal tower over $\mathbb{F}_{q^2}$ in [4] is $(q+2)$-bounded. In [6] one finds a condition implying that certain recursive Artin-Schreier towers are 2-bounded.

Definition 1.7. Let $p = \operatorname{char}(\mathbb{F}_q)$. We say that a finite field extension is a *p-extension* if its degree is a power of the prime number p.

With some further assumptions, the reverse statement of Proposition 1.2 holds:

Proposition 1.8. *Let H_3/H_1 be a finite and separable p-extension of $\mathbb{F}_q$-function fields. Suppose that H_2 is an intermediate field such that both extensions H_3/H_2 and H_2/H_1 are Galois extensions. If the extension H_3/H_1 is 2-bounded, then also the extensions H_3/H_2 and H_2/H_1 are 2-bounded.*

Proof. Let P_1 be a place of H_1 and denote by P_3 a place of H_3 above P_1, and set $P_2 := P_3 \cap H_2$. Since both extensions H_3/H_2 and H_2/H_1 are Galois with degrees that are powers of the characteristic p, it follows from Hilbert's different formula (see [10]) that the following inequalities hold:

$$d(P_3|P_2) \geq 2(e(P_3|P_2) - 1) \text{ and } d(P_2|P_1) \geq 2(e(P_2|P_1) - 1).$$

The transitivity of different exponents then gives

$$\begin{aligned} d(P_3|P_1) &= e(P_3|P_2)d(P_2|P_1) + d(P_3|P_2) \\ &\geq e(P_3|P_2) \cdot 2 \cdot (e(P_2|P_1) - 1) + 2 \cdot (e(P_3|P_2) - 1) \\ &= 2 \cdot (e(P_3|P_1) - 1) \geq d(P_3|P_1), \end{aligned}$$

where the last inequality above follows from the hypothesis that the field extension H_3/H_1 is 2-bounded. Hence the inequalities above are in fact equalities, and we finally conclude that:

$$d(P_3|P_2) = 2(e(P_3|P_2) - 1) \text{ and } d(P_2|P_1) = 2(e(P_2|P_1) - 1).$$

□

Remark 1.9. If a Galois p-extension H_2/H_1 is 2-bounded then we have (for all places P_2 of the field H_2)

$$d(P_2|P_1) = 2(e(P_2|P_1) - 1),$$

since the inequality

$$d(P_2|P_1) \geq 2(e(P_2|P_1) - 1)$$

follows from Hilbert's different formula.

Now we deal with the concept of B-boundedness for composite fields. Let $E = E_1 \cdot E_2$ be the composite field of E_1 and E_2, where E_1 and E_2 are finite and separable extensions of an $\mathbb{F}_q$-function field F. If both E_1/F and E_2/F are 1-bounded (i.e., they are tame extensions), then clearly E/F is also 1-bounded. The next result deals with the 2-bounded case:

Proposition 1.10. *Let $E = E_1 \cdot E_2$ be the composite field as above. Suppose that both extensions E_1/F and E_2/F are Galois p-extensions and 2-bounded. Then the extension E/F is also a 2-bounded Galois p-extension.*

Proof. It is clear that E/F is a Galois p-extension. Since the Galois group of E_1/F is a finite p-group, say of order p^m, we can refine this extension

$$F = H_0 \subseteq H_1 \subseteq H_2 \subseteq \ldots \subseteq E_1 = H_m$$

in such a way that each H_{i+1}/H_i is a cyclic extension of degree p. Moreover each extension H_j/H_0 is Galois, for $j = 1, 2, \ldots, m$. Proposition 1.8 applied to $H_0 \subseteq H_{m-1} \subseteq H_m$ shows that both extensions H_m/H_{m-1} and H_{m-1}/H_0 are

2-bounded. Again, Proposition 1.8 applied to $H_0 \subseteq H_{m-2} \subseteq H_{m-1}$ shows that both extensions H_{m-1}/H_{m-2} and H_{m-2}/H_0 are 2-bounded, and so on. We have then refined the extension E_1/F into Galois steps of degree p and each step is a 2-bounded extension. Of course the same holds for the other extension E_2/F. Proposition 1.10 now follows from repeated applications of Lemma 0.1. □

Remark 1.11. Suppose that E_1/F is a tame extension and that E_2/F is a 2-bounded Galois p-extension. For a place Q of the composite field $E = E_1 \cdot E_2$, denote by Q_1, Q_2 and P its restrictions to E_1, E_2 and F. Denote by

$$m := e(Q_1|P) \text{ and } q := e(Q_2|P).$$

From Abhyankar's lemma (see [10]) we have:

$$e(Q|Q_2) = m \text{ and } e(Q|Q_1) = q.$$

Since $d(Q_2|P) = 2(q-1)$ (see Remark 1.9), from the transitivity of different exponents we conclude that

$$d(Q|Q_1) + q \cdot (m-1) = (m-1) + m \cdot 2(q-1).$$

Hence we have $d(Q|Q_1) = (m+1)\cdot(q-1)$. In particular the field extension E/E_1 is $(1+M)$-bounded with $M := \max\{e(Q_1|P); \text{ with } Q_1 \text{ a place of } E_1\}$.

2. The Galois closure of a tower

Let $\mathcal{F} = (F_0, F_1, F_2, \dots)$ be a tower of function fields over $\mathbb{F}_q$; in particular $\mathbb{F}_q$ is algebraically closed in F_n, for all n. Denote by E_n the Galois closure of the field extension F_n/F_0, for $n = 0, 1, 2, \dots$. The infinite sequence $\mathcal{E}$ of function fields

$$\mathcal{E} := (E_0 = F_0, E_1, E_2, \dots, E_n, \dots)$$

is called the *Galois closure* of $\mathcal{F}$ *over* F_0. Note that the inclusions $E_n \subseteq E_{n+1}$ are not necessarily strict and that the full constant field of E_n may be larger than $\mathbb{F}_q$.

We start with a simple condition ensuring that $\mathcal{E}$ is also an $\mathbb{F}_q$-tower; i.e., ensuring that the field $\mathbb{F}_q$ is algebraically closed in E_n, for all n.

Proposition 2.1. *Let $\mathcal{F}$ be an $\mathbb{F}_q$-tower with a nonempty splitting locus $Z(\mathcal{F}) \neq \emptyset$. Then*

a) *The Galois closure $\mathcal{E}$ is an $\mathbb{F}_q$-tower.*
b) *$Z(\mathcal{E}/F_0) = Z(\mathcal{F}/F_0)$.*
c) *$V(\mathcal{E}/F_0) = V(\mathcal{F}/F_0)$.*

Proof. Let P be a place of F_0 with $\deg P = 1$ that splits completely in all extensions F_n/F_0, for all n. If $\sigma : F_n \to \overline{F}_0$ is an embedding over F_0 into an algebraic closure $\overline{F}_0$ of the field F_0, then it is clear that the place P also splits completely in the field extension $\sigma(F_n)/F_0$. Since the Galois closure E_n is the composite of such fields $\sigma(F_n)$ (as σ varies), then the place P splits completely in E_n/F_0. This shows that $\mathbb{F}_q$ is algebraically closed in E_n, for all n, and this proves item a).

The inclusion $Z(\mathcal{E}/F_0) \subseteq Z(\mathcal{F}/F_0)$ is trivial, and the argument given above shows the other inclusion $Z(\mathcal{F}/F_0) \subseteq Z(\mathcal{E}/F_0)$. Hence item b) holds.

The inclusion $V(\mathcal{F}/F_0) \subseteq V(\mathcal{E}/F_0)$ is trivial. Reversely, if a place of F_0 is unramified in the extension F_n/F_0, it is unramified in $\sigma(F_n)/F_0$ (for all σ) and hence it is also unramified in the Galois closure E_n/F_0. □

Theorem 2.2. *Let $\mathcal{F} = (F_0, F_1, F_2, \dots)$ be an $\mathbb{F}_q$-tower and denote $p := \mathrm{char}(\mathbb{F}_q)$. Suppose that the hypothesis a), b) and c) below hold:*

a) *The splitting locus is nonempty; i.e., $Z(\mathcal{F}/F_0) \neq \emptyset$.*
b) *The ramification locus is finite; i.e., $\deg V(\mathcal{F}/F_0) < \infty$.*
c) *Each extension F_{n+1}/F_n is a 2-bounded Galois p-extension.*

If the tower $\mathcal{F}$ is asymptotically good, then its Galois closure $\mathcal{E}$ over F_0 is also asymptotically good. Moreover we have that the tower $\mathcal{E}$ is also 2-bounded with a limit satisfying:

$$\lambda(\mathcal{E}) \geq \frac{\#Z(\mathcal{F}/F_0)}{g(F_0) - 1 + \deg V(\mathcal{F}/F_0)}.$$

Proof. From Proposition 2.1 we know that $\mathcal{E}$ is an $\mathbb{F}_q$-tower such that

$$Z(\mathcal{E}/F_0) = Z(\mathcal{F}/F_0) \text{ and } V(\mathcal{E}/F_0) = V(\mathcal{F}/F_0).$$

We have clearly that

$$\lambda(\mathcal{E}) \geq \frac{\#Z(\mathcal{E}/F_0)}{\gamma(\mathcal{E})}.$$

If we show that $\mathcal{E}$ is also 2-bounded, then the result follows from Proposition 1.5. As follows from Proposition 1.4, we just have to show that each extension E_{n+1}/E_n in the tower $\mathcal{E} = (E_0 = F_0, E_1 = F_1, E_2, E_3, \dots)$ is a 2-bounded extension. Note that each extension E_{n+1}/E_n is a p-extension. We assume by induction that the extensions E_n/F_n and E_n/E_{n-1} are both 2-bounded (they are Galois p-extensions).

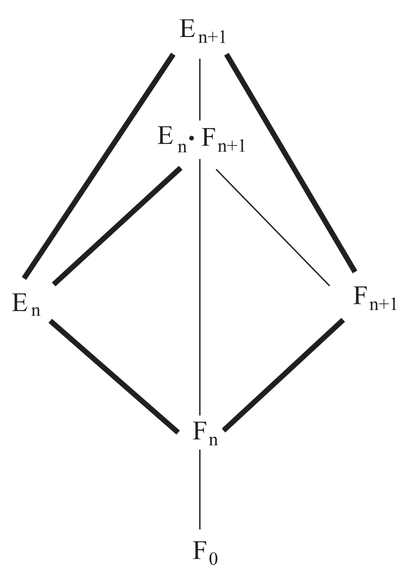

Figure 1

Considering the Galois extensions E_n/F_n and F_{n+1}/F_n, we get from Proposition 1.10 that the composite extension $E_n \cdot F_{n+1}/F_n$ is 2-bounded. Applying Proposition 1.8 to the situation below

$$F_n \subseteq E_n \subseteq E_n \cdot F_{n+1},$$

we see that $E_n \cdot F_{n+1}/E_n$ is also 2-bounded. Of course the field E_{n+1} is the Galois closure of the extension $E_n \cdot F_{n+1}/F_0$, and any embedding σ over F_0 of the field $E_n \cdot F_{n+1}$ is such that $\sigma(E_n) = E_n$. Hence $\sigma(E_n \cdot F_{n+1}) = E_n \cdot \sigma(F_{n+1})$ is a 2-bounded Galois p-extension of E_n, for all σ. Repeated applications of Proposition 1.10 gives that E_{n+1}/E_n is 2-bounded. Since E_{n+1}/E_n and E_n/F_n are 2-bounded, we get from Proposition 1.2 that E_{n+1}/F_n is 2-bounded. Applying now Proposition 1.8 to the situation

$$F_n \subseteq F_{n+1} \subseteq E_{n+1},$$

we conclude that the extension E_{n+1}/F_{n+1} is also 2-bounded. This finishes the proof of Theorem 2.2. □

Remark 2.3. Hypothesis a) and b) in Theorem 2.2 are very natural. Indeed, if a tower $\mathcal{E} = (E_0, E_1, E_2, \dots)$ is such that it is asymptotically good and there exists an index j such that the extensions E_n/E_j are Galois extensions for all $n \geq j$, then we have that the ramification locus $V(\mathcal{E}/E_0)$ is a finite set. In this situation we also have that there exists an index $m \geq 0$ and a rational place P of the field E_m that splits completely in the extensions E_n/E_m for all $n \geq m$ (see Theorem 2.26 in [7]).

Remark 2.4. Suppose $\mathcal{F}$ is a tame $\mathbb{F}_q$-tower satisfying the hypothesis a) and b) of Theorem 2.2. Then both towers $\mathcal{F}$ and $\mathcal{E}$ are tame and asymptotically good. Moreover,

$$\lambda(\mathcal{F}) \geq \lambda(\mathcal{E}) \geq \frac{\#Z(\mathcal{F}/F_0)}{g(F_0) - 1 + \deg V(\mathcal{F}/F_0)/2}.$$

The inequality $\lambda(\mathcal{F}) \geq \lambda(\mathcal{E})$ holds since $\mathcal{F}$ is a subtower of $\mathcal{E}$ (see [5]), and the other inequality follows easily from Propositions 1.5 and 2.1.

Let $\mathcal{F}$ be the recursive tower over $\mathbb{F}_{p^2}$ with p an odd prime number, given by the equation

$$Y^2 = \frac{X^2 + 1}{2X}.$$

One has that (see [7])

$$\#Z(\mathcal{F}/F_0) = 2p - 2 \quad \text{and} \quad \deg V(\mathcal{F}/F_0) = 6.$$

It follows that

$$\lambda(\mathcal{F}) = \lambda(\mathcal{E}) = p - 1;$$

i.e., the tower $\mathcal{F}$ and its Galois closure $\mathcal{E}$ are optimal towers over $\mathbb{F}_{p^2}$. □

Denote by $\mathcal{F}_1$ the recursive tower over $\mathbb{F}_{q^2}$ given by the equation

$$Y^q + Y = \frac{X^q}{1 + X^{q-1}}.$$

The tower $\mathcal{F}_1$ attains the Drinfeld-Vladut bound; i.e., $\lambda(\mathcal{F}_1) = q - 1$ (see [5]).

Denote by $\mathcal{F}_2$ the recursive tower over the finite field with 8 elements given by the equation

$$Y^2 + Y = \frac{X^2 + X + 1}{X}.$$

The tower $\mathcal{F}_2$ satisfies $\lambda(\mathcal{F}_2) = 3/2$ (see [8]).

The next theorem shows that their Galois closures over F_0 have the same limits.

Theorem 2.5. *Let $\mathcal{F}_1$ and $\mathcal{F}_2$ be as above, and denote by $\mathcal{E}_1$ and $\mathcal{E}_2$ their Galois closures over F_0. Then we have:*

$$\lambda(\mathcal{E}_1) = \lambda(\mathcal{F}_1) \quad \textit{and} \quad \lambda(\mathcal{E}_2) = \lambda(\mathcal{F}_2);$$

i.e., the tower $\mathcal{E}_1$ attains the Drinfeld-Vladut bound and the tower $\mathcal{E}_2$ attains the Zink bound for $p = 2$.

Proof. Both towers $\mathcal{F}_1$ and $\mathcal{F}_2$ satisfy the hypothesis in Theorem 2.2 (see [5], [8] and [6]). For the tower $\mathcal{F}_1$ we have (see [5])

$$\#Z(\mathcal{F}_1/F_0) = q^2 - q \quad \text{and} \quad \deg V(\mathcal{F}_1/F_0) = q + 1.$$

It follows from Theorem 2.2 that

$$\lambda(\mathcal{E}_1) \geq q - 1 \quad \text{and hence} \quad \lambda(\mathcal{E}_1) = q - 1.$$

The last equality above follows from the Drinfeld-Vladut bound.

For the tower $\mathcal{F}_2$ we have (see [8])

$$\#Z(\mathcal{F}_2/F_0) = 6 \quad \text{and} \quad \deg V(\mathcal{F}_2/F_0) = 5.$$

It follows from Theorem 2.2 that

$$\lambda(\mathcal{E}_2) \geq 3/2 \quad \text{and hence} \quad \lambda(\mathcal{E}_2) = 3/2.$$

The last equality above follows from

$$3/2 = \lambda(\mathcal{F}_2) \geq \lambda(\mathcal{E}_2),$$

since the tower $\mathcal{F}_2$ is a subtower of $\mathcal{E}_2$ (see [5]). ∎

Remark 2.6. The Galois closure $\mathcal{E}_1$ of the tower $\mathcal{F}_1$ above was also considered in the recent paper [14]. There a more computational proof is given that $\mathcal{E}_1$ is an optimal tower. In [11], applications of Galois towers to coding theory are discussed.

Now we deal with the Galois closure of the tower in [4]. Consider again the tower $\mathcal{F}_1$ above; i.e., the tower $\mathcal{F}_1 = (F_0, F_1, \dots)$ where $F_n = \mathbb{F}_{q^2}(z_0, z_1, \dots, z_n)$ with the relations

$$z_{i+1}^q + z_{i+1} = \frac{z_i^q}{1 + z_i^{q-1}}.$$

Consider the tower $\mathcal{F}_1' = (F_0', F_0, F_1, \dots)$ where $F_0' = \mathbb{F}_{q^2}(z_0')$ with $z_0^q + z_0 = z_0'$. Note that the extension F_0/F_0' is also 2-bounded and hence $\mathcal{F}_1'$ is 2-bounded. It is easily seen that only the zero and the pole of the function z_0' ramify in the tower $\mathcal{F}_1'$, and that the $(q-1)$ rational places of F_0' corresponding to $z_0' = \alpha$ with $\alpha \in \mathbb{F}_q^*$ are completely splitting. Note that the function $z_0^q + z_0$ takes elements of $\mathbb{F}_{q^2}$ into the subfield $\mathbb{F}_q$. Consider now the Kummer extension

$$H_0 := F_0'(x_0) \text{ with } x_0^{q+1} = z_0'$$

and denote by $\mathcal{H} := H_0 \cdot \mathcal{F}_1'$ the composite tower of $\mathcal{F}_1'$ with the field H_0; i.e.,

$$\mathcal{H} = (H_0, H_1, H_2, \dots) \text{ with } H_n := H_0 \cdot F_{n-1}.$$

Defining recursively elements $x_n \in H_n$ by $x_n := z_{n-1}/x_{n-1}$, one can check that the tower $\mathcal{H}$ above is the same as the tower in [4]. Let $\mathcal{E}_1'$ denote the Galois closure over F_0' of the tower $\mathcal{F}_1'$. It follows from Theorem 2.2 that $\mathcal{E}_1'$ is a 2-bounded tower. Finally, we consider the tower $\mathcal{G} := H_0 \cdot \mathcal{E}_1'$. All fields in the tower $\mathcal{G}$ are Galois extensions of the field F_0' and hence $\mathcal{G}$ contains the Galois closure of $\mathcal{H}$ over the field H_0. We show now that the tower $\mathcal{G}$ is optimal. From Proposition 2.1 we have

$$\#Z(\mathcal{E}_1'/F_0') = q-1 \quad \text{and} \quad \deg V(\mathcal{E}_1'/F_0') = 2.$$

From the definition of the field H_0 we have

$$\#Z(\mathcal{G}/H_0) = q^2-1 \quad \text{and} \quad \deg V(\mathcal{G}/H_0) = 2.$$

Note that the function x_0^{q+1} takes $\mathbb{F}_{q^2}^*$ into $\mathbb{F}_q^*$. The arguments in Remark 1.11 with $M = q+1$ show that the tower $\mathcal{G}$ is $(q+2)$-bounded and hence optimal, as follows from Proposition 1.5.

Since the Galois closure of $\mathcal{H}$ over H_0 is a subtower of $\mathcal{G}$ we have then proved:

Theorem 2.7. *Denoting by $\mathcal{H} := (H_0, H_1, \dots)$ the optimal tower over $\mathbb{F}_{q^2}$ in* [4]*, we have that its Galois closure over the field H_0 is also an optimal tower.*

Remark 2.8. Let $\mathcal{F}$ be an $\mathbb{F}_q$-tower and suppose that its Galois closure $\mathcal{E}$ over F_0 is also an $\mathbb{F}_q$-tower. It can happen that $\lambda(\mathcal{F}) > \lambda(\mathcal{E})$.

Question 2.9. What is the limit of the Galois closure of the tower in [1]?

Question 2.10. Are there recursive Galois towers? Are there asymptotically good recursive Galois towers?

References

[**1**] J. Bezerra, A. Garcia, H. Stichtenoth, *An explicit tower of function fields over cubic finite fields and Zink's lower bound for $A(q^3)$*, to appear in J. Reine Angew. Math.

[**2**] V. G. Drinfeld, S. G. Vladut, *The number of points of an algebraic curve*, Func. Anal. **17**, pp. 53-54, 1983.

[**3**] N. Elkies, *Explicit modular towers*, Proc. of the 35^{th} Annual Allerton Conference on Communication, Control and Computing, Urbana (IL) 1997.

[**4**] A. Garcia, H. Stichtenoth, *A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound*, Inventiones Math. **121**, pp.211-222, 1995.

[**5**] A. Garcia, H. Stichtenoth, *On the asymptotic behaviour of some towers of function fields over finite fields*, J. Number Theory **61**, pp. 248-273, 1996.

[**6**] A. Garcia, H. Stichtenoth, *Some Artin-Schreier towers are easy*, preprint 2005.

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

[**8**] G. van der Geer, M. van der Vlugt, *An asymptotically good tower of function fields over the field with eight elements*, Bull. London Math. Soc. **34**, pp 291-300, 2002.

[**9**] Y. Ihara, *Some remarks on the number of rational points of algebraic curves over finite fields*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28**, pp. 721-724, 1981.

[**10**] H. Stichtenoth, "Algebraic Function Fields and Codes", Springer Universitext, Berlin-Heidelberg, 1993.

[**11**] H. Stichtenoth, *Transitive and self-dual codes attaining the Tsfasman-Vladut-Zink bound*, preprint 2005.

[**12**] M. A. Tsfasman, S. G. Vladut, T. Zink, *Modular curves, Shimura curves, and Goppa codes, better than the Varshamov-Gilbert bound*, Math. Nachr. **109**, pp. 21-28, 1982.

[**13**] A. Weil, "Sur les courbes algébriques et les variétés qui s'en déduisent", Act. Sc. et Industrielles **1041**, Hermann, Paris, 1948.

[**14**] A. Zaytsev, *The Galois closure of the Garcia-Stichtenoth tower*, preprint 2005.

[**15**] T. Zink, *Degeneration of Shimura surfaces and a problem in coding theory*, in Fundamentals of Computation Theory, L. Budach (ed.), Lecture Notes in Computer Science, Vol. **199**, Springer, Berlin, pp. 503-511, 1985.

Authors' addresses:

A. Garcia, Instituto de Matemática Pura e Aplicada IMPA, 22460-320 Rio de Janeiro RJ, Brazil. e-mail: garcia@impa.br

H. Stichtenoth, Universität Duisburg-Essen, FB Mathematik, 45117 Essen, Germany. e-mail: stichtenoth@uni-essen.de
and Sabanci University – MDBF, 34956 – Tuzla-Istanbul, Turkey.