# Asymptotically Good Towers of Global Fields

Farshid Hajir and Christian Maire

**Abstract.** The study of the maximal $p$-extension of a global field $k$ unramified everywhere and totally split at a finite set of places of $k$ has at least two important applications: it gives information on the asymptotic behavior of discriminants versus degree in the number field case (as measured by the Martinet constant $\alpha(t)$), and on the relationship between genus and the number of places of degree one (for large genus) in the function field case (as measured by the Ihara constant $A(q)$). We survey recent work on class-field-theoretical constructions of towers of global fields which are optimal for the study of these phenomena, including best known examples in both settings; these contain, among others, an infinite unramified tower of totally complex number fields with small root discriminant improving Martinet's record. We show that allowing wild ramification to limited depth does lead to asymptotically good towers. However, we demonstrate also that the investigation of the infinitude of these towers involves difficulties absent in the tame case.

## 1. Introduction and Definitions

An infinite tower of global fields $K_0 \subset K_1 \subset K_2 \cdots$ is "asymptotically good" if the relationship between certain of its layers' invariants is in some sense optimal. The precise condition is: (1) for number fields, that $\mathrm{rd}_{K_i} := |\operatorname{disc} K_i|^{1/[K_i:\mathbb{Q}]}$ remain bounded from above, and (2) for function fields with fixed finite constant field $\mathbb{F}_q$, that $N_{K_i}/g_{K_i}$ remain bounded away from 0, where $g_K$, $N_K$ are, respectively, the genus, and the number of places of degree 1 of $K$.

The relationship between these invariants ($\mathrm{disc}_K$ vs. $[K:\mathbb{Q}]$, and $g_K$ vs. $N_K$) are governed by important general bounds (Stark-Odlyzko for number fields and Hasse-Weil for function fields). The interest of asymptotically good towers is that they measure the sharpness of the leading terms of these bounds.

In the number field case, currently the only method for constructing asymptotically good towers is that of $p$-class field towers, for a fixed prime $p$. The same method works well for function fields; however, at least when $q$ is a square, there

F. Hajir was partially supported by a Mathematical Sciences Postdoctoral Fellowship from the NSF.

are other rich sources of asymptotically good towers as well: modular curve constructions [14], certain types of explicit equations [7] (which potentially are always modular! cf. [4]), and a new "rigid" construction of Frey, Kani, and Völklein [6].

In this paper, we survey the $p$-class field tower constructions. One fixes a prime $p$ and a finite non-empty set $S$ of places of a base field $K$ and studies the maximal $p$-extension of $K$ which is everywhere unramified and totally split at $S$. For these applications, it is also possible to allow a finite number of places to ramify, as long as we can obtain a bound for the minimal number of relations of the Galois groups which appear. In §2 we recall all of this; we give the best known examples for totally complex and totally real number fields (§3) and for function fields over fields with 2, 3 and 5 elements (§4).

In §5 we consider extensions where wild ramification can occur but only to a limited depth; we show first that these lead to asymptotically good towers. We state a theorem (theorem 5.5) which shows that allowing wild ramification leads to complications in the study of the minimal number of relations of the resulting Galois groups.

We conclude with some open problems which come up naturally in the search for asymptotically good towers.

### 1.1. Martinet's constant

For a number field $k$ of degree $n = r_1 + 2r_2$ over $\mathbb{Q}$, with signature $(r_1, r_2)$, let $t = t_k := r_1/n$ be its "infinity type," i.e. the proportion of its embeddings into $\mathbb{C}$ which factor through $\mathbb{R}$. We will write $\mathrm{disc}_k$, $\mathrm{rd}_k$ for its discriminant and root discriminant, respectively. Thanks to the work of Stark [32], Odlyzko [22, 23], Poitou [25] and Serre [30], we have a very good lower bound for $\mathrm{rd}_k$, an asymptotic version of which reads: for a number field $k$ of infinity type $t$ and large enough degree,

$$\mathrm{rd}_k \geq A^t B^{1-t}\,, \tag{1}$$

with $A = 60$, $B = 22$; under GRH, one may take $A = 215$, $B = 44$.

For fixed $t \in \mathbb{Q} \cap [0,1]$, and integers $n$ such that number fields of degree $n$ and infinity type $t$ exist, we let $\alpha_n(t)$ be the minimal root discriminant attained by number fields of degree $n$ and infinity type $t$ and define

$$\alpha(t) = \liminf_n \alpha_n(t)\,.$$

For more details see [18, 10]. From (1), we see that

$$\alpha(t) \geq A^t B^{1-t}, \quad t \in \mathbb{Q} \cap [0,1]\,.$$

A nested sequence of distinct number fields $K_0 \subset K_1 \subset \cdots$ is "asymptotically good" (Tsfasman-Vladut [34]) if $\mathrm{rd}_{K_j}$ is bounded from above. An asymptotically good tower with fixed infinity type $t$ and root discriminant bounded above by $R$ gives an upper bound $\alpha(t) \leq R$. In §4, we will present the best current upper bounds for $\alpha(0)$ and $\alpha(1)$, namely (see [11])

$$B \leq \alpha(0) < 82.2, \quad A \leq \alpha(1) < 954.3\,.$$

### 1.2. Function field case

We will fix a finite field $\mathbb{F}_q$ and ask how large the group of rational points $X(\mathbb{F}_q)$ of a smooth absolutely irreducible algebraic curve $X$ of genus $g$ over $\mathbb{F}_q$ can be as $g$ tends to infinity. Actually, to maintain notational consistency with number fields, we will consider the corresponding function fields $K = \mathbb{F}_q(X)$ and count the places of degree 1. Let $N_q(g)$ be the maximum number of degree 1 places of a genus $g$ function field with contant field $\mathbb{F}_q$. By the celebrated theorem of Hasse-Weil,

$$N_q(g) \leq q + 1 + 2g\sqrt{q}\,.$$

Various improvements of this bound have been obtained in the last two decades. To measure the asymptotically optimal bound, Ihara introduced

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

In the 80's, Ihara [14] and, Tsfasman, Vladut and Zink [35] independently showed by using modular curves that $A(q) \geq \sqrt{q} - 1$ if $q$ is a square. Shortly thereafter, Drinfeld and Vladut [3] proved that for all $q$,

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

and so $A(q) = \sqrt{q} - 1$ for square $q$. Using class field towers, Serre showed that there is an absolute constant $c > 0$ such that $A(q) > c \log q$ for all $q$. Variations on Serre's proof [31] can be found in Neiderreiter-Xing [21], Temkine [33] and Li-Maharaj [17]. Recently, Elkies, Kresch, Poonen, Wetherell, and Zieve [5] have shown that $\liminf_g N_q(g)/g \geq (\sqrt{q} - 1)/3$ for square $q$ and $\liminf_g N_q(g)/g \geq c' \log q$ for an absolute constant $c' > 0$ (all $q$). When $q$ is not prime, it can be shown that the growth of $A(q)$ is faster than logarithmic (e.g. [21, 33, 17]). The major outstanding problem here is, then, to improve Serre's lower bound for $A(q)$ when $q$ is prime.

We will be contented here with describing what is known for three small prime values of $q$, namely $q = 2$, 3 and 5. The best known bounds are: $A(2) \geq 81/317$ (see [19]), $A(3) \geq 12/25$ (see [1]) and $A(5) \geq 8/11$ (see [2, 33]): we will present these examples in §4.

## 2. Tamely Ramified Situation

We fix a prime $p$ and two finite sets $S$ and $T$ of places of $k$ such that:

1. In the function field case, $S$ is non-empty and contains only degree 1 places.
2. In the number field case, $S$ contains all infinite places $S_\infty$ of $k$.
3. $S \cap T = \emptyset$.
4. For all places $\mathfrak{p} \in T$, $p$ divides $\mathbb{N}\mathfrak{p} - 1$, where $\mathbb{N}\mathfrak{p}$ is the absolute norm. In the function field case that means that $p$ divides $q^{\deg(\mathfrak{p})} - 1$ for $\mathfrak{p} \in T$.

Now we define $k_T^S$ to be the maximal $p$-extension (inside a fixed algebraic closure) of $k$ unramified ouside $T$ in which $S$ splits completely. By our assumptions, the

ramification in $k_T^S/k$ is tame; put $G_T^S = \mathrm{Gal}(k_T^S/k)$. One has to introduce two quantities:

**Definition 2.1.** *Let $G$ be a finitely generated pro-$p$-group. Then*

1. *$d(G)$ is the minimal number of generators of $G$: $d(G) = \dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p)$.*
2. *$r(G)$ is the minimal number of relations of $G$: $r(G) = \dim_{\mathbb{F}_p} H^2(G, \mathbb{F}_p)$.*

By the Burnside Basis Theorem, the generator rank of a group is the same as that of its maximal abelian quotient, thus $d(G_T^S)$ can be understood in terms of class field theory (it is the $p$-rank of the $S$-ray class group mod $T$). The deepest known fact about these groups was first established by Shafarevich (see [15], or [2]):

**Theorem 2.2.** *With the above assumptions,*

$$r(G_T^S) - d(G_T^S) \leq |S| - 1 + \theta_{k,T}\,,$$

*where $\theta_{k,T} = 1$ when $k$ contains $\mu_p$ and $T = \emptyset$, 0 otherwise.*

**Remark 2.3.** *One has the trivial inequalities: $d(G_\emptyset^S) \leq d(G_T^S) \leq d(G_\emptyset^S) + |T|$.*

The famous Theorem of Golod-Shafarevich says that for a non-trival finite $p$-group $G$, $r(G) > d(G)^2/4$. Thus,

**Theorem 2.4.** *If*

$$d(G_T^S) \geq 2 + 2\sqrt{|S| + \theta_{k,T}}\,,$$

*then $G_T^S$ is infinite.*

The last ingredient we need is a standard genus theory bound for the $p$-rank of the $S$-class group in a degree $p$ Galois extension.

**Theorem 2.5.** *Suppose $k/k'$ is a Galois extension of degree $p$. Let $S' = S \cap k'$ be the set of places of $k'$ lying under the places in $S$. Suppose $r$ places of $k'$ ramify in $k$. Then*

$$d(G_\emptyset^S) \geq r - |S'| - \delta_{k'}\,,$$

*where $\delta_{k'} = 1$ when $k'$ contains $\mu_p$, 0 otherwise.*

For this and more refined genus theory bounds, see e.g. [28, 27].

## 3. Number Fields

A first observation is that the layers of an infinite tamely ramified tower form an asymptotically good family, (i.e. they have bounded root discriminant) [10]:

**Theorem 3.1.** *Let $k$ be a number field of degree $n$ over $\mathbb{Q}$ of infinity type $t$ such that $G_T^S$ is infinite. Then*

$$\alpha(t) \leq \mathrm{rd}_k \prod_{\mathfrak{p} \in T} \left(N_{k/\mathbb{Q}}\mathfrak{p}\right)^{1/n}.$$

### 3.1. Martinet's example

The first idea was to construct a number field $k$ with small root discriminant admitting an infinite *unramified* 2-extension ($S = S_\infty$, $T = \emptyset$). The layers of such a tower comprise a family with *constant* root discriminant. Since 1978, the best such example known has been that of Martinet [18]: he proved that the field $\mathbb{Q}(\cos(2\pi/11), \sqrt{2}, \sqrt{-23})$ with root discriminant $2^{3/2}11^{4/5}23^{1/2}$ has an infinite unramified 2-tower ($T = \emptyset$, $S = S_\infty$), and so $\alpha(0) < 92.4$. Martinet also provided a totally real infinite unramified tower: $\mathbb{Q}(\sqrt{2}, \sqrt{29}, \sqrt{3 \cdot 5 \cdot 7 \cdot 23 \cdot 29})$ has an infinite unramified 2-tower, giving $\alpha(1) < 1058.6$.

### 3.2. An infinite unramified tower which improves Martinet's record

In [10], we found that class field towers over non-Galois base fields seem to yield asymptotically good towers. We now apply that idea to give an unramified tower with root discriminant smaller than the previous example.

Let $k' = \mathbb{Q}(\xi)$ where $\xi$ is a root of $f = x^5 - 2x^4 + 3x^3 - 3x^2 - x + 1$. The discriminant of $f$ is $-31391$, a prime; thus, this is also the discriminant of $k'$, and $\mathcal{O}_{k'} = \mathbb{Z}[\xi]$. Since $\mathrm{disc}_{k'}$ is negative, $k'$ has signature $(3, 1)$. Since $\mathrm{disc}_{k'}$ is a quadratic discriminant, it follows (see Kondo [16]) that the Galois group of $f$ is $S_5$; indeed, the Galois closure of $k'$ is an unramified $A_5$-extension of $\mathbb{Q}(\sqrt{-31391})$. We will not need this fact, however.

The element $\eta = -36\xi^4 + 125\xi^3 - 221\xi^2 + 182\xi - 80 \in \mathcal{O}_{k'}$ is negative at all three real places of $k'$. Its minimal polynomial is $g(y) = y^5 + 223y^4 + 18336y^3 + 10907521y^2 + 930369979y + 18559139599$. The $\mathcal{O}_{k'}$-ideal it generates factors into nine prime ideals of $\mathcal{O}_{k'}$: $\eta = \pi_7\pi'_7\pi_{11}\pi'_{11}\pi_{13}\pi_{19}\pi'_{19}\pi_{23}\pi_{29}$ where $\pi_r$ generates an ideal of norm $r$. We let $k = k'(\sqrt{\eta})$, a totally complex field of degree 10. A defining polynomial for $k$ is $g(y^2)$. We note that $\eta$ is congruent to a square modulo $4\mathcal{O}_k$; explicitly, $\eta = \beta^2 - 4\gamma$ with $\beta = \xi^4 + \xi + 1$ and $\gamma = 11\xi^4 - 31\xi^3 + 56\xi^2 - 45\xi + 20$. Thus, $k/k'$ is ramified at the three real places and at the nine primes dividing $\eta$ and nowhere else. Thus, the root discriminant of $k$ is $rd_k = 31391^{1/5}(7^2 \cdot 11^2 \cdot 13 \cdot 19^2 \cdot 23 \cdot 29)^{1/10} = 84.375\ldots$ By theorem 2.5 ($p = 2$), the 2-rank of the ideal class group of $k$ is at least $9+3-(3+1)-1 = 7$. (This is confirmed by a Pari calculation which gives $\mathrm{Cl}_k = \mathbb{Z}/3 \oplus (\mathbb{Z}/2)^7$.) By theorem 2.4, $k$ admits an infinite everywhere unramified 2-tower since $2 + 2\sqrt{5+1} = 2 + \sqrt{24} < 7$. To our best knowledge, this tower gives the least root discriminant for an *unramified* tower which is known to be infinite.

### 3.3. The best known bounds for $\alpha(0)$ and $\alpha(1)$

Tamely ramified towers and asymmetric (non-Galois) constructions of the base (such as the one presented above) were two ideas introduced in [10] for improving Martinet's constant. We briefly present the best known current estimates for $\alpha(0)$ and $\alpha(1)$ (see [11] for details).

**3.3.1.** TOTALLY COMPLEX SITUATION The totally imaginary field $k = \mathbb{Q}(\theta)$ where $\theta$ is a root of

$$x^{12} + 339x^{10} - 19752x^8 - 2188735x^6 + 284236829x^4 + 4401349506x^2 + 15622982921$$

has discriminant $7 \cdot 13 \cdot 19^2 \cdot 23^4 \cdot 29 \cdot 31 \cdot 35509^2$; it admits an infinite 2-extension ramified at a prime $\mathfrak{p}_9$ with absolute norm 9 and unramified everywhere else. Thus $\alpha(0) \leq \mathrm{rd}_k \cdot 9^{1/12} < 82.2$.

**3.3.2.** TOTALLY REAL SITUATION The totally real field $k = \mathbb{Q}(\theta)$ where $\theta$ is a root of

$$x^{12} - 56966x^{10} + 959048181x^8 - 5946482981439x^6 + 14419821937918124x^4 - 12705425979835529941x^2 + 352705306960207836 8989$$

has discriminant $7^{10} \cdot 13^7 \cdot 29^4 \cdot 41^4 \cdot 97 \cdot 113^2$; it admits an infinite 2-extension ramified at a prime $\mathfrak{p}_{13}$ with absolute norm 13 and unramified elsewhere. Thus $\alpha(1) \leq \mathrm{rd}_k \cdot 13^{1/12} < 954.3$.

## 4. Function Fields

As in the number field case, a tamely ramified $p$-extension of function fields is asymptotically good, meaning $N_K/g_K$ is bounded from below for the layers $K$ of the $p$-extension. (This was used in [2] to give improved lower bounds for $A(3)$ and $A(5)$.) To be precise, [2]:

**Theorem 4.1.** *Fix a prime $p$ not dividing $q$. Let $k$ be a genus $g$ function field with constant field $\mathbb{F}_q$, $S$ a non-empty set of degree 1 places of $k$, $T$ a (possibly empty) set of places of $k$ disjoint from $S$. If $G_T^S$ is infinite, then*

$$A(q) \geq \frac{|S|}{g - 1 + \frac{1}{2}\sum_{\mathfrak{p} \in T} \deg \mathfrak{p}}\,.$$

### 4.1. Unramified towers

The best lower bound for $A(2)$ has been given by Niederreiter and Xing [19]:

Let $k = \mathbb{F}_2(x)$, $N_0 = x^4$ and $N_1 = (x^2 + x + 1)(x^6 + x^3 + 1) \in F_2[x]$. Let $K_i$ be the subfield of the cyclotomic function field $k_{N_i}$ associated to $N_i$ for $i = 0, 1$ (for more details see [13]). Consider now the subfield $F_i$ of $K_i$ fixed by $\langle \overline{x+i} \rangle$. Put $F = F_0F_1$. Then $[F : k] = 84$. Now let $S$ be the set of places of $F$ lying over $\infty$ together with one place lying over $x$. Then $|S| = 81$. For this example, and $p = 2$, $G_\emptyset^S$ is infinite, and so

$$0.255 < \frac{81}{317} \leq A(2) \leq \sqrt{2} - 1 < 0.414\,.$$

**4.2. Tamely ramified towers**

The following example is from [1]: Let $k = \mathbb{F}_3(x, \sqrt{D})$, where $D = (x^{27} - x)(x^9 - x)(x+1)(x^3 - x)^{-2}(x^3 - x^2 + x + 1)^{-1} \in \mathbb{F}_3[x]$; the polynomial $D$ has 11 prime factors over $\mathbb{F}_3$. If we take $p = 2$, $S$ to be the set of $k$-places above $x$, $x - 1$ and $1/x$, $T$ to consist of the unique $k$-place above $x + 1$, Golod-Shafarevich implies that $k_T^S$ is infinite, hence by theorem 4.1,

$$0.48 = 12/25 \leq A(3) \leq \sqrt{3} - 1 < 0.74\,.$$

The following example is from [2]. For the field $k = \mathbb{F}_5(x, \sqrt{D})$ where $D = (x-1)(x-2)(x-3)(x-4)(x^2+x+1)(x^2+3)(x^2+2)(x^2+x+2)(x^2+2x+3)$ with $p = 2$, $S$ all places above $x$ and $1/x$, and $T$ the place above $x - 1$, one has $k_T^S/k$ is infinite and then

$$0.72 < 8/11 \leq A(5) \leq \sqrt{5} - 1 < 1.24\,.$$

Note that by using unramified extensions, Temkine [33] has recovered the same bound for $A(5)$.

## 5. Wild Ramification

We fix a prime $p$. Now we suppose (for simplicity) that $T$ consists solely of places dividing $p$ in the number field case, and in the function field case we suppose that $p \mid q$. To each prime $\mathfrak{p} \in T$ we associate $i_\mathfrak{p} \in [0, \infty]$. We call $T(I) = \{(\mathfrak{p}, i_\mathfrak{p}), \mathfrak{p} \in T\}$, and define $k_{T(I)}^S$ as being the maximal $p$-extension of $k$ unramified outside $T$, totally decomposed for all places in $S$, such that $D_\mathfrak{p}^{(i_\mathfrak{p})}$ is trivial, for all $\mathfrak{p}$ in $T$, where $D_\mathfrak{p}^{(i_\mathfrak{p})}$ is the ramification group with upper numbering (see for example [29] for more details). The condition $i_\mathfrak{p} = \infty$ means that there is no restriction for ramification at $\mathfrak{p}$. Note that we can assume without loss of generality that $i_\mathfrak{p} > 1$ as the following proposition demonstrates.

**Proposition 5.1.** *If $i_\mathfrak{p} \leq 1$, $\mathfrak{p}$ is unramified in $k_{T(I)}^S/k$.*

*Proof.* Fix $\mathfrak{p} \in T$. Let $K$ be a field such that $k \subset K \subset k_{T(I)}^S$. By the restriction property of ramification groups, $D_\mathfrak{p}^{(i_\mathfrak{p})}(K/k)$ is trivial. Put $n = \psi_{K/k}(i_\mathfrak{p})$ where $\psi_{K/k}$ is the Herbrand function associated to $\mathfrak{p}$ in $K/k$: $D_\mathfrak{p}^{(i_\mathfrak{p})}(K/k) = \{1\} \Rightarrow D_{\mathfrak{p},(n)}(K/k) = \{1\}$ where $D_{\mathfrak{p},(j)}(K/k)$ is the ramification group with lower numbering. If $n \leq 1$, then since $D_{\mathfrak{p},(1)}(K/k) \subset D_{\mathfrak{p},(n)}(K/k)$, we find that $D_{\mathfrak{p},(1)}(K/k) = \{1\}$. But $D_{\mathfrak{p},(0)}(K/k)/D_{\mathfrak{p},(1)}(K/k)$ has order prime to $p$ and $D_{\mathfrak{p},(0)}(K/k)$ is a $p$-group, hence $D_{\mathfrak{p},(0)}(K/k) = \{1\}$.

Now we want to show that $n \leq 1$. Suppose $n \geq 1$; $m = \lfloor n \rfloor \geq 1$. We have

$$i_\mathfrak{p} = \psi_{K/k}^{-1}(n) = \frac{g_1 + \cdots + g_m + (n-m)g_{m+1}}{g_0}$$

where $g_i = |D_{\mathfrak{p},(i)}(K/k)|$. Since $D_{\mathfrak{p},(0)}(K/k)/D_{\mathfrak{p},(1)}(K/k)$ is trivial, $g_0 = g_1$. So one obtains ([29, Chapter IV §3]):

$$1 + \frac{m-1}{g_0} + \frac{(n-m)g_{m+1}}{g_0} \leq i_p \leq 1\,,$$

giving $n = m = 1$. □

The main question of this section is the following:

**Problem 5.2.** *What is the relation rank of the group $G^S_{T(I)}$?*

Before looking more closely at this question we explain why it is interesting for the problem of finding asymptotically good towers.

**Theorem 5.3.** *Assume that for all $\mathfrak{p} \in T$, $i_\mathfrak{p} > 1$ is finite. Suppose that $k^S_{T(I)}/k$ is infinite. Then*

1) *In the number field case, if $k$ has degree $n$ and infinity type $t$, one has:*

$$\alpha(t) \leq \mathrm{rd}_k \cdot \left( \prod_{\mathfrak{p} \in T} N_{k/\mathbb{Q}} \mathfrak{p}^{i_\mathfrak{p}+1} \right)^{1/n}.$$

2) *In the function field case, suppose $p \mid q$, $k$ is a genus $g$ function field with constant field $\mathbb{F}_q$, $S$ is a non-empty set of degree 1 places of $k$ disjoint from $T$; then one has:*

$$A(q) \geq \frac{|S|}{g - 1 + \frac{1}{2}\sum_{\mathfrak{p} \in T}(i_\mathfrak{p}+1)\deg \mathfrak{p}}\,.$$

*Proof.* Let $K$ be such that $k \subset K \subset k^S_{T(I)}$. By restriction, for all $\mathfrak{p} \in T$, $D^{(i_\mathfrak{p})}_\mathfrak{p}(K/k)$ is trivial. Let $\mathfrak{p} \in T$. By definition one has:

$$D^{(i_\mathfrak{p})}_\mathfrak{p}(K/k) = D_{\mathfrak{p},(\psi_{K/k}(i_\mathfrak{p}))}(K/k)\,,$$

where $\psi_{K/k}$ is Herbrand function. Put $n = \psi_{K/k}(i_\mathfrak{p})$ and $m = \lfloor n \rfloor$. Then for all $\mathfrak{P} \mid \mathfrak{p}$, $\mathfrak{P}$ a prime of $K$, one knows the $\mathfrak{P}$-valuation $v_\mathfrak{P}(\mathcal{D}_{K/k})$ of the different of $K/k$ [29]:

$$v_\mathfrak{P}(\mathcal{D}_{K/k}) = g_0 + g_1 + \cdots + g_m - (m+1)\,,$$

where $g_j = |D_{\mathfrak{p},(j)}(K/k)|$; $g_j = 1$ for all $j \geq m+1$. If we use the definition of $\psi$, and the fact that $\varphi = \psi^{-1}$ is the reciprocal function, one gets:

$$i_p = \varphi_{K/k}(n) = \frac{g_1 + \cdots + g_m + (n-m)}{g_0}\,,$$

and then

$$\begin{aligned} v_\mathfrak{P}(\mathcal{D}_{K/k}) &= g_0 + g_1 + \cdots + g_m - (m+1) \\ &= g_0(i_\mathfrak{p}+1) - (m+1) - (n-m) \\ &\leq e_\mathfrak{P}(K/k)(i_\mathfrak{p}+1) \end{aligned}$$

because $g_0 = e_\mathfrak{P}(K/k)$. The rest follows easily as in [2]. □

### 5.1. A sub-extension of $k^S_{T(I)}$

For a finite extension $K/k$ we consider $T_K$ and $S_K$ the set of places of $K$ above $T$ and $S$. For all places $\mathfrak{P} \in T_K$ we let $i_{\mathfrak{P}} = i_{\mathfrak{p}}$ where $\mathfrak{P} \cap \mathcal{O}_k = \mathfrak{p} \in T$, and we write simply $K^S_{T(I)}$ instead of $K^{S_K}_{T_K(I_K)}$.

So now we can define $k_\infty \subseteq k^S_{T(I)}$ inductively as follows: start with $k_0 = k$; for each $i \geq 0$, let $k_{i+1}$ be the maximal abelian extension of $k_i$ contained in $(k_i)^S_{T(I)}$; for the whole tower, put $k_\infty = \cup k_i$. Then $k_\infty \subseteq k^S_{T(I)}$. Note that in the tamely ramified situation, $k_\infty = k^S_{T(I)}$. Put $G = \mathrm{Gal}(K_\infty/k)$. In [24] Perret proposed a bound for $r(G) - d(G)$ when $G$ is finite. Niederreiter and Xing [20] showed that Perret's conjecture would imply the infinitude of a certain tower over $\mathbb{F}_2$ violating the Drinfeld-Vladut bound.

We note that if $k_\infty/k$ is infinite, it gives better estimates for $\alpha(t)$ and $A(q)$ than those of theorem 5.3, namely:

- $\alpha(t) \leq \mathrm{rd}_k \cdot \left( \prod_{\mathfrak{p} \in T} \left(N_{k/\mathbb{Q}}\right) \mathfrak{p}^{\lfloor i_\mathfrak{p} \rfloor^* + 1} \right)^{1/n}$, in the number field case and
- $A(q) \geq \dfrac{|S|}{g - 1 + \frac{1}{2} \sum_{\mathfrak{p} \in T} (\lfloor i_\mathfrak{p} \rfloor^* + 1) \deg \mathfrak{p}}$ in the function field case,

where $\lfloor i_\mathfrak{p} \rfloor^* = \lfloor i_\mathfrak{p} \rfloor$ if $i_\mathfrak{p}$ is not an integer, $\lfloor i_\mathfrak{p} \rfloor^* = i_\mathfrak{p} - 1$ otherwise.

This comes from the following observation: If $\mathfrak{p}$ is ramified in $K/k$, let

$$n(i_\mathfrak{p}) = \sup_j \{ D^{(j)}_\mathfrak{p}(K/k) \neq \{e\} \}.$$

Then $n(i_\mathfrak{p}) \leq i_\mathfrak{p}$. But if $K/k$ is an abelian extension we know that $n(i_\mathfrak{p})$ is an integer and so $n(i_\mathfrak{p}) \leq \lfloor i_\mathfrak{p} \rfloor^*$: this is the Hasse-Arf Theorem (see [29] for example). To conclude we use the proof of Perret [24].

### 5.2. Iwasawa theory

Suppose that for all $\mathfrak{p} \in T$, $i_\mathfrak{p} = \infty$. Then the difference $r - d$ is well-understood (see [15, 9]). In particular, if $T$ contains all places of $k$ above $p$ with $i_\mathfrak{p} = \infty$, then $r - d = -(r_2 + 1)$ (for $p > 2$).

One has the following natural question:

**Problem 5.4.** *Can one give explicitly a function $f$ depending on $S$ and on $T(I)$ with* **values in** $\mathbb{R}$ *such that*

$$r(G^S_{T(I)}) - d(G^S_{T(I)}) \leq f(S, T(I))?$$

When all the indices $i_\mathfrak{p} = \infty$, Shafarevich has given a very satisfactory answer. However, at least when some of the indices in $I$ are finite and others are not, the groups in question are not even necessarily finitely presentable! For example, we have the following theorem [12]:

**Theorem 5.5.** *Let $p = 2$. Let $\ell$ be a prime such that $\ell \equiv -1 \pmod{16}$ and put $k = \mathbb{Q}(\sqrt{-\ell})$. Let $\mathfrak{p}_1$ and $\mathfrak{p}_2$ be the two primes of $k$ above 2. Take $1 < i_{\mathfrak{p}_1} < \infty$ and $i_{\mathfrak{p}_2} = \infty$. Then $G^S_{T(I)}$ is a finitely generated pro-2-group with $r(G^S_{T(I)}) = \infty$.*

*Proof.* We give only the two crucial points of the proof:

1) The condition on $\ell$ forces the decomposition group of $\mathfrak{p}_1$ in $k^S_{T(I)}/k$ to be exactly the absolute Galois group of the maximal $p$-extension $\mathcal{K}_{\mathfrak{p}_1}$ of $k_{\mathfrak{p}_1}$ (the completion of $k$ at $\mathfrak{p}_1$): this is an application of a result of Wingberg [36].
2) Let $\mathcal{G}$ be the Galois group of the absolute $p$-extension of a local field $k$, and let $\mathcal{G}^i$ be the subgroup of $\mathcal{G}$ with upper numbering. Then for $i > 1$ the number of relations of $\mathcal{G}/\mathcal{G}^i$ is infinite: this is a result of Gordeev [8]. □

In view of theorem 5.3, it would be very interesting to investigate the above problem when all the indices are finite.

## 6. Two Further Questions

To finish we want to mention two questions. The first is studied in [11]:

**Problem 6.1.** *Does every infinite $T$-ramified $p$-tower $k^S_T/k$ contain an intermediate field $K$ (of finite degree over $k$) such that $K$ has an infinite* unramified *$p$-tower $K^S_\emptyset/K$?*

**Problem 6.2.** *Consider, for simplicity, the number field situation and $p = 2$. Suppose that for all primes $\mathfrak{p}$ of $k$ not dividing 2, the maximal $\{\mathfrak{p}\}$-ramified 2-extension $k_{\{\mathfrak{p}\}}$ over $k$ is infinite. Does this imply that the maximal unramified 2-extension of $k$ is infinite?*

The second can give a very nice application for bounding $\alpha(t)$ and is, in essence, a refinement of the Golod-Shafarevich criterion. For instance, it has long been conjectured that the imaginary quadratic field $k$ of discriminant $-5460 = -4 \cdot 3 \cdot 5 \cdot 7 \cdot 13$ whose class group has exponent 2 and rank 4 has an infinite unramified 2-class field tower. It is easy to see that this field satisfies the hypothesis of problem 6.2, a positive answer to which would then yield $\alpha(0) \leq \sqrt{5460} < 74$.

## References

[1] W. Aitken and F. Hajir, *Some asymptotically good towers of function fields*, in preparation.

[2] B. Angles and C. Maire, *A note on tamely ramified towers of global functions fields,* Preprint 1999.

[3] V. G. Drinfeld and S. G. Vladut, *Number of points of an algebraic curve,* Funct. Anal. **17** (1983), 53–54.

[4] N. Elkies, *Explicit Modular Towers*, Proceedings of the Thirty-Fifth Annual Allerton Conference on Communication, Control and Computing (1997, T. Basar and A. Vardy, eds), Univ. of Illinois at Urbana-Champaign 1998, pp. 23–32.

[5] N. Elkies, A. Kresch, B. Poonen, J. Wetherell and M. Zieve, *Curves of every genus with many points II: asymptotically good families*, in preparation.

[6] G. Frey, E. Kani and H. Völklein, *Curves with infinite $K$-rational geometric fundamental group* in Aspects of Galois Theory (Gainesville, FL, 1996), 85–118, London Math. Soc. Lecture Note Ser., 256, Cambridge Univ. Press, Cambridge, 1999, **46** (1994), 467–476.

[7] 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.

[8] N. L. Gordeev, *Infinitude of the number of relations in the Galois group of the maximal p-extension of a local field with restricted ramification,* Math. USSR **18** (1982), 513–524.

[9] K. Haberland, Galois cohomology of algebraic number fields, V.E.B. Deutscher Verlag der Wissenschaften 1970.

[10] F. Hajir and C. Maire, *Tamely ramified towers and discriminants bounds for number fields,* Preprint 1999.

[11] F. Hajir and C. Maire, *Tamely ramified towers and discriminants bounds for number fields II,* in preparation.

[12] F. Hajir and C. Maire, *Sur les extensions ramifiées de corps de nombres*, in preparation.

[13] D. R. Hayes, *Explicit class field theory for rational function fields*, Trans. Amer. Math. Soc. **189** (1974), 77–91.

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

[15] H. Koch, Galoissche Theorie der $p$-Erweiterungen, VFB Deutscher Verlag der Wissenschaften, Berlin 1970.

[16] T. Kondo, *Algebraic number fields with the discriminant equal to that of quadratic number field*, J. Math. Soc. Japan **47** (1995), 31–36.

[17] W. W. Li and H. Maharaj, *Coverings of curves with asymptotically many rational points*, Preprint, 1999.

[18] J. Martinet, *Tours de corps de classes et estimations de discriminants,* Invent. Math. **44** (1978), 65–73.

[19] H. Niederreiter and C. Xing, *Towers of global function fields with asymptotically many rational places and an improvement on the Gilbert-Varshamov bound,* Math. Nach **195** (1998), 171–186.

[20] H. Niederreiter and C. Xing, *A counterexample to Perret's conjecture on infinite class field towers for global function fields,* Finite Fields Appl. **5** (1999), 240–245.

[21] H. Niederreiter and C. Xing, *Curve sequences with asymptotically many rational points* in Applications of Curves Over Finite Fields (ed. M. Fried) Contemp. Math. vol. 245, American Math. Soc., 1999.

[22] A. M. Odlyzko, *Lower bounds for discriminants of number fields II*, Tokoku Math. J. **29** (1977), 209–216.

[23] A. M. Odlyzko, *Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: a survey of recent results*, Sém. de Théorie des Nombres, Bordeaux **2** (1990), 119–141.

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

[25] G. Poitou, *Minorations de discriminants (d'aprés A. M. Odlyzko)*, Séminaire Bourbaki, Vol. 1975/76, 28ème année, Exp. No. 479, pp. 136–153, Lecture Notes in Math. 567, Springer 1977.

[26] P. Roquette, On Class field towers, in Algebraic Number Theory, ed. J. Cassels, A. Fröhlich, Academic Press 1980.

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

[28] R. Schoof, *Infinite class field towers of quadratics fields*, J. Reine Angew. Math. **372** (1986), 209–220.

[29] J.-P. Serre, Corps locaux, Hermann, Paris, 1962.

[30] J.-P. Serre, *Minorations de discriminants*, note of October 1975, published on pp. 240–243 in vol. 3 of Jean-Pierre Serre, Collected Papers, Springer 1986.

[31] J.-P. Serre, *Rational Points on Curves Over Finite Fields*, Harvard Course Notes by F. Gouvea (unpublished), 1985.

[32] H. M. Stark, *Some effetive cases of the Brauer-Siegel theorem*, Invent. Math. **23** (1974), 135–152.

[33] A. Temkine, *Hilbert class field towers of function fields over finite fields and lower bounds for $A(q)$*, Preprint 1999.

[34] M. A. Tsfasman and S. G. Vladut, Asymptotic properties of global fields and generalized Brauer-Siegel Theorem, Prétirage 98–35, Institut Mathématiques de Luminy, 1998.

[35] M. A. Tsfasman, S. G. Vladut and T. Zink, Modular curves, *Shimura curves and Goppa codes better than the Varshamov-Gilbert bound,* Math. Nach. **109** (1982), 21–28.

[36] K. Wingberg, *Galois groups of local and global type,* J. reine angew. Math. **517** (1999), 223–239.

Farshid Hajir
Department of Mathematics,
California State University, San Marcos,
San Marcos CA 92096, U.S.A.
*E-mail address*: `fhajir@csusm.edu`

Christian Maire
Department A2X,
University of Bordeaux I,
351, cours de la Libération,
33400 Talence, France
*E-mail address*: `maire@math.u-bordeaux.fr`