The Golod Safarevic Theorem and Applications

Thomas Grubb

December 14, 2018

1 Introduction

Given a algebraic number field k, the *Hilbert class field* of k is the maximal abelian extension of k which is unramified everywhere. The existence and uniqueness of the Hilbert class field was proven by Furtwängler in 1906, whose work solved a conjecture of Hilbert regarding the splitting of principle prime ideals in the ring of integers of k, $\mathcal{O}_k$. Further, the extension H_k/k is Galois, and via class field theory we have a canonical isomorphism of $Gal(H_k/k)$ with the class group C_k of k.

Furtwängler's work in this area lead him to question whether successively taking Hilbert class fields could ever result in an infinite chain of extensions of k. Specifically, if we define k_1 to be the Hilbert class field of k and k_i the Hilbert class field of k_{i-1}, does

$$k \subset k_1 \subset k_2 \subset \dots$$

always terminate? One can easily see that the above chain or "class tower" terminates if and only if k can be embedded into a finite extension L for which $\mathcal{O}_L$ is a PID. This question gained interest throughout the early 1900's, until it was answered in 1964 by Golod and Safarevic in the negative [3].

Specifically, Golod and Safarevic produced a group theoretic result which allows one to bound the number of relations in terms of the number of generators in a finite p group which is proven via group cohomology. In this paper we will present a short introduction to the cohomology of profinite groups and then discuss the theorem of Golod Safarevic. For this we will follow closely the exposition of Serre [16] and Neukirch, Schmidt, and Wingberg [9]. After establishing this result we will explore connections to class field towers and survey various directions of work in this area.

2 Cohomology of Profinite Groups

In this section we will give a brief introduction to profinite groups and their cohomology to establish the tools and notation required for the Golod Safarevic theorem. A topological group G is *profinite* if it arises as the projective limit of finite groups, each given the discrete topology. Such a group is compact

and totally disconnected; conversely, and compact totally disconnected group is profinite. A profinite group G is *pro-p* if it arises as the projective limit of p groups.

Given a profinite group G, we let C_G denote the abelian category of abelian groups on which G acts continuously; objects in C_G will be called *discrete G modules*.

To define cohomology for G with coefficients in a discrete G module A, we need a cochain complex. This arises in the same fashion as it does for finite group cohomology so long as we remember we are now working with topological groups. Indeed we define $C^n(G, A)$ to be the set of all *continuous* maps $G^n \to A$ and the coboundary map $d : C^n(G, A) \to C^{n+1}(G, A)$ by

$$\begin{aligned} df(g_1, \ldots, g_n, g_{n+1}) =& g_1 f(g_1, \ldots, g_n, g_{n+1}) \\ &+ \sum_{i=1}^{n} (-1)^i f(g_1, \ldots, g_i g_{i+1}, \ldots, g_{n+1}) \\ &+ (-1)^{n+1} f(g_1, \ldots, g_n). \end{aligned}$$

Taking cohomology of the above cochain complex gives the desired cohomology groups $H^q(G, A)$.

In practice we frequently reduce statements on the cohomology of profinite groups to the easier to manage cohomology of finite groups.

Proposition 2.1. *Let (G_i) be a projective system of profinite groups, and (A_i) an inductive system of discrete G_i modules (with the obvious requirement that the two systems be consistent with one another and the actions of G_i on A_i). Then if $G = \varprojlim G_i$ and $A = \varinjlim A_i$, we have for all $q \geq 0$*

$$H^q(G, A) = \varinjlim H^q(G_i, A_i).$$

Proof. There is a canonical map on cochains

$$\varinjlim C^*(G_i, A_i) \to C^*(G, A)$$

which is an isomorphism, and hence passes to an isomorphism on cohomology. □

Thus if we are given a profinite group G and a discrete G module A, we may compute $H^q(G, A)$ via the following corollary, where A^U denotes the fixed set of the subgroup U.

Corollary 2.2. *Let A be a discrete G module. Then for $q \geq 0$,*

$$H^q(G, A) = \varinjlim H^q(G/U, A^U),$$

where the limit is taken over all open normal subgroups $U \subset G$. □

Further corollaries that derive from their counterparts in the finite setting include the facts that $H^q(G, A)$ are torsion and that $H^q(G, A) = 0$ if $q \geq 1$ and A is injective.

For the eventual proof of the Golod Safarevic inequality we will need one final equivalent characterization of group cohomology with coefficients in $\mathbb{Z}/p\mathbb{Z}$. Given a profinite group G, let $\mathbb{F}_p[G]$ denote its group ring. Then we have

Theorem 2.3. *For $i \geq 0$,*

$$Ext_i^{\mathbb{F}_p[G]}(\mathbb{F}_p, \mathbb{F}_p) \cong H^i(G, \mathbb{Z}/p\mathbb{Z}).$$

□

We now move to defining cohomological dimension. Cohomological dimension arises in various areas and in some sense determines the "complexity" needed to write down certain projective resolutions . We will see later that for pro p groups cohomology with coefficients in $\mathbb{Z}/p\mathbb{Z}$ determines (among other things) the dimension entirely.

Given a prime number p and a profinite group G, we call the *p-cohomological dimension* of G, $cd_p(G)$, to be the smallest such n such that $H^q(G, A)$ has no p torsion for $q > n$ and for A a torsion G module. We admit the possibility that $n = \infty$, and further define the *cohomological dimension* of G to be

$$cd(G) = \sup_p cd_p(G).$$

We have the following equivalent characterizations of cohomological dimension.

Proposition 2.4. *Let G be a profinite group, p a prime number, and n a positive integer. The following are equivalent.*

- $cd_p(G) \leq n$
- *For any discrete G module A which is a p-primary torsion group, then $H^q(G, A) = 0$ for $q > n$.*
- $H^{n+1}(G, A) = 0$ *when A is a simple discrete G module killed by p.*

Proof. We will show the equivalence of the first two statements, and leave out the third for now. For any discrete torsion G module A, let $A(p)$ denote its p-primary torsion subgroup. The short exact sequence

$$0 \to A(p) \to A \to A/A(p) \to 0$$

gives a long exact sequence in cohomology

$$\cdots \to H^{i-1}(G, A/A(p)) \to H^i(G, A(p)) \to H^i(G, A) \to H^i(G, A/A(p)) \to \dots$$

Tensoring with $\mathbb{Z}_p$ picks out the p-primary torsion of the above groups and maintains exactness; as $A/A(p)$ has no p torsion and $A(p)$ is a p group we obtain

$$H^i(G, A(p)) \cong H^i(G, A)(p),$$

i.e. the p primary part of $H^i(G, A)$ is simply $H^i(G, A(p))$. The equivalence of the first two statements follows readily from this. □

Via a similar argument we obtain the following:

Proposition 2.5. *Assume $cd_p(G) \leq n$ and A is a discrete p-divisible G module. Then the p primary component of $H^q(G, A)$ is zero for $q > n$. As a corollary, if $cd(G) \leq n$ and A is a discrete divisible G module, then $H^q(G, A) = 0$ for $q > n$.* □

3 Cohomology of pro p groups

Having set up a (much too brief) framework of profinite group cohomology in the previous section, we will now specialize to the case when G is a pro p group. The main results in this section will be an interpretation of $H^1(G, \mathbb{Z}/p\mathbb{Z})$ and $H^2(G, \mathbb{Z}/p\mathbb{Z})$ in terms of the number of generators and relations inside G. This will be used in the next section to prove the Golod-Safarevic theorem and give a negative answer to the class field tower problem.

For our work on generators and relations of pro p groups, it be useful to have a notion of free pro p groups. We will define them formally, but the reader should skip the definition and just think of them as the analog of usual free groups in the pro p setting. Namely, for any natural number d we get a pro p group $F(d)$ of cohomological dimension 1 with $H^1(F(d), \mathbb{Z}/p\mathbb{Z}) = (\mathbb{Z}/p\mathbb{Z})^d$ and with the standard universal mapping property, i.e. maps $F(d) \to G$ are indexed by d elements $g_1, \ldots, g_d \in G$. Free pro p groups may also be associated to infinite sets with minor modifications, but we will focus on the finite rank case here.

Formally, if I is a set we let $L(I)$ denote the discrete free group generated by the $x_i \in I$. Take X to be the family of normal subgroups N of $L(I)$ for which almost all of the x_i are contained in N and for which $L(I)/N$ is a finite p group. Then we set

$$F(I) = \varprojlim_{N \in X} L(I)/N.$$

Our first actua lresult of this section will provide a refinement of Proposition 2.4 when G is a pro p group. For this we need a lemma.

Lemma 3.1. *Let G be a pro p group and A a nonzero simple discrete G module killed by p. Then $A \cong \mathbb{Z}/p\mathbb{Z}$, and the action of G on A is trivial.*

Proof. As G is compact and A is discrete, the orbit $\{ga : g \in G\}$ is finite for any a in A. If we choose a nonzero $a \in A$ and let $a_1, \ldots, a_k$ denote the elements in the orbit of A, then the submodule spanned by $a_1, \ldots, a_k$ is finite, nonzero, and stable under the G action. By simplicity of A, the a_i must generate A and hence A is finite.

Now the action of G on A is continuous, so the stabilizer of any a in A is open. As A is finite, we have

$$Stab(A) = \cap_{a \in A} Stab(a)$$

open in G; hence we may reduce to the action of $G/Stab(A)$ on A. In this setting we are examining the action of a finite p group on a simple module killed by p, from which the result follows by classical finite group theory. □

Combining this calculation with Proposition 2.4 gives the following.

Proposition 3.2. *Let G be a pro p group. Then $cd(G) \leq n$ if and only if $H^{n+1}(G, \mathbb{Z}/p\mathbb{Z}) = 0$.* □

We can see from this that, for a pro p group G, cohomology with coefficients in $\mathbb{Z}/p\mathbb{Z}$ encapsulates much of the cohomology theory for G. We will use this to our advantage for the remainder of the section, and as such we will use

$$H^i(G) = H^i(G, \mathbb{Z}/p\mathbb{Z})$$

for shorthand. The cohomology groups $H^i(G)$ are finite abelian groups killed by p, and hence we may view them as $\mathbb{F}_p$ vector spaces. By the dimension of $H^i(G)$ we mean their dimension when regarded as such spaces. Recall that the action of G on $\mathbb{Z}/p\mathbb{Z}$ is trivial, and hence we may identify

$$H^1(G) = \mathrm{Hom}(G, \mathbb{Z}/p\mathbb{Z}).$$

Given G, a set of elements $\{g_i : i \in I\}$ *generates* G if the group generated algebraically by the g_i is dense in G. With a view towards bounding the minimal number of generators of a given group G, we have the following proposition.

Proposition 3.3. *A morphism of pro p groups $f : G_1 \to G_2$ is surjective if and only if the induced map on cohomology $H^1(f) : H^1(G_2) \to H^1(G_1)$ is injective.*

Proof. Identifying $H^1(G_i)$ with $\mathrm{Hom}(G_i, \mathbb{Z}/p\mathbb{Z})$ we see that $H^1(f)$ is merely precomposition by f. Thus the forward implication is clear. The reverse implication follows by an argument akin to extension of characters. □

We can reformulate this using Pontryagin duality. Given G_1, G_2 as above, let G_i^* denote their Frattini subgroups. One can show that $G_i^* = G_i^p \cdot \overline{[G_i, G_i]}$; in particular, we have Pontryagin duality

$$H^1(G_i) = \mathrm{Hom}(G_i/G_i^*, \mathbb{Q}/\mathbb{Z}).$$

This leads to the dual statement of the preceding proposition.

Proposition 3.4. *Let $f : G_1 \to G_2$ be a morphism of pro p groups. Then f is surjective if and only if the induced map $G_1/G_1^* \to G_2/G_2^*$ is surjective.* □

We can now relate the dimension of $H^1(G)$ to the size of a minimal generating set for G.

Theorem 3.5. *Let $\{g_i : i \in I\}$ be a set of elements in G. Then the g_i generate G if and only if the residues $\overline{g_i}$ generate G/G^*. If the g_i generate G, then $|I| \geq \dim H^1(G)$.*

Proof. This follows easily from the previous two propositions. Let H be the subgroup of G generated by $\{g_i : i \in I\}$. Then the inclusion $H \hookrightarrow G$ is surjective if and only if the induced map $H/H^* \to G/G^*$ is surjective, showing the first statement.

For the bound on the size of the generating set, note that giving a generating set $\{g_i : i \in I\} \subset G$ gives a morphism from the free pro p group $F(I) \to G$. If this map is surjective then we get an injection

$$H^1(G) \to H^1(F(I)) \cong (\mathbb{Z}/p\mathbb{Z})^I$$

and hence $\dim(H^1(G)) \leq |I|$. □

In particular, one may conclude that the size of a minimal generating set of G is equal to $\dim H^1(G)$. We call this the *rank* of G, and denote it $d(G)$.

Next we move to the relation rank of G, leaving several details out as they are similar to the previous case. If F is a free pro p group and $R \triangleleft F$ is normal, we say a set $\mathcal{R}$ generates R if R is the smallest *normal* subgroup containing $\mathcal{R}$. Note that $H^1(R) = \mathrm{Hom}(R/R^*, \mathbb{Z}/p\mathbb{Z})$ admits an action of F/R, since F/R acts on R/R^* by inner automorphisms. With some additional effort one can use this fact to obtain

Proposition 3.6. *Let $\mathcal{R}$ be a minimal generating set for $R \triangleleft F$. Then*

$$\dim H^1(R)^{F/R} = |\mathcal{R}|.$$

□

Note that the group $H^1(R)^{F/R}$ is begging for a spectral sequence to be used with it. We will achieve this as follows. Let G be a pro p group of rank d, allowing us to write a short exact sequence

$$1 \to R \to F(d) \to G \to 1.$$

The spectral sequence for group cohomology gives us a five term exact sequence

$$0 \to H^1(G) \to H^1(F(d)) \to H^1(R)^G \to H^2(G) \to H^2(F(d)).$$

But free pro p groups have cohomological dimension 1, and hence

$$0 \to H^1(G) \to H^1(F(d)) \to H^1(R)^G \to H^2(G) \to 0.$$

By taking dimensions over $\mathbb{F}_p$ and recalling that d is the rank of G, we have proven

Theorem 3.7. *If G is a rank d pro p group with presentation $1 \to R \to F(d) \to G \to 1$, then*

$$\dim H^2(G) = \dim H^1(R)^G.$$

In particular, the minimal number of relations needed in a presentation of G is given by $\dim H^2(G)$. □

In this context we will call $r(G) = \dim H^2(G)$ the *relation rank* of G.

4 The Golod Safarevic Inequality

We have finally developed enough machinery to give an account of the Golod Safarevic inequality. Since the original proof of the inequality in [3], there have been various refinements and alternative proofs. We will follow the proof of Serre [16].

Theorem 4.1. *Let G be a finite non trivial p group. Then $r(G) > d(G)^2/4$.*

The above theorem will follow from a more general result on local algebras. Suppose R is a finite dimensional algebra over a field k, with $I \subset R$ a two sided ideal. Assume that $R = k \oplus I$ and that I is nilpotent, so that R is a local ring.

If now P is a finitely generated left R module, the groups $\operatorname{Tor}_i(P, k)$ are finite dimensional vector spaces over k. We set $t_i(P) = \dim_k \operatorname{Tor}_i(P, k)$. If we specialize to $R = k$, running through the calculations allows one to show

$$\begin{aligned} t_0(k) &= 1, \\ t_1(k) &= \dim_k I/I^2 \\ t_2(k) &= \dim_k \operatorname{Tor}_1^R(I, k). \end{aligned}$$

The main theorem we will show is as follows.

Theorem 4.2. *If $I \neq 0$, then $t_2(k) > t_1(k)^2/4$.*

Assuming Theorem 4.2 for the moment, let us prove the Golod Safarevic inequality.

Proof. If G is a finite p group let $k = \mathbb{F}_p$ and let R denote the group ring $\mathbb{F}_p[G]$, with maximal ideal I the augmentation ideal of R. One can show via induction on $|G|$ that I is nilpotent, and hence we may apply Theorem 4.2 in this setting. We thus have

$$\dim_{\mathbb{F}_p} \operatorname{Tor}_2^{\mathbb{F}_p[G]}(\mathbb{F}_p, \mathbb{F}_p) > \left(\dim_{\mathbb{F}_p} \operatorname{Tor}_1^{\mathbb{F}_p[G]}(\mathbb{F}_p, \mathbb{F}_p)\right)^2 /4.$$

Now as $\mathbb{F}_p$ is a field, the groups $\operatorname{Tor}_i^{\mathbb{F}_p[G]}(\mathbb{F}_p, \mathbb{F}_p)$ and $\operatorname{Ext}_i^{\mathbb{F}_p[G]}(\mathbb{F}_p, \mathbb{F}_p)$ are dual to one another. In particular, $\dim_i \operatorname{Tor}_i^{\mathbb{F}_p[G]}(\mathbb{F}_p, \mathbb{F}_p) = \dim_i \operatorname{Ext}_i^{\mathbb{F}_p[G]}(\mathbb{F}_p, \mathbb{F}_p)$. But now $\operatorname{Ext}_i^{\mathbb{F}_p[G]}(\mathbb{F}_p, \mathbb{F}_p) = H^i(G, \mathbb{Z}/p\mathbb{Z})$! Unraveling these inequalities gives

$$\dim_{\mathbb{F}_p} H^2(G, \mathbb{Z}/p\mathbb{Z}) > (\dim_{\mathbb{F}_p} H^1(G, \mathbb{Z}/p\mathbb{Z}))^2/4,$$

and applying the relationship between cohomology, generators, and relations of G gives the desired result. □

It thus remains to prove Theorem 4.2. It relies on the beautifully simple observation that $d^2 - 4r$ is the discriminant of the quadratic polynomial $x^2 - dx + r$, and that $r > d^2/4$ is equivalent to this polynomial having no real roots.

Proof. Keeping the notation as above, let $d = t_1(k)$ and $r = t_2(k)$. The hypothesis $I \neq 0$ ensures that

$$d = \dim_k I/I^2 > 0.$$

Now Nakayama's Lemma implies that a basis of I/I^2 lifts to a basis of I. Thus we have a surjection

$$0 \to J \to R^d \to I \to 0$$

with $J \subset I \cdot R^d$. The previous sequence gives a long exact sequence of Tor groups, showing $r = t_1(I) = t_0(J)$. By a similar argument as above we may write J as a quotient of R^r, and hence we have the start of a (minimal) free resolution of I

$$R^r \xrightarrow{\epsilon} R^d \to I \to 0,$$

with the image of ϵ equal to J.

Tensoring with $(R/I)^n$, we have

$$(R/I)^r \to (R/I)^d \to I/I^{n+1} \to 0.$$

But $J \subset I \cdot R^d$, so that ϵ factors through $(R/I^{n-1})^r$, showing that in fact we have a sequence

$$(R/I^{n-1})^r \to (R/I^n)^d \to I/I^{n+1} \to 0.$$

By taking dimensions over k, we obtain for any $n \geq 1$

$$d \cdot \dim_k R/I^n \leq (r \cdot \dim_k R/I^{n-1} + \dim_k I/I^{n+1}).$$

Define $a_n = \dim_k R/I^n$. Note that I is nilpotent, so a_n is eventually constant. Using the fact that $R = k \oplus I$, we obtain $\dim_k I/I^{n+1} = a_{n+1} - 1$. Thus we have an eventually constant sequence of numbers (a_n) satisfying

$$da_n \leq ra_{n-1} + a_{n+1} - 1.$$

The first consequence is that $r \geq 1$. Indeed if $r = 0$, we have

$$da_n \leq a_{n+1} - 1,$$

contradicting the fact that a_n is eventually constant.

Now assume $d^2 - 4r^2 \geq 0$, so that $x^2 - dx + r$ factors as

$$(x - \lambda)(x - \mu)$$

with λ, μ positive real numbers with $\lambda \leq \mu$.

To finish, let us set $A_n = a_n - \lambda a_{n-1}$. We have

$$\begin{aligned} A_{n+1} - \mu A_n &= a_{n+1} - (\lambda + \mu)a_n + \lambda\mu a_{n-1} \\ &= a_{n+1} - da_n + ra_{n-1}. \end{aligned}$$

Thus we conclude

$$A_{n+1} - \mu A_n \geq 1.$$

Finally, since $a_0 = 0, a_1 = 1$, and $a_2 = d + 1$, we get $A_0 = 0, A_1 = 1$, and $A_2 = 1 + \mu$, which gives via induction

$$A_n \geq 1 + \mu + \cdots + \mu^{n-1}.$$

This is absurd, since $\mu\lambda = r$, $r \geq 1$, and $\mu \geq \lambda$ implies $\mu \geq 1$ and hence A_n is unbounded. But a_n is eventually constant, so A_n must be as well. □

5 Applying the Golod Safarevic Inequality in Characteristic Zero

In this section we will apply the Golod Safarevic inequality to show that there are fields with infinite Hilbert towers. We will start in the characteristic zero setting and then discuss the function field setting. Throughout the remainder of the paper we will maintain the notion that G is a (possibly finite) pro p group of rank $d = d(G)$ and relator rank $r = r(G)$.

The result in the number field setting relies on the following result of Iwasawa. The proof relies on class field theory and will be left out.

Proposition 5.1. *Let K be a Galois p extension of a number field k with Galois group G. Assume K has no unramified cyclic extension of degree p, and let r_1, r_2 denote the number of real and complex embeddings of k. Then*

$$r(G) - d(G) \leq r_1 + r_2.$$

□

For a given number field k it will be useful to look at the Hilbert class tower one prime at a time. That is to say, given k we let H_k^p denote it's Hilbert p class field, the maximal abelian unramified p extension of k. It is a Galois extension of k whose Galois group is canonically identified with the p primary part of the class group of k. Iterating this process again yields a "p class tower" for k,

$$k \subset k_1 \subset k_2 \subset \ldots$$

Now if a number field k has an infinite p class tower it will also have an infinite class tower, and hence we can focus on p class towers. This is fortuitous, since all of the work leading to this has relied on our groups being pro p.

Theorem 5.2. *For each p there exists a number field k and an infinite unramified Galois extension L/k whose Galois group is pro p. In particular for any p there are fields with infinite p class towers.*

Proof. Let k be a number field, and K the largest unramified extension of k whose Galois group G is pro p. If G is finite, then we are in the situation of Proposition 5.1, and hence we have

$$r(G) - d(G) \leq r_1 + r_2.$$

Using the Golod Safarevic inequality we conclude that

$$\frac{d^2(G)-4d(G)}{4} \leq r_1 + r_2.$$

Now K certainly contains the p Hilbert class field of k. If we let C_p denote the p primary part of the class group of k, it follows that C_p is a quotient of G and hence $d(G) \geq d(C_p)$. Thus assuming K is finite over k we will reach a contradiction if the class group of k has large p rank relative to the degree of k over $\mathbb{Q}$. Indeed for any p we can find such a field k; we will construct an example for $p = 2$. Let

$$k = \mathbb{Q}(\sqrt{-p_1p_2p_3p_4p_5p_6})$$

for 6 distinct primes $p_i \geq 3$. Then k will have no totally real embeddings and a unique complex embedding up to conjugation, so we have $r_1 = 0$ and $r_2 = 1$. The extensions $\mathbb{Q}(\sqrt{-p_i})/k$ are independent, abelian, and of degree 2 for each i, so that the class group of k has 2 rank at least $6 - 1 = 5$ (with equalitiy depending on congruences mod 4). Since

$$\frac{5^2 - 4 \cdot 5}{4} = \frac{5}{4} > 1 = r_1 + r_2$$

we see immediately that k has an infinite 2 class tower. □

Having constructed this family of fields with infinite class towers, one is lead to try and classify exactly which number fields have an infinite class tower. Currently this question is wildly out of reach, and to give such a classification would require major advances in nonabelian class field theory.

An interesting tool that appears in the study of class towers arises by examining the root discriminant of a field. If k is a number field of degree n over $\mathbb{Q}$, we let denote the *root discriminant* rd_k by

$$rd_k = |d_k|^{1/n},$$

where d_k is the usual discriminant of k. Minkowski's geometry of numbers allows one to show that there are only finitely many number fields with discriminant bounded by any positive real number. However, it was unknown for some time if the same was true with the root discriminant. In fact if this was true, infinite class towers would be impossible! It is an easy calculation to show that the root discriminant is preserved under unramified extensions of number fields, and hence any field with an infinite class tower gives rise to an infinite family of fields with constant root discriminant.

This simple realization has led to a large amount of interplay between examining root discriminants and class towers. Let

$$R = \liminf_{k/\mathbb{Q}} rd_k$$

denote the limit infimum of the root discriminants for all number fields, ordered by degree. Then by the preceding remark, if a given number field k has root

discriminant less than R we know that its class tower *must* be finite. On the flip side, if we are given a number field k with an infinite class tower, we may immediately conclude $R \leq rd_k$.

Several attempts at bounding R were made utilizing the geometry of numbers. Minkowski himself produced such a bound shortly after his work on the usual discriminant of a field [7], and later Rogers [14] and Mulhollen [8] gave improved bounds using similar methodology. The first breakthrough came in a series of three papers from Odlyzko [11], [12], [13], who used Stark's relation of d_k to the zeroes of the the zeta function of k to produce improved bounds such as

$$R \geq 60^{r_1/n} 22^{2r_2/n} + o(1)$$

as $n \to \infty$. In particular Odlyzko notes that this implies that fields such as $\mathbb{Q}[\sqrt{-3 \cdot 5 \cdot 7}]$ have finite class towers.

In [6], Martinet focused on the flip side by showing that certain explicit fields have finite class towers. Inspired by Odlyzko's bounds, Martinet raised the question of determining the smallest value t for which a quadratic imaginary field with class group having 2-rank t must have an infinite class tower. Combining the Golod Safarevic inequality with the example $\mathbb{Q}[\sqrt{-3 \cdot 5 \cdot 7}]$ we see immediately that $t = 4$ or $t = 5$, with Martinet conjecturing that the correct answer was $t = 4$.

Since this conjecture there has been much work on examining the class towers of quadratic imaginary fields, but no conclusive answer has been found. Building on work of Martinet, Hajnir has shown that if Cl_k contains a copy of $(\mathbb{Z}/4\mathbb{Z})^3$ then k has an infinite class tower, which has led some to believe that $t = 4$ is the correct answer [4]. However, recent work of Boston and Wang [1] has led them to guess that in fact $t = 5$. Focusing on $\mathbb{Q}[\sqrt{-4 \cdot 3 \cdot 5 \cdot 7 \cdot 13}]$, they show that Cl_k has exactly 4 generators and 5 relations and using machinery in pro p group theory and computer algebra they are led to conjecture that the class tower of k is "finite (but very large)."

In fact the importance of examining $\mathbb{Q}[\sqrt{-4 \cdot 3 \cdot 5 \cdot 7 \cdot 13}]$ was raised in the original papers of Odlyzko! If it turns out that it's class tower is finite, it will disprove the conjecture of Martinet. If it has an infinite class tower, then it will provide a significant lowering of our best known upper bound on R. For consideration, the best known current bounds on R are

$$4\pi e^{\gamma} \approx 22.38 \leq R \leq 82.2,$$

the lower bound coming from contributions of O'Brien to p group theory in [10] and the upper bound coming from an explicit (but ugly) number field with an infinite tamely ramified 2 tower found by Hajir and Maire in [5]. It should be noted that under the Generalized Riemann Hypothesis, Serre [17] has used the explicit formulas of Weil to give a short proof of

$$8\pi e^{\gamma} \approx 44.76 \leq R,$$

and if Martinet's conjecture is true and $\mathbb{Q}[\sqrt{-4 \cdot 3 \cdot 5 \cdot 7 \cdot 13}]$ does indeed have

an infinite 2 class tower, we will have

$$R \leq \sqrt{5460} \approx 73.89.$$

6 Applications in Characteristic p

We will now provide an analogous application of the Golod Safarevic inequality in the function field setting. To provide context in this setting we first recall a theorem of Weil. Let $\mathbb{F}_q$ denote the finite field of q elements, and let X be a smooth absolutely irreducible projective curve of genus g over $\mathbb{F}_q$. Then Weil has shown the number of $\mathbb{F}_q$ rational points on X satisfies

$$|\#X(\mathbb{F}_q) - (q+1)| \leq 2g\sqrt{q}.$$

If one fixes q and allows the genus to grow to infinity, we get an asymptotic bound

$$\#X(\mathbb{F}_q) \leq 2g\sqrt{q} + o(1),$$

and hence the question was raised of finding

$$A(q) = \limsup_X \frac{\#X(\mathbb{F}_q)}{g_X},$$

where the limit is taken over smooth absolutely irreducible projective curves over $\mathbb{F}_q$ with genus tending to infinity.

It turns out that Weil's bound is not tight; in fact work of Drinfeld and Vladut has shown

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

which is in fact sharp when $q = p^2$ [2].

In general good lower bounds for $A(q)$ are unknown. Independently Serre [18] and Schoof [15] introduced class towers as a tool for bounding $A(q)$ from below. We will follow the exposition of Schoof, whose inspiration for working on the $q = 2$ case came from studying binary error correcting codes.

Recall that there is a natural correspondence between algebraic curves X over $\mathbb{F}_q$ and finite extensions of the function field $\mathbb{F}_q(t)$, given by sending a curve X to the field of rational functions on X. Given such a curve X we will denote its corresponding function field by k, and S will denote a finite set of places of k. If we fix a seperable closure $\overline{k}$ of k, we define the S Hilbert class field $H_S(k)$ of k to be the maximal abelian unramified extension of k in $\overline{k}$ in which all places of S totally split.

As in the characteristic zero setting, we can discuss class towers by setting $k_1 = H_S(k)$, letting S_1 denote the places of k_1 lying over the places of S, and iterating the process by examining the S_1 Hilbert class field of k_1. In this way we get a sequence of fields $k \subset k_1 \subset k_2 \subset \ldots$ and a corresponding tower of unramified covers of X. We say that X has an infinite S class tower when the sequence $k \subset k_1 \subset \ldots$ does not terminate.

Schoof utilizies infinite class towers to bound $A(q)$ in a manner reminiscent of the bounds on root discriminants using the following proposition.

Proposition 6.1. *Let X be a genus g curve over $\mathbb{F}_q$ and S a nonempty set of rational places of X. If X has an infinite S class field tower, then*

$$A(q) \geq \frac{\#S}{g-1}.$$

Proof. Let X_i denote the curve of genus g_i corresponding to k_i in the class field tower of k. The Hurwitz formula for unramified morphisms of curves gives

$$2g_i - 2 = [k_i : k](2g - 2).$$

Since the places in S split totally, and since S consists solely of rational places, we also have $\#X_i(\mathbb{F}_q) \geq [k_i : k] \cdot \#S$. As a result of this, we have

$$A(q) \geq \lim_{i\to\infty} \frac{\#X_i(\mathbb{F}_q)}{g_i} \geq \lim_{i\to\infty} \frac{[k_i : k]\#S}{[k_i : k](g-1)} = \frac{\#S}{g-1}$$

as desired. □

In order to actually produce such a curve with an infinite S class tower, Schoof appeals to the Golod Safarevic inequality in the same manner as Section 5. Specifically, Schoof uses the Golod Safarevic inequality to show that if the 2 rank of the S class group of k is large compared to the 2 rank of the group of S units in k, then k will admit an infinite S class tower.

With this result in hand, Schoof presents a ramified degree 8 cover X of $\mathbb{P}^1_{\mathbb{F}_2}$ with an infinite S class tower, where S is the set of places above ∞. The curve X can be written down explicitly enough to allow calculations. For instance, it is a straightforward calculation to show $\#S = 4$, and the conductor discriminant product formula allows Schoof to conclude $g_X = 19$. This example, combined with Prop 6.1, allows Schoof to conclude $A(2) \geq \frac{4}{19-1} = \frac{2}{9}$. Combined with the upper bounds of Drinfeld and Vladut, we obtain

$$\frac{2}{9} \approx .222 \leq A(2) \leq .414 \approx \sqrt{2} - 1,$$

which (to the best of my knowledge) are the best current bounds on $A(2)$.

7 Acknowledgements

Thanks to Benedict Gross, Cristian Popescu, David Stapleton, and Wei Yin for their patience and helpful comments during the writing of this paper. Thanks also to Google Translate, which allowed me to hack my way through the French articles.

8 References

1. N. Boston and J. Wang. The 2-class Tower of $\mathbb{Q}(\sqrt{-5460})$. ArXiv preprint 1710.10681.

2. V. G. Drinfeld and S. G. Vladut. The Number of Points on an Algebraic Curve. Funktsional Anal i Prilozhen 17 (1983), 68-69.

3. E. S. Golod and I. R. Safarevic. On the Class Field Tower. Izv. Akad. Nauk SSSR Ser. Mat. 28 (1964), 261-272.

4. F. Hajir. On a Theorem of Koch. Pacific J. Math. 176 (1996), no. 1, 15-18.

5. F.Hajir and C.Maire. Tamely ramified towers and discriminant bounds for number fields II., J. Symbolic Comput. 33 (2002), 415-423.

6. J. Martinet. Tours de corps de classes et estimations de discriminants. Invent. Math. 44 (1978), 65-73.

7. H. Minkowski. Theoremes Arithmetiques. C. R. Acad. Sci. Paris 112 (1891), 209-212.

8. H. P. Mulholland. On the Product of n Complex Homogenous Linear Forms. J. London Math. Soc. (1960), 241-250.

9. J. Neukirch, A. Schmidt, and K. Wingberg. Cohomology of Number Fields, Grundl. Math. Wiss., vol. 323, Springer, Berlin, 2000.

10. E.A.OBrien. The p-group generation algorithm, J. Symbolic Comput. 9 (1990), 677-698.

11. A. M. Odlyzko. Lower Bounds for Discriminants of Number Fields. Acta Arith. 29 (1976), no. 3, 275-297.

12. A. M. Odlyzko. Lower Bounds for Discriminants of Number Fields II. Tohoku Math J. 29 (1977), 209-216.

13. A. M. Odlyzko. Some ANalytic Estimates of Class Numbers and Discriminants. Invent. Math. 29 (1975), 275 - 286.

14. C. A. Rogers. The Product of n Real Homogenous Linear Forms. Acta Math. (1950), 185-208.

15. R. Schoof. Algebraic Curves over $\mathbb{F}_2$ with Many Rational Points. J. of Number Theory 41 (1992), 6-14.

16. J. P. Serre. Galois Cohomology. Lecture Notes in Mathematics 5, Springer (1964).

17. J. P. Serre. Minorations de Discriminants. OEuvres, Vol III, Springer-Verlag (1986), 240-243.

18. J. P. Serre. Sur le Nombre des Points Rationnels d'une Courbe Algebrique Sur un Corps Fini. C. R. Acad. Sci. Paris 296 (1983), 397-402.