SOLVABLE COVERS WITH MANY RATIONAL POINTS

DANNY NEFTIN AND MICHAEL E. ZIEVE

ABSTRACT. For any prime p, the existence of curves C over $\mathbb{F}_p$ for which the number of $\mathbb{F}_p$-points $\#C(\mathbb{F}_p)$ grows linearly with the genus g_C is known by a nonconstructive approach of Serre via class field towers. This has motivated the investigation of the growth of $\#C(\mathbb{F}_p)$ for various families of curves C.

Given $\ell \in \mathbb{N}$, we consider all Galois covers $C \to \mathbb{P}^1$ with a solvable Galois group of derived length at most ℓ, and show using a theorem of Frey-Perret-Stichtenoth that the growth of $\#C(\mathbb{F}_p)$ is at most $g_C/\log^{\circ\ell} g_C$, where $\log^{\circ\ell}$ is log iterated ℓ times.

The main result shows that this bound is sharp. That is, we construct covers $C \to \mathbb{P}^1$ with solvable Galois groups of any given derived length ℓ such that the growth of $\#C(\mathbb{F}_p)$ is $g_C/\log^{\circ\ell} g_C$.

1. INTRODUCTION

The growth and distribution in the number of $\mathbb{F}_q$-rational points $\#C(\mathbb{F}_q)$ on families of curves C when $q \to \infty$ is well understood in light of Deligne's equidistribution theorem. In the past few decades there has been a significant interest in the analogous problem concerning the growth of $\#C(\mathbb{F}_q)$ when q is fixed and the genus $g_C \to \infty$.

Weil's theorem gives a linear upper bound on $\#C(\mathbb{F}_q)$ in terms of g_C, for all (smooth, geometrically irreducible) curves C over $\mathbb{F}_q$:

$$\#C(\mathbb{F}_q) \le 2\sqrt{q}g_C + q + 1$$

Following bounds of Ihara [8] and Manin [11], Drinfeld and Vladut [1] improved Weil's bound asymptotically by showing that $\#C(\mathbb{F}_q) \le (\sqrt{q}-1+o(1))g_C$. That is,

$$\limsup_{g_C\to\infty} \frac{\#C(\mathbb{F}_q)}{g_C} \le \sqrt{q} - 1, \tag{1.1}$$

where the limit is taken over all curves C over $\mathbb{F}_q$.

For square q, Ihara [9] used modular curves to construct curves C over $\mathbb{F}_q$ with arbitrarily large genus for which $\#C(\mathbb{F}_q)/g_C$ is arbitrarily close to $\sqrt{q}-1$, proving that (1.1) is in fact an equality. A major problem in this area is to determine whether (1.1) is an equality for non-square q. To answer this problem affirmatively, it is in particular required to construct sequences of curves C of arbitrarily large genus with *linear growth*, i.e. curves C for which $\#C(\mathbb{F}_q)/g_C > \gamma_q$ for some constant $\gamma_q > 0$.

This problem has led to several other remarkable constructions of curves with linear growth: curves defined by recursive equations by Garcia-Stichtenoth [6] (cf. [7]); curves obtained using rigidity methods and an analysis of their Jacobians, by Frey-Kani-Völklein [3] (cf. [2]); certain degenerate Shimura curves over cubic fields, by Zink [19]. However, for prime q the only known sequences of curves with

linear growth arise from a nonconstructive approach to class field towers via the Golod-Shafarevich inequality[1]; An approach which was first taken by Serre [17] and subsequently followed by many authors, see [15].

It is therefore desirable to understand the growth of $\#C(\mathbb{F}_q)$ with g_C for families of curves C over $\mathbb{F}_q$, for an arbitrary fixed prime power q. Frey-Perret-Stichtenoth [4] (cf. [10, Theorem 1]) showed that there is a positive constant $a_q > 0$ such that for every abelian cover $C \to \mathbb{P}^1$ over $\mathbb{F}_q$ with $g_C > 0$:

$$\#C(\mathbb{F}_q) < a_q \frac{g_C}{\log g_C},$$

where log, unless otherwise mentioned, is with respect to the natural base.

In fact, by Kresch-Wetherell-Zieve [10] this is precisely the growth for abelian covers. That is, there is a constant b_q and abelian covers $C \to \mathbb{P}^1$ over $\mathbb{F}_q$ of arbitrary positive genus such that:

$$\#C(\mathbb{F}_q) > b_q \frac{g_C}{\log g_C}.$$

In this paper we consider the growth of $\#C(\mathbb{F}_q)$ for solvable covers $C \to \mathbb{P}^1$ over $\mathbb{F}_q$ when the derived length is bounded. More generally we fix a (smooth, geometrically irreducible) curve D over $\mathbb{F}_q$ with an $\mathbb{F}_q$-rational point and consider (smooth, geometrically irreducible) covers $C \to D$ defined over $\mathbb{F}_q$. A cover $C \to D$ is *of (derived) length* ℓ if $C \to D$ is Galois with solvable Galois group of derived length ℓ. We use [4] to obtain the following upper bound:

Theorem 1.1. *For every $\ell \in \mathbb{N}$ and a curve D over $\mathbb{F}_q$, there is a constant $c_{D,\ell}$ such that for every length ℓ cover $C \to D$:*

$$\#C(\mathbb{F}_q) < c_{D,\ell} \frac{g_C}{\log^{\circ \ell} g_C},$$

where $\log^{\circ \ell}$ denotes the ℓ-th iterate of log.

The main result of this paper is a construction which shows that $g_C/\log^{\circ \ell} g_C$ is precisely the growth for covers of length ℓ:

Theorem 1.2. *For every integer $\ell > 0$ and curve D over a perfect field k of positive characteristic, there exists a constant $d_{D,\ell} > 0$ and length ℓ covers $C \to D$ with arbitrarily large genus g_C such that:*

$$\#C(k) > d_{D,\ell} \frac{g_C}{\log^{\circ \ell} g_C}.$$

Furthermore, the covers $C \to D$ can be chosen to be Galois with Galois group which is a (standard) iterated wreath product of abelian groups.

We note that Theorem 1.2 applies to curves D over any perfect field k of positive characteristic and in particular over any prime field. The case $\ell = 1$ and $D = \mathbb{P}^1$ gives the result for abelian covers $C \to \mathbb{P}^1$.

The covers $C = C_\ell$ are constructed from length $\ell - 1$ Galois covers $C_{\ell-1} \to D$. Letting G be the Galois group of $C_{\ell-1} \to D$, C_ℓ is constructed as a fiber product of a (cyclic) Artin-Schreier cover $\tilde{C} \to C_{\ell-1}$ with its conjugates $\tilde{C}^\sigma \to C_{\ell-1}, \sigma \in G \setminus \{1\}$. The key ingredient is allowing enough ramification in a G-invariant set

[1][2, Remark 5.4] shows that the construction in [3] does not give the desired result for prime q.

S of points of $C_{\ell-1}$ to construct the cover $\tilde{C} \to C_{\ell-1}$ using Riemann-Roch, while keeping the different exponent and hence the genus of C sufficiently small, basing on the fact that the covers $\tilde{C}^\sigma \to C_{\ell-1}, \sigma \in G$, have the same branch points.

This construction leaves a considerable amount of freedom in the choice of covers $\tilde{C}$, allowing a large amount of ramification in a set of points which is unbounded as ℓ grows. We are therefore hopeful that particular choices will lead to the construction of explicit covers $C_\ell, \ell \in \mathbb{N}$, whose number of points grows linearly with the genus.

Also note that sequences of curves with many points are used in coding theory to generate efficient error correcting codes, see [15]. Curves with linear growth lead to codes that are asymptotically good. As a consequence of Theorem 1.1, the length of solvable covers is unbounded in a sequence of curves with linear growth.

2. Preliminaries on iterative logarithms

To prove Theorem 1.1, we shall need several basic facts concerning iterative logarithms which are given by the following lemmas. By writing $\log^{\circ\ell}(x)$, we implicitly assume that x is large enough for the expression to be defined. That is, for $\ell = 1$, $x > x_0 = 0$, and for all $\ell \geq 2$, $x > x_\ell := e^{x_{\ell-1}}$.

Lemma 2.1. *Assume $\ell \geq 1$. There exists $x_\ell > 0$ such that for every x, y satisfying $y > x_\ell$ and $x - y > x_\ell$, one has:*

$$\log^{\circ\ell}(x-y) > \log^{\circ\ell}(\frac{x}{y}) \geq \log^{\circ\ell} x - \log^{\circ\ell} y. \tag{2.1}$$

Proof. Set $x_1 := 2$ The first inequality is clear since $\log^{\circ\ell}$ is an increasing function and $x - y > \frac{x}{y}$ for $y > x_1$ and $x > y + x_1$. For the second inequality, we argue by induction on ℓ. For $\ell = 1$, equality holds. Let $\ell > 1$ and set x_ℓ so that $x_\ell \geq x_{\ell-1}$ and $\log^{\circ(\ell-1)} x, \log^{\circ(\ell-1)} y > x_1$, for all $y > x_\ell$ and $x > y + x_\ell$. By induction we get:

$$\begin{aligned} \log^{\circ\ell}(\tfrac{x}{y}) &> \log(\log^{\circ(\ell-1)} x - \log^{\circ(\ell-1)} y) \\ &> \log\log^{\circ(\ell-1)} x - \log\log^{\circ(\ell-1)} y = \log^{\circ\ell} x - \log^{\circ\ell} y, \end{aligned}$$

where the latter inequality follows from the first inequality in (2.1) with $\ell = 1$. □

Lemma 2.2. *Let $\ell \geq 2$ and $g(y) := \frac{\log^{\circ\ell}(\frac{y}{\log^{\circ\ell} y})}{\log^{\circ\ell} y}$. There exists a y_ℓ such that $g(y)$ is increasing and $0 < g(y) < 1$, for all $y \geq y_\ell$. Moreover, $\lim_{y\to\infty} g(y) = 1$.*

Proof. Since $\log^{\circ\ell}$ is increasing, the inequalities $0 < g(y) < 1$ hold when $\log^{\circ\ell} y > 1$. By Lemma 2.1, if $\log^{\circ\ell} y > x_\ell$ and $y > \log^{\circ\ell} y + x_\ell$, then

$$1 \geq g(y) \geq \frac{\log^{\circ\ell} y - \log^{\circ(2\ell)} y}{\log^{\circ\ell} y} = 1 - \frac{\log^{\circ(2\ell)} y}{\log^{\circ\ell} y}.$$

Thus $\lim_{y\to\infty} g(y) = 1$.

It remains to show that $g(y)$ is increasing starting from some y_ℓ. Let $h(y) = \log^{\circ\ell} y$. Then

$$g'(y) = \frac{1}{h(y)^2}(h'(\frac{y}{h(y)})(1 - y\frac{h'(y)}{h(y)}) - h'(y)h(\frac{y}{h(y)})).$$

Let $z = \frac{y}{h(y)}$. To show $g'(y) > 0$, it suffices to show

$$h(y)^2 g'(y) = h'(z)(1 - zh'(y)) - h'(y)h(z) > 0,$$

or for large enough y (and hence z)

$$\frac{h'(z)}{h(z)}\frac{(1-zh'(y))}{h'(y)} > 1. \tag{2.2}$$

Since $h'(y) = \frac{1}{\prod_{k=0}^{\ell-1}\log^{\circ k}y}$, the LHS of (2.2) equals:

$$\frac{h'(z)}{h(z)}(\frac{1}{h'(y)} - z) = \frac{\prod_{k=0}^{\ell-1}\log^{\circ k}y - z}{\prod_{k=0}^{\ell}\log^{\circ k}z} = \frac{\prod_{k=1}^{\ell}\log^{\circ k}y - 1}{\prod_{k=1}^{\ell}\log^{\circ k}z} \tag{2.3}$$

For sufficiently large y, $\log^{\circ k}y > \log^{\circ k}z + 1$ for $1 \le k \le \ell$. In particular, the RHS of (2.3) is greater than 1, as desired. □

Lemma 2.3. *Let $\ell \ge 1$. Let u and f be real valued continuous increasing functions on an interval $[x_0, \infty)$ such that $\lim_{x\to\infty} u(x) = 1$, $f(x) = u(x)x\log^{\circ\ell}x$, and x_0 is sufficiently large so that $\log^{\circ\ell}y > \log^{\circ\ell}(\frac{y}{\log^{\circ\ell}y}) > 1$ for all $y \in \mathrm{Im}f$.*

Then there exists a continuous increasing function $v : [y_\ell, \infty) \to \mathbb{R}^+, y_\ell > 0$, with $\lim_{y\to\infty} v(y) = 1$ such that for all $y \ge y_\ell$:

$$f^{-1}(y) < \frac{y}{v(y)\log^{\circ\ell}(y)}.$$

Proof. By Lemma 2.2, there exists y_ℓ for which the function $v : [y_\ell, \infty) \to \mathbb{R}$ given by

$$v(y) := \frac{\log^{\circ\ell}(\frac{y}{\log^{\circ\ell}y})}{\log^{\circ\ell}y}u(\frac{y}{\log^{\circ\ell}y}),$$

is continuous, increasing, and satisfies $0 < v(y) < 1$. Since

$$u(\frac{y}{\log^{\circ\ell}y}) < u(\frac{y}{v(y)\log^{\circ\ell}y}) \text{ and } \log^{\circ\ell}(\frac{y}{\log^{\circ\ell}y}) < \log^{\circ\ell}(\frac{y}{v(y)\log^{\circ\ell}y})$$

one has:

$$y < f(\frac{y}{v(y)\log^{\circ\ell}(y)}).$$

Since f is increasing we get the desired assertion. □

Remark 2.4. Equivalently, under the same assumptions on u and f, Lemma 2.3 asserts the existence of $x_\ell \in \mathbb{N}$ and an increasing function $v_{K,\ell}$ with limit 1, such that for every $x \ge x_\ell$:

$$x \le \frac{f(x)}{v(f(x))\log^{\circ\ell}(f(x))}.$$

Lemma 2.5. *Let $c > 0$ and assume $y < cx\log^{\circ\ell}x$ for sufficiently large x, y so that $c\log^{\circ\ell}x, \log^{\circ\ell}y > 1$. Then $y/\log^{\circ\ell}y < cx$.*

Proof. Since the function $f(y) = y/\log^{\circ\ell}y$ is increasing when $\log^{\circ\ell}y > 1$, we have:

$$\frac{y}{\log^{\circ\ell}y} < \frac{cx\log^{\circ\ell}x}{\log^{\circ\ell}(cx\log^{\circ\ell}x)} < \frac{cx\log^{\circ\ell}x}{\log^{\circ\ell}x} = cx. \quad \square$$

3. Upper bound

The number $\#C(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points in a degree d cover $C \to D$ defined over $\mathbb{F}_q$ is bounded above by $d\#D(\mathbb{F}_q)$. Therefore to bound the number of $\mathbb{F}_q$-rational points on such covers we bound their degrees.

We let K be the function field of D and let h_K denote the class number of K. In particular, K has transcendence degree 1 over $\mathbb{F}_q$ and $\mathbb{F}_q$ is algebraically closed in K. Recall that L/K is *regular* if $\mathbb{F}_q$ is algebraically closed in L. We use the following bound for regular abelian extensions of K:

Theorem 3.1. (Frey, Perret, Stichtenoth [4]) *Let L/K be a finite regular abelian extension and $n := [L : K]$. Then*

$$g_L \geq \frac{1}{4} n(\log_q n + 4(g_K - 1) - \log_q h_K).$$

As a corollary to Theorem 3.1, one has:

Corollary 3.2. *Let L/K be a regular abelian extension and n its degree. Then*

$$\frac{g_L}{n} > c_q \log n - 1,$$

where $c_q = 1/(4 \log q)$.

To derive Corollary 3.2 we use the following bound on class numbers:

Lemma 3.3. $h_K \leq (\sqrt{q} + 1)^{2g_K}$.

Proof. Let $g = g_K$ be the genus of K. The class group of K is isomorphic to the group of $\mathbb{F}_q$-rational points on the Jacobian variety J_K. The number of $\mathbb{F}_q$-rational points on J_K is:

$$\#J_K(\mathbb{F}_q) = \prod_{i=1}^{2g} (1 - a_i),$$

where $a_1, \ldots, a_{2g}$ are the roots of the characteristic polynomial of the Frobenius automorphism of J_F, see [14, Chp. 2, Theorem 1.1]. Since $|a_i| = q^{1/2}$ for $i = 1, \ldots, 2g$, we have:

$$\#J_K(\mathbb{F}_q) = \prod_{i=1}^{2g} (1 - a_i) \leq \prod_{i=1}^{2g} (\sqrt{q} + 1) = (\sqrt{q} + 1)^{2g}. \quad \square$$

Proof of Corollary 3.2. Let h_K be the class number of K and g its genus. By Lemma 3.3, $\log_q(h_K) \leq 2g \log_q(\sqrt{q} + 1)$. Since $\log_q(\sqrt{q} + 1) < 2$ for all q:

$$\log_q(h_K) < 4g.$$

It therefore follows from Theorem 3.1 that:

$$\frac{g_L}{n} > \frac{1}{4}(\log_q n - 4) = c_q \log n - 1. \tag{3.1}$$

$\square$

We use this corollary to give a lower bound on the genus in terms of the degree:

Proposition 3.4. *Let $\ell \geq 1$. There exist $n_\ell > 0$ and an increasing function $e_\ell : [n_\ell, \infty) \to [0,1]$ with limit 1 such that for every finite regular solvable extension L/K with length ℓ and degree $n := [L:K]$ at least n_ℓ, one has:*

$$\frac{g_L}{n} > c_q \log^{\circ \ell}(n) e_\ell(\log n) - 1,$$

where $c_q = 1/(4 \log q)$.

Definition 3.5. The increasing functions $e_\ell : [n_\ell, \infty) \to [0,1], n_\ell > 0, \ell \in \mathbb{N}$, with limit 1, are defined inductively as follows. Let $n_1 := 0$ and $e_1(x) = 1$ for all $x \geq 0$.

For $\ell \geq 2$, let $n_\ell > 0$ and $e_\ell : [n_\ell, \infty) \to \mathbb{R}$ be such that:

$$x < \frac{y}{e_\ell(y) \log^{\circ(\ell-1)} y},$$

for every x, y subject to $y = e_{\ell-1}(\log x) x \log^{\circ(\ell-1)} x$ and $y \geq n_\ell$. There exist such n_ℓ, and e_ℓ by Lemma 2.3.

Proof of Proposition 3.4. We argue by induction on ℓ. For $\ell = 1$, the assertion follows from Corollary 3.2.

Assume $\ell > 1$ and let M be a subfield of L such that M/K is of length $\ell - 1$ and L/M is abelian. Let $d := [M:K]$. By Corollary 3.2:

$$\frac{g_L}{n/d} > c_q \log \frac{n}{d} - 1,$$

and hence:

$$\frac{g_L}{n} > c_q \frac{\log n}{d} - \frac{c_q \log d + 1}{d} > c_q \frac{\log n}{d} - 1. \tag{3.2}$$

We assume that n_ℓ is sufficiently large so that for every $n \geq n_\ell$ and d such that $\log d \leq n_{\ell-1}$, one has $(\log n)/d \geq \log^{\circ \ell} n$. Thus, we may assume $\log d > n_{\ell-1}$.

By the Riemann-Hurwitz formula $g_L - 1 \geq \frac{n}{d}(g_M - 1)$. In particular, $\frac{g_L}{n} > \frac{g_M}{d} - 1$. By induction we have:

$$\frac{g_L}{n} > \frac{g_M}{d} - 1 \geq c_q \log^{\circ(\ell-1)}(d) e_{\ell-1}(\log d) - 1. \tag{3.3}$$

It follows from (3.2) and (3.3) that

$$\frac{g_L}{n} > \max(c_q \frac{\log n}{d} - 1, c_q \log^{\circ(\ell-1)}(d) e_{\ell-1}(\log d) - 1).$$

For a fixed n, the function $f_1(x) := c_q \frac{\log n}{x}$ decreases while $f_2(x) := c_q \log^{\circ(\ell-1)}(x) e_{\ell-1}(\log x)$ increases. We assume n_ℓ is large enough so that f_1 and f_2 intersect for $n \geq n_\ell$, and let d_{opt} be their intersection point. By definition of d_{opt}, one has $\log n = d_{\mathrm{opt}} f_2(d_{\mathrm{opt}})$, and hence by definition of e_ℓ one has:

$$d_{\mathrm{opt}} < \frac{\log n}{\log^{\circ \ell}(n) e_\ell(\log n)}.$$

We therefore have:

$$\frac{g_L}{n} > \max(f_1(d) - 1, f_2(d) - 1) \geq f_1(d_{\mathrm{opt}}) - 1 = c_q \frac{\log n}{d_{\mathrm{opt}}} - 1 > c_q \log^{\circ \ell}(n) e_\ell(\log n) - 1,$$

as required. □

We can now derive Theorem 1.1:

Proof of Theorem 1.1. Let K be the function field of D. By Proposition 3.4, there is an increasing function $\tilde{e}_{K,\ell} : [n_\ell, \infty) \to [0,1]$ such that for every regular extension L/K with length ℓ and degree $n := [L : K]$ at least n_ℓ, the genus $g := g_L$ is at least $y(n) := n\log^{\circ\ell}(n)\tilde{e}_{K,\ell}(n)$. Let $g_\ell > 0$ and $v_{K,\ell} : [g_\ell, \infty) \to \mathbb{R}$ be the increasing function with limit 1, obtained by applying Lemma 2.3 with $u := \tilde{e}_{K,\ell}$. As in Remark 2.4, there is an n'_ℓ such that:

$$n < \frac{y(n)}{v_{K,\ell}(y(n))\log^{\circ\ell}(y(n))} < \frac{g}{v_{K,\ell}(y(n))\log^{\circ\ell} g},$$

if $n \geq n'_\ell$. As $v_{K,\ell} \circ y$ is increasing, this implies that there is a constant $c_{K,\ell}$ such that for every regular extension L/K of length ℓ:

$$[L : K] < c_{K,\ell}\frac{g_L}{\log^{\circ\ell} g_L}.$$

In particular, for every regular cover $C \to D$ of length ℓ:

$$\#C(\mathbb{F}_q) \leq \#D(\mathbb{F}_q) \cdot [K(C) : K(D)] < c_{K,\ell}\#D(\mathbb{F}_q)\frac{g_C}{\log^{\circ\ell} g_C}. \quad \square$$

4. Constructing covers with large genus

Let k be a perfect field of characteristic $p > 0$ and D a curve over k with a k-rational point. We construct covers of D whose genus and degree are as in Theorem 1.2. Furthermore, letting K be the function field of D we prove:

Theorem 4.1. *Let S be a finite set of primes of K. There exists a constant $c_{S,\ell}$ and solvable extensions L/K of length ℓ and arbitrarily large genus g_L such that the primes of S split completely in L and*

$$g_L \leq c_{S,\ell} d\log^{\circ\ell}(d),$$

where $d := [L : K]$. Furthermore, L can be chosen to be Galois over K with Galois group isomorphic to a (standard) iterated wreath product of abelian groups.

Theorem 1.2 is deduced from Theorem 4.1 as follows:

Proof of Theorem 1.2. Since D has a k-rational point, K has a degree 1 prime $\mathfrak{p}$. We apply Theorem 4.1 with $S = \{\mathfrak{p}\}$ to obtain field extensions L/K of length ℓ and arbitrarily large degree d_L in which $\mathfrak{p}$ splits completely, and:

$$g_L \leq c_{K,\ell} d_L \log^{\circ\ell}(d_L).$$

By Lemma 2.5, for such fields L with sufficiently large degree and hence genus:

$$\frac{g_L}{\log^{\circ\ell} g_L} \leq c_{K,\ell} d_L. \tag{4.1}$$

The fields L for which (4.1) holds, correspond to covers $C \to D$ for which:

$$\#C(k) \geq d_L \geq \frac{1}{c_{K,\ell}}\frac{g_L}{\log^{\circ l} g_L}. \quad \square$$

To construct fields L as in Theorem 4.1, we use Artin-Schreier extensions. Let $p = \mathrm{char}(K)$ and $\wp(x) := x^p - x \in k[x]$. For an additive subgroup $\Gamma \leq K^+$, denote by $K(\wp^{-1}\Gamma)$ the Artin-Schreier extension obtained by adjoining to K the roots of $\wp(x) - \gamma$, for all $\gamma \in \Gamma$.

For a prime $\mathfrak{p}$ of K, let $v_\mathfrak{p}$ be a discrete valuation associated to $\mathfrak{p}$, normalized so that $v_\mathfrak{p}(K^\times) = \mathbb{Z}$. For $\gamma \in \Gamma$, define $m_\mathfrak{p}(\gamma) := -1$ if there exists $z \in K$ such that $v_\mathfrak{p}(\gamma - (z^p - z)) \geq 0$ and $m_\mathfrak{p}(\gamma) := m$ if m is prime to p and there exists $z \in K$ such that $v_\mathfrak{p}(\gamma - (z^p - z)) = -m < 0$. By [5, Lemma 3.7.7], such m is unique and $m_\mathfrak{p}(\gamma)$ is well defined. We shall use the following basic properties of Artin-Schreier extensions:

Lemma 4.2. *Let $\Gamma \leq K^+$ be finite and $L = K(\wp^{-1}\Gamma)$. Then*

(1) *A prime $\mathfrak{p}$ of K is unramified in L if and only if $m_\mathfrak{p}(\gamma) = -1$ for all $\gamma \in \Gamma$.*
(2) *If $v_\mathfrak{p}(\gamma) > 0$ for all $\gamma \in \Gamma \setminus \{0\}$, then $\mathfrak{p}$ splits completely in L.*
(3) *If L contains no nontrivial unramified extensions of K, the genus g_L is given by:*

$$g_L = 1 + [L : K](g_K - 1) + \frac{1}{2} \sum_{\gamma \in \Gamma, \mathfrak{p}} (m_\mathfrak{p}(\gamma) + 1) \deg \mathfrak{p}, \tag{4.2}$$

where $\mathfrak{p}$ runs through the primes of K.

Proof. For cyclic Γ, Part (1) appears in [18, Proposition 3.7.8]. The general case follows since $\mathfrak{p}$ is unramified in L/K if and only if $\mathfrak{p}$ is unramified in all cyclic subextensions $K(\wp^{-1}\gamma)/K$, $\gamma \in \Gamma$.

For cyclic $\Gamma = \langle \gamma \rangle$, Part (2) follows from Kummer's theorem [18, Theorem 3.3.7] and since the reduction mod $\mathfrak{p}$ of the polynomial $\wp(x) - \gamma$ splits. The general case follows from the cyclic since $\mathfrak{p}$ splits completely in L if and only if it splits completely in all cyclic subextensions $K(\wp^{-1}\gamma)/K$, $\gamma \in \Gamma$.

In [18, Proposition 3.7.8], the genus is described for cyclic ramified Artin-Schreier extensions $K(\wp^{-1}\gamma)/K$, $\gamma \in K$ as:

$$g_{K(\wp^{-1}\gamma)} = 1 + p(g_K - 1) + \frac{p-1}{2} \sum_{\mathfrak{p}} (m_\mathfrak{p}(\gamma) + 1) \deg \mathfrak{p}. \tag{4.3}$$

Since $m_\mathfrak{p}(\gamma) = m_\mathfrak{p}(a\gamma)$ for all $a \in \mathbb{F}_p^\times$, (4.3) gives (4.2) for $K(\wp^{-1}\gamma)/K$. Letting $L_i, 1 \leq i \leq t$, be the subfields of L of degree p over K, [5, Theorem 2.1] implies:

$$g_L = \sum_{i=1}^{t} g_{L_i} - \frac{p^n - p}{p - 1} g_K, \tag{4.4}$$

where n is the rank of Γ. Part (3) now follows by a simple calculation combining (4.2) for cyclic extensions, (4.4), and the one-to-one correspondence between $L_i, 1 \leq i \leq t$ and cyclic subgroups of Γ. □

We can now prove Theorem 4.1.

Proof of Theorem 4.1. Let $S_0 = \{\mathfrak{q}_1, \ldots, \mathfrak{q}_\ell\}$ be a set of ℓ distinct primes of K which is disjoint from S, and $\tilde{S} = S_0 \cup S$. We show that there are constants $c_{\tilde{S},r}$ and elementary abelian p-extensions L_r/L_{r-1}, $1 \leq r \leq \ell$, $L_0 = K$, with arbitrarily large degree, such that:

(Ram) The primes of $S \cup \{\mathfrak{q}_{r+1}, \ldots, \mathfrak{q}_\ell\}$ split completely in L_r, and L_r/L_{r-1} is ramified only over $\mathfrak{q}_r$, for every $1 \leq r \leq \ell$;

(Gen) The genus is bounded by $g_{L_1} < \tilde{c}_{\tilde{S},1}[L_1 : K] \log[L_1 : K]$, and by:

$$\frac{g_{L_r}}{[L_r : K]} \leq 2\frac{g_{L_{r-1}}}{[L_{r-1} : K]} + \tilde{c}_{\tilde{S},r},$$

for $2 \leq r \leq \ell$.

(Gal) The extension L_r/K is Galois with Galois group

$$G_r := \mathrm{Gal}(L_r/K) \cong (\mathbb{Z}/p\mathbb{Z}) \wr G_{r-1} = (\mathbb{Z}/p\mathbb{Z})^{|G_{r-1}|} \rtimes G_{r-1},$$

where $G_{r-1} := \mathrm{Gal}(L_{r-1}/K)$, $r = 2, \ldots, \ell$, and $\wr$ denotes the standard wreath product.

We partition the proof into four steps. In the fourth step we show that the constants $\tilde{c}_{\tilde{S},r}, 1 \leq r \leq \ell$, lead to the desired constant $c_{S,\ell}$.

Step I: Constructing extensions L_1/K with Galois group $(\mathbb{Z}/p\mathbb{Z})^n$, for any $n \geq 1$, which satisfy (Ram) and (Gen).

We claim that there is $\gamma \in K$ with a pole only at $\mathfrak{q}_1$ such that $(v_{\mathfrak{q}_1}(\gamma), p) = 1$, and $v_{\mathfrak{p}}(\gamma) > 0$ for all $\mathfrak{p} \in \tilde{S} \setminus \{\mathfrak{q}_1\}$. By the strong approximation theorem [18, Theorem 1.6.5] there is $\gamma_1 \in K$ with $v_{\mathfrak{p}}(\gamma_1) \geq 0$ for all $\mathfrak{p} \notin \tilde{S}$ and $v_{\mathfrak{p}}(\gamma_1) > 0$ for $\mathfrak{p} \in \tilde{S} \setminus \{\mathfrak{q}_1\}$. If $(v_{\mathfrak{q}_1}(\gamma_1), p) = 1$ the claim follows by setting $\gamma := \gamma_1$. Otherwise construct a $\gamma_2 \in K$ which has a pole only at $\mathfrak{q}_1$ such that $(v_{\mathfrak{q}_1}(\gamma_2), p) = 1$, as follows. Consider the Riemann-Roch spaces $L(a\mathfrak{q}_1) = \{x \in K | (x) \geq -a\mathfrak{q}_1\}$, $a \in \mathbb{N}$. Since by Riemann-Roch $L((2g_K - 1)\mathfrak{q}_1) \subsetneq L(2g_K\mathfrak{q}_1) \subsetneq L((2g_K + 1)\mathfrak{q}_1)$, there is a $\gamma_2 \in L((2g_K + 1)\mathfrak{q}_1)$ with $(v_{\mathfrak{q}_1}(\gamma_2), p) = 1$. Setting $\gamma := \gamma_1\gamma_2$ proves the claim.

Let $1 = \alpha_1 < \cdots < \alpha_n$ be the n smallest positive integers that are prime to p, $\Gamma_1 := \langle \gamma^{\alpha_1}, \ldots, \gamma^{\alpha_{i-1}} \rangle$ the additive subgroup of K^+ generated by $\gamma^{\alpha_i}, 1 \leq i \leq n$, and $L_1 := K(\wp^{-1}\Gamma_1)$ an abelian extension of K.

Set $d_{\tilde{S}} := -v_{\mathfrak{q}_1}(\gamma)$. By Lemma 4.2 all primes in $S \cup \{\mathfrak{q}_2, \ldots, \mathfrak{q}_\ell\}$ split completely in L_1 and L_1/K is ramified only at $\mathfrak{q}_1$. For any elements $a_1, \ldots, a_n \in \mathbb{F}_p$ which are not all 0,

$$m_{\mathfrak{q}_1}(\sum_{i=1}^{n} a_i\gamma^{\alpha_i}) = d_{\tilde{S}} \max(\alpha_i | a_i \neq 0).$$

Hence $K(\wp^{-1}\gamma^{\alpha_i}) \notin K(\wp^{-1}\langle \gamma^{\alpha_1}, \ldots, \gamma^{\alpha_{i-1}} \rangle)$ for all $i = 1, \ldots, n$. This shows that the extensions $K(\wp^{-1}\gamma^{\alpha_i}), i = 1, \ldots, n$, are linearly disjoint over K, and hence that $\mathrm{Gal}(L_1/K) \cong (\mathbb{Z}/p\mathbb{Z})^n$. Lemma 4.2.(3) then implies that the genus of L_1 is:

$$g_{L_1} = 1 + p^n(g_K - 1) + \frac{p-1}{2}\sum_{i=1}^{n}(\alpha_i d_{\tilde{S}} + 1)p^{i-1} \deg \mathfrak{q}_1.$$

Since $\alpha_i d_{\tilde{S}} + 1 \leq 2nd_{\tilde{S}}$, the above sum is bounded by $2d_{\tilde{S}} \deg \mathfrak{q}_1 n(p^n - 1)/(p - 1)$. Hence g_{L_1} is at most $\tilde{c}_{\tilde{S},1} np^n$ for some constant $\tilde{c}_{\tilde{S},1}$.

Step II: Constructing L_r from a given L_{r-1} which is Galois over K. Let $S_r := S \cup \{\mathfrak{q}_{r+1}, \ldots, \mathfrak{q}_\ell\}$ and Q_r be the set of primes of L_{r-1} lying over $\mathfrak{q}_r$. Let b be the smallest integer for which the following divisor of L_{r-1}:

$$B = b\sum_{\mathfrak{q} \in Q_r} \mathfrak{q} - \sum_{\mathfrak{p}} \mathfrak{p}$$

has degree at least $2g_{L_{r-1}}-2$, where $\mathfrak{p}$ runs through the primes of L_{r-1} lying above primes in S_r. Since $\deg B = [L_{r-1}:K](b\deg \mathfrak{q}_r - \sum_{\mathfrak{p}\in S_r}\deg\mathfrak{p})$, one has:

$$b = \lceil \frac{2g_{L_{r-1}} - 2 + |G_{r-1}|\sum_{\mathfrak{p}\in S_r}\deg\mathfrak{p}}{|G_{r-1}|\deg\mathfrak{q}_r} \rceil.$$

Let $\mathfrak{q}\in Q_r$. Since $\deg B \geq 2g_{L_{r-1}}-2$, the Riemann-Roch theorem implies that

$$L(B) \subsetneq L(B+\mathfrak{q}) \subsetneq L(B+2\mathfrak{q}).$$

Thus, there is an element $\gamma \in L(B+2\mathfrak{q})\setminus L(B)$ with $(v_\mathfrak{q}(\gamma),p)=1$. We let Γ_r be the additive subgroup $\langle \gamma^\sigma, \sigma\in G_{r-1}\rangle \leq L_{r-1}^+$, and $L_r := L_{r-1}(\wp^{-1}\Gamma_r)$.

Step III: Showing that L_r satisfies (Ram), (Gen), and (Gal) for $1<r\leq \ell$. Since $v_\mathfrak{p}(\gamma^\sigma)\geq 0$ for every prime $\mathfrak{p}\notin Q_r$ and $\sigma\in G_{r-1}$, Lemma 4.2.(b) shows that the extensions $L_{r-1}(\wp^{-1}\gamma^\sigma)/L_{r-1}$, $\sigma\in G_{r-1}$, and hence L_r/L_{r-1}, ramify only over primes dividing $\mathfrak{q}_r$. Since $v_\mathfrak{p}(\gamma^\sigma)>0$ for every $\mathfrak{p}$ lying above a prime in S_r and $\sigma\in G_{r-1}$, Lemma 4.2 implies that such primes $\mathfrak{p}$ split completely in $L_{r-1}(\wp^{-1}\gamma^\sigma)$,$\sigma\in G_{r-1}$, and hence in L_r. Thus (Ram) holds.

For any $\alpha=\sum_{\sigma\neq 1}a_\sigma\gamma^\sigma\in\Gamma_r, a_\sigma\in\mathbb{F}_p$, we have:

$$m_\mathfrak{q}(\gamma) = -v_\mathfrak{q}(\gamma) > b \geq -v_\mathfrak{q}(\alpha)\geq m_\mathfrak{q}(\alpha).$$

Hence, $L_{r-1}(\wp^{-1}\gamma)$ is linearly disjoint from $L_{r-1}(\wp^{-1}\gamma^\sigma|\sigma\in G_{r-1}\setminus\{1\})$ over L_{r-1}. By symmetry, the extensions $L_{r-1}(\wp^{-1}\gamma^\sigma), \sigma\in G_{r-1}$, are linearly disjoint over L_{r-1}. Thus, $[L_r:L_{r-1}]=p^{|G_{r-1}|}$. Using Lemma 4.2.(3) we get:

$$\begin{aligned}\tfrac{g_{L_r}}{[L_r:K]} &= \tfrac{g_{L_r}}{|G_{r-1}|p^{|G_{r-1}|}} \\ &= \tfrac{g_{L_{r-1}}}{|G_{r-1}|} - \tfrac{p^{|G_{r-1}|}-1}{p^{|G_{r-1}|}|G_{r-1}|} + \tfrac{1}{2|G_{r-1}|p^{|G_{r-1}|}}\sum_{\mathfrak{q}\in Q_r,\gamma\in\Gamma_r}(m_\mathfrak{q}(\gamma)+1)\deg\mathfrak{q}.\end{aligned}$$

Note that the second summand is negative, $|Q_r|=|G_{r-1}|$, $|\Gamma_r|=p^{|G_{r-1}|}$, and $m_\mathfrak{q}(\gamma)$ is bounded by $b+2$. Thus,

$$\frac{g_{L_r}}{[L_r:K]} < \frac{g_{L_{r-1}}}{[L_{r-1}:K]} + \frac{1}{2}(b+3)\deg\mathfrak{q}_r. \tag{4.5}$$

By definition of b the second summand is bounded by:

$$\frac{1}{2}(b+3)\deg\mathfrak{q}_r \leq \frac{g_{L_{r-1}}}{[L_{r-1}:K]} + 2\deg\mathfrak{q}_r + \frac{1}{2}\sum_{\mathfrak{p}\in S_r}\deg\mathfrak{p}. \tag{4.6}$$

Setting $\tilde{c}_{\tilde{S},r} = 2\deg\mathfrak{q}_r + (1/2)\sum_{\mathfrak{p}\in S_r}\deg\mathfrak{p}$, we obtain (Gen) from (4.5) and (4.6).

It remains to show that (Gal) holds. Since G_{r-1} permutes $\gamma_\sigma, \sigma\in G_{r-1}$, the action of every $\tau\in G_{r-1}$ extends to an action on L_r permuting the subfields $L_{r-1}(\wp^{-1}\gamma_\sigma), \sigma\in G_{r-1}$. Hence L_r/K is Galois. Since Γ_r is a free cyclic G_{r-1}-module, the Galois group $\mathrm{Gal}(L_r/L_{r-1})$ is isomorphic to $\mathrm{Ind}_1^{G_{r-1}}\mathbb{F}_p$ as a G_{r-1}-module, giving rise to a short exact sequence:

$$1\to \mathrm{Ind}_1^{G_{r-1}}\mathbb{F}_p \to \mathrm{Gal}(L_r/K)\to G_{r-1}\to 1. \tag{4.7}$$

Since by Shapiro's lemma [16, Chp. 1, Proposition 10], $\mathrm{H}^2(G_{r-1},\mathrm{Ind}_1^{G_{r-1}}\mathbb{F}_p)=\{1\}$, the short exact sequence (4.7) splits and $\mathrm{Gal}(L_r/K)\cong \mathrm{Ind}_1^H\mathbb{F}_p\rtimes H\cong C_p\wr H$.

Step IV: Conclusion of theorem. Set $c_{S,1} = \tilde{c}_{\tilde{S},1}$ which depends only on S and a choice of additional primes in K. The theorem then holds for $\ell = 1$ by (Gen). Assume $\ell > 1$ and that there is a constant $c_{S,\ell-1}$ such that

$$\frac{g_{L_{\ell-1}}}{[L_{\ell-1} : K]} \leq c_{S,\ell-1} \log^{\circ(\ell-1)} [L_{\ell-1} : K]$$

for the constructed extensions $L_{\ell-1}/K$. By (Gal), $[L_{\ell-1} : K] < \log_p[L_\ell : K]$, and hence (Gen) gives:

$$\begin{array}{rcl} \frac{g_{L_\ell}}{[L_\ell:K]} & \leq & 2\frac{g_{L_{\ell-1}}}{[L_{\ell-1}:K]} + \tilde{c}_{\tilde{S},\ell} \\ & \leq & 2c_{S,\ell-1}\log^{\circ(\ell-1)}[L_{\ell-1} : K] + \tilde{c}_{\tilde{S},\ell} \\ & < & 2c_{S,\ell-1}\log^{\circ(\ell-1)} \log_p[L_\ell : K] + \tilde{c}_{\tilde{S},\ell}. \end{array} \tag{4.8}$$

Since for $p \geq 3$, $\log_p[L_\ell : K] \leq \log[L_\ell : K]$ and

$$\log^{\circ(\ell-1)} \log_2[L_{\ell-1} : K] = \log^{\circ(\ell-1)}(\frac{\log[L_\ell : K]}{\log 2}) \leq \frac{\log^{\circ \ell}[L_\ell : K]}{\log 2},$$

(4.8) ensures the existence of a constant $c_{S,l}$ as required in the theorem. □

Remark 4.3. (1) Our construction of L_1 extends an argument in [10] in which the functions were chosen explicitly and D was $\mathbb{P}^1$. However, this construction fails for $L_r, r > 1$, since choosing a function γ using Riemann-Roch as in Step I, over L_r, enlarges the different exponent causing the genus to exceed its desired growth rate.

(2) Step IV shows that for $p > 3$, the constant $c_{S,r}$ obtained for solvable extensions of length $r > 1$ is essentially twice the constant $c_{S,r-1}$. More precisely, for $p \geq 3$ the proof gives length ℓ extensions L_ℓ/K of arbitrarily large degree d and genus g_L such that for every $\ell \in \mathbb{N}$:

$$g_{L_\ell} \leq 2^{\ell-1} c_{S,1} d \log^{(\ell)} d + o_d(d \log^{(\ell)} d).$$

References

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

[2] G. Frey and E. Kani, Projective p-adic representations of the k-rational geometric fundamental group. Arch. Math., **77** (2001), 32–46.

[3] G. Frey, E. Kani, and H. Völklein, Curves with infinite K-rational geometric fundamental group. In Aspects of Galois theory (Gainesville, FL, 1996), vol. **256** of London Math. Soc. Lecture Note Ser., Cambridge Univ. Press, Cambridge, (1999) 85-118.

[4] G. Frey, M. Perret, H. Stichtenoth, On the different of abelian extensions of global fields. *Coding Theorey and Algebraic Geometry (Lumminy, 1991),* Lect. Notes in Math. **1518**, Springer-Verlag, New York, (1992), 26–32.

[5] A. Garcia, H. Stichtenoth, Elementary abelian p-extensions of algebraic function fields, Manuscripta Math. **72** (1991), 67–79.

[6] A. Garca, H. Stichtenoth, A tower of Artin-Schreier extensions of function fields attaining the Drinfel'd-Vladut bound. Invent. Math. **121** (1995), no. 1, 211-222.

[7] A. Garcia, H. Stichtenoth, A. Bassa, P. Beelen, Towers of Function Fields over Non-prime Finite Fields, arXiv:1202.5922.

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

[9] Y. Ihara, Algebraic curves mod p and arithmetic groups. Algebraic Groups and Discontinuous Subgroups (Boulder, Colo., 1965), Proc. Sympos. Pure Math. **9**, Amer. Math. Soc., Providence, (1966), 265–271.
[10] A. Kresch, L. Wetherell, M. E. Zieve, Curves of every genus with many points, I: Abelian and toric families, J. Algebra **250** (2002), 353–370.
[11] Y. I. Manin, What is the maximum number of points on a curve over F2? J. Fac. Sci. Univ. Tokyo **28**, (1981), 715–720.
[12] Y. I. Manin, S. G. Vladut, Linear codes and modular curves. Itogi Nauki i Tekhniki **25** (1984), 209–257. [J. Soviet Math. 30 (1985), 2611–2643.]
[13] N. Elkies, Explicit modular towers. Proceedings of the Thirty-Fifth Annual Allerton Conference on Communication, Control and Computing, (ed. T. Basar and A. Vardy), Univ. of Illinois at Urbana-Champaign, (1998), 23–32.
[14] J.S. Milne, Abelian varieties. Lecture notes, version 2.0 (2008).
[15] H. Niederreiter, C.P. Xing, Towers of global function fields with asymptotically many rational places and an improvement on the Gilbert-Varshamov bound. Math. Nachr. **195** (1998), 171–186.
[16] J.-P. Serre, Galois Cohomology, Springer, edition of 1996.
[17] J.-P. Serre, Sur le nombre des points rationnels dune courbe algebrique sur un corps fini. C. R. Acad. Sci. Paris **296** (1983), 397–402.
[18] H. Stichtenoth, Algebraic Function Fields and Codes (2nd edition). Graduate Texts in Mathematics **254**, Springer Verlag (2009).
[19] T. Zink, Degeneration of Shimura surfaces and a problem in coding theory. Fundamentals of Computation Theory (Cottbus, 1985), Lect. Notes in Comput. Sci. 199, Springer-Verlag, New York, (1985), 503–511.

Department of Mathematics, University of Michigan, Ann Arbor, USA
E-mail address: neftin@umich.edu

Department of Mathematics, University of Michigan, Ann Arbor, USA
E-mail address: zieve@umich.edu