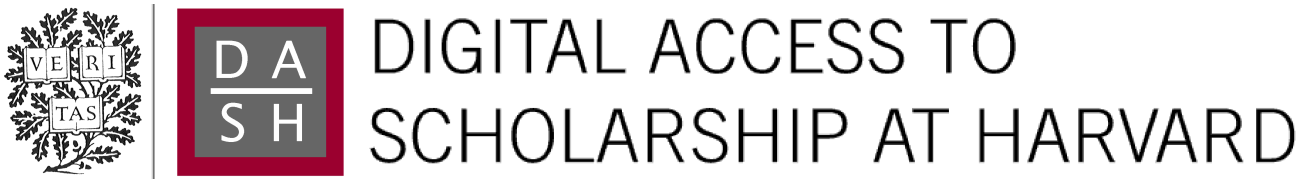

Curves of Every Genus with Many Points, II: Asymptotically Good Families

CURVES OF EVERY GENUS WITH MANY POINTS, II: ASYMPTOTICALLY GOOD FAMILIES

NOAM D. ELKIES, EVERETT W. HOWE, ANDREW KRESCH, BJORN POONEN, JOSEPH L. WETHERELL, AND MICHAEL E. ZIEVE

Abstract. We resolve a 1983 question of Serre by constructing curves with many points of every genus over every finite field. More precisely, we show that for every prime power q there is a positive constant c_q with the following property: for every integer $g \geq 0$, there is a genus-g curve over $\mathbb{F}_q$ with at least $c_q g$ rational points over $\mathbb{F}_q$. Moreover, we show that there exists a positive constant d such that for every q we can choose $c_q = d \log q$. We show also that there is a constant $c > 0$ such that for every q and every $n > 0$, and for every sufficiently large g, there is a genus-g curve over $\mathbb{F}_q$ that has at least cg/n rational points and whose Jacobian contains a subgroup of rational points isomorphic to $(\mathbb{Z}/n\mathbb{Z})^r$ for some $r > cg/n$.

1. Introduction

Let q be a power of a prime p and let $\mathbb{F}_q$ be the field with q elements. We will study the function

$$N_q(g) := \max\{\#C(\mathbb{F}_q) : C \text{ is a curve of genus } g \text{ over } \mathbb{F}_q\},$$

where by a *curve* over a field k we mean a smooth, projective, geometrically irreducible 1-dimensional variety over k. In particular, we will be interested in upper and lower bounds on the asymptotic quantities

$$A^+(q) := \limsup_{g\to\infty} N_q(g)/g \qquad \text{and} \qquad A^-(q) := \liminf_{g\to\infty} N_q(g)/g.$$

The quantity that we call $A^+(q)$ is denoted $A(q)$ in most current literature.

We begin by reviewing the known bounds on $A^+(q)$. The upper bound $A^+(q) \leq 2\sqrt{q}$ follows from the well-known inequality

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

which was proved by Weil [26] in the 1940s. Serre writes [21] that for a long time Weil's inequality was considered "essentiellement «optimale»." The situation changed in 1981, when Manin [16] (following Goppa) and Ihara [12] found bounds on $N_q(g)$ that are significantly better than the Weil bound when g is large compared to q. Ihara's idea was refined by Drinfel'd and Vlăduţ [2] to prove that, for fixed q, we have

$$N_q(g) \leq (\sqrt{q} - 1 + o(1))g \qquad \text{as } g \to \infty, \tag{1}$$

which shows that $A^+(q) \leq \sqrt{q} - 1$.

Date: 23 July 2002.

The authors thank Jordan Ellenberg, Yasutaka Ihara, and Felipe Voloch for helpful conversations. N. E. and B. P. were supported in part by Packard Fellowships; in addition, B. P. was supported by NSF Grant DMS-9801104 and a Sloan Fellowship. A. K., J. W., and M. Z. were supported in part by NSF Mathematical Sciences Postdoctoral Research Fellowships.

The problem of finding lower bounds for $A^+(q)$ leads to the problem of producing curves over $\mathbb{F}_q$ with many points. Serre [20, 22] used class field towers to construct infinite sequences of such curves; in this way, he showed that $A^+(q) > 0$ for all q. In fact he proved that $A^+(q) > c \log q$ for some $c > 0$ not depending on q, and his proof gave better bounds for nonprime q. Ihara [8, 9, 11, 12] used supersingular points on Shimura curves to show that if q is a square we have $A^+(q) \geq \sqrt{q} - 1$; together with the Drinfel'd-Vlăduţ bound (1), this proves that $A^+(q) = \sqrt{q} - 1$ for every square q. Several other authors proved further results along similar lines. (For a survey, see the introduction to [14].) But qualitatively the situation today is similar to that in 1983:

- There is no nonsquare q for which one knows whether or not $A^+(q) = \sqrt{q} - 1$.
- For square q, every known sequence $\{C_i\}$ of curves over $\mathbb{F}_q$ whose genera g_i tend to infinity and for which $\#C_i(\mathbb{F}_q)/g_i \to \sqrt{q} - 1$ has the property that C_i is modular (of elliptic, Shimura, or Drinfel'd types) for all sufficiently large i (see [3, 4]).

In this paper we consider the problem of finding lower bounds for $A^-(q)$. To show that $A^-(q)$ is greater than some constant c, one must show that for *every* sufficiently large g there is a curve of genus g over $\mathbb{F}_q$ with more than cg points. Unfortunately, the class field tower and modular curve constructions mentioned above miss infinitely many genera [1], so they do not lead immediately to lower bounds for $A^-(q)$. In fact, before now there was no q for which it was known whether $A^-(q) > 0$; furthermore, even the much weaker assertion $\lim_{g\to\infty} N_q(g) = \infty$ was proved only recently [14].

The main result of this paper gives an affirmative answer to a 1983 question of Serre [21]:

Theorem 1.1. *For every q, we have $A^-(q) > 0$.*

We also discuss quantitative refinements of this result. For instance, at the end of Section 3.2 we show that there is a constant $d > 0$ such that $N_q(g) \geq (d \log q)g$. In particular, we find that $A^-(q) \geq d \log q$ for all q. This can be strengthened for square q:

Theorem 1.2. *We have*

$$A^-(q) \geq \begin{cases} \dfrac{\sqrt{q} - 1}{2 + (\log 2/\log q)} & \text{if } q \text{ is an even square;} \\ \dfrac{\sqrt{q} - 1}{2 + (\log 4/\log q)} & \text{if } q \text{ is an odd square.} \end{cases}$$

For odd square $q < 417$, Corollary 6.2 in Section 6 gives an improved lower bound.

Theorem 1.1 shows that for every sufficiently large integer g there exist curves of genus g with many points. Theorem 1.3 below shows that we can simultaneously force the rational points of the Jacobian to contain certain groups. Suppose C is a curve over a field k and $n > 1$ is an integer. We define the *n-rank* $r_n(C)$ of C to be the largest integer r such that the group $(\mathbb{Z}/n\mathbb{Z})^r$ can be embedded in the group of k-rational points of the Jacobian of C.

Theorem 1.3. *There exists a constant $c > 0$ such that for all integers $n > 1$ and prime powers q the following statement holds: For all sufficiently large integers g, there is a genus-g curve C over $\mathbb{F}_q$ with $r_n(C) > (c/n)g$ and $\#C(\mathbb{F}_q) > (c/n)g$.*

Our proofs of these results involve covers of curves. A *cover* of a curve C over a field k is another curve B over k together with a nonconstant separable map $B \to C$ over k. Our strategy for proving Theorems 1.1 and 1.2 is to begin with some sequence of curves

with many points that achieve "enough" genera, and then to fill in the missing genera via degree-2 covers. More specifically, we start with a sequence of curves over $\mathbb{F}_q$ that have many points and whose genera grow at most exponentially. Then we show that for every curve C in this sequence, and for every integer h greater than some constant multiple of the genus of C, there exists a degree-2 cover $B \to C$ over $\mathbb{F}_q$ such that B has genus h. Either B or its quadratic twist B' will have at least as many $\mathbb{F}_q$-rational points as C, because $\#B(\mathbb{F}_q) + \#B'(\mathbb{F}_q) = 2\#C(\mathbb{F}_q)$. To produce the sequence of curves we use class field towers and Shimura curves (see Section 3). To produce the degree-2 covers, we use the following result of independent interest:

Proposition 1.4. *Let C be a curve of genus g over a finite field k. For every integer $h \geq 4g$, there exists a genus-h curve B over k that admits a degree-2 covering map $B \to C$ defined over k.*

In the next section we prove Proposition 1.4, as well as a generalization of the proposition to curves over arbitrary fields. We prove Theorem 1.1 and a weak version of Theorem 1.2 in Sections 3.2 and 3.3, respectively. In Section 4 we prove Theorem 1.3 and in Section 5 we prove the full version of Theorem 1.2. We end in Section 6 by discussing limitations on the results obtainable by our methods. Our proof of Theorem 1.1 relies on Serre's proof [22] that $A^+(q) > 0$ for all q; since Serre's proof has not been published, we include a version of it as an appendix.

2. Degree-2 covers

In this section we prove Proposition 1.4 and give an analogous result for curves over infinite fields.

2.1. **Finite fields.** Suppose C is a curve over $\mathbb{F}_q$. Let $g(C)$ denote the genus of C, and let $\mathbb{F}_q(C)$ denote the function field of C. For every positive integer d, let $n_d(C)$ denote the number of places of C of degree d. We begin with a lemma that gives a lower bound on $n_d(C)$ for large enough d.

Lemma 2.1. *Let C be a curve over $\mathbb{F}_q$ of genus g.*

(i) *For every $d > 0$ we have $n_d(C) > (q^d - (6g+3)q^{d/2})/d$.*
(ii) *If $g > 1$ and $d > 2g$ we have $n_d(C) > 0$.*
(iii) *If q is odd and $d > 2g$ then $n_d(C) \geq 2^{2g}$, with equality if and only if $q = d = 3$, $g = 1$, and $\#C(\mathbb{F}_3) = 6$.*
(iv) *Assume $g \geq 900$. If j is a positive integer and $d \geq \log_q(j \log j + 1) + \sqrt{g}$, then $n_d(C) > j$.*

Proof. (i) Clearly $\#C(\mathbb{F}_{q^d}) = \sum_{m|d} m \cdot n_m(C)$, so by Möbius inversion we find that

$$dn_d(C) = \sum_{m|d} \mu(d/m)\#C(\mathbb{F}_{q^m}). \tag{2}$$

Combining the Weil lower bound on $\#C(\mathbb{F}_{q^d})$ with the Weil upper bounds on the various $\#C(\mathbb{F}_{q^m})$, we find that

$$dn_d(C) \geq q^d + 1 - 2gq^{d/2} - \sum_{\substack{m|d \\ 1 \leq m < d}} \left(q^m + 1 + 2gq^{m/2}\right).$$

Using the fact that $q + q^2 + \cdots + q^{\lfloor d/2 \rfloor} < 2q^{d/2}$, we see that

$$\sum_{\substack{m|d \\ 1 \le m < d}} \left(q^m + 1 + 2gq^{m/2}\right) < \sum_{1 \le m \le d/2} ((2g+1)q^m + 1) < (4g+2)q^{d/2} + d/2.$$

Thus $dn_d(C) > q^d - (6g+2)q^{d/2} - d/2$, and (i) follows.

(ii) Suppose $g \ge 2$ and $d \ge 2g+1$. If $q > 2$ then $q^{d/2} \ge q^{g+1/2} > 6g+3$, so by (i) we have $n_d(C) > 0$. Suppose $q = 2$. If $g \ge 5$ or if $d \ge g+6$ then once again we have $2^{d/2} > 6g+3$, and (i) shows that $n_d(C) > 0$. We are left to consider six triples (q, d, g). For each one, we can show that $n_d(C) > 0$ by combining equation (2) with the refined Weil bound $|\#C(\mathbb{F}_q) - q - 1| \le g\lfloor 2\sqrt{q} \rfloor$ (see [20, Théorème 1]) and the trivial bound $\#C(\mathbb{F}_q) \ge 0$.

(iii) We assume $g \ge 1$, since (iii) is well-known when $g = 0$ (it amounts to the existence of irreducible polynomials over $\mathbb{F}_q$ of arbitrary positive degree). If $q \ge 5$ then (iii) follows from (i), so assume $q = 3$. In this case (iii) again follows from (i) except when (g, d) is one of $(1,3), (1,4), (2,5)$. When (g, d) is either $(1,4)$ or $(2,5)$ then (iii) follows from (2) and the Weil bounds. When $(g, d) = (1, 3)$, the statement can be proved by considering the possible zeta functions of elliptic curves over $\mathbb{F}_3$.

(iv) Define $f(x) = 2^{\sqrt{x}/2}/2 - (6x+3)$. A short computation shows that $f(900)$ is positive and that $f(x)$ is increasing for $x \ge 900$. We conclude that $(6g+3) \le 2^{\sqrt{g}/2}/2 \le q^{d/2}/2$; applying (i), we find that $n_d(C) \ge q^d/2d$.

Note that $d \ge 30$ and that $q^d/2d$ is an increasing function of d for d in this range. When $j = 1$, this shows that $q^d/2d \ge 2^{30}/60 > j$. When $j \ge 2$, we find that

$$\frac{q^d}{2d} \ge \frac{(j \log j + 1)q^{30}}{2\log_q(j \log j + 1) + 60} \ge \frac{2^{30} j \log j}{4 \log_2 j + 60} \ge \frac{2^{30} j \log j}{64 \log_2 j} > j.$$

In both cases, $n_d(C) > j$, as desired. □

Proof of Proposition 1.4. The assertion is clear when $g = 0$, so we assume $g \ge 1$.

First suppose q is even. If $\#C(\mathbb{F}_q) > 0$ then let R be a rational point of C. Set $m = 2h - 4g + 1$; by Riemann-Roch, there exists a function f in $\mathbb{F}_q(C)$ having polar divisor mR. Let $B \to C$ be the cover of C obtained by adjoining a root of $X^2 + X + f$ to $\mathbb{F}_q(C)$. This cover has degree two; its different is $(m+1)R'$, where R' is the point of B lying over R. By Hurwitz, the genus of B is h, and we are done. We are left with the case where $\#C(\mathbb{F}_q) = 0$. Since every genus-1 curve over a finite field has a rational point, we must have $g \ge 2$. Then Lemma 2.1(ii) guarantees the existence of a place P of degree $d := h - 2g + 1$. By Riemann-Roch, there exists $f \in \mathbb{F}_q(C)$ with polar divisor P. If we form B as before, the different of the cover $B \to C$ is $2P'$, where P' is the place of B lying above P. Again the genus of B is h, and we are done.

Now suppose q is odd. Let $J(\mathbb{F}_q)$ be the group of degree-zero divisor classes on C (or equivalently, the group of $\mathbb{F}_q$-rational points on the Jacobian of C). Let $d = h - 2g + 1$, and let T_d denote the set of places on C of degree d. Consider the map $T_d \to J(\mathbb{F}_q)/2J(\mathbb{F}_q)$ defined by $P \mapsto [P - P_0]$, where P_0 is any fixed degree-d divisor on C. Suppose that $\#T_d > \#(J(\mathbb{F}_q)/2J(\mathbb{F}_q))$. Then there are distinct places $P, P' \in T_d$ with the same image in $J(\mathbb{F}_q)/2J(\mathbb{F}_q)$, so there is a function f on C having divisor $P - P' + 2D$ for some divisor D. Adjoining $\sqrt{f}$ to the function field of C produces a degree-2 cover $B \to C$ over $\mathbb{F}_q$, with the genus of B equal to $2g + d - 1 = h$. Thus we need only show that $\#T_d > \#(J(\mathbb{F}_q)/2J(\mathbb{F}_q))$. But $\#(J(\mathbb{F}_q)/2J(\mathbb{F}_q))$ is equal to the number of 2-torsion points in $J(\mathbb{F}_q)$,

and this is at most 2^{2g}. Lemma 2.1(iii) supplies the needed inequality so long as we are not in the exceptional case where $q = d = 3$, $g = 1$, and $\#C(\mathbb{F}_q) = 6$. But in that case $\#J(\mathbb{F}_q) = 6$, so $\#(J(\mathbb{F}_q)/2J(\mathbb{F}_q)) = 2$ and the result follows. □

Remark. The argument given above for even q can be modified to show that every curve over a finite field of characteristic 3 has Artin-Schreier covers of every sufficiently large genus. However, the analogous statement in characteristic $p > 3$ is not true; the degree of the different of an Artin-Schreier cover $B \to C$ is divisible by $p-1$, so for any such cover we have $g(B) \equiv g(C) \bmod (p-1)/2$.

2.2. **Arbitrary fields.** Although we will not need it for our main results, we now discuss a generalization of Proposition 1.4 to arbitrary fields. The *index* of a curve C is the positive integer I such that the image of the degree map $\mathrm{Div}(C) \to \mathbb{Z}$ equals $I\mathbb{Z}$; equivalently, I is the greatest common divisor of the degrees of all places of C. A classical result of F. K. Schmidt asserts that curves over finite fields have index 1 (this follows from Lemma 2.1(ii); see [25, Cor. V.1.11] for a more elementary proof). Over some infinite fields, higher indices are possible; for instance, a conic over $\mathbb{Q}$ with no rational points has index 2.

Proposition 2.2. *Let C be a curve of genus g over a field k and let I be its index. If $B \to C$ is a degree-2 cover of C of genus h, then $h \equiv 1 \pmod{I}$. Conversely, if h is an integer satisfying $h \geq 4g$ and $h \equiv 1 \pmod{I}$, then there exists a degree-2 cover $B \to C$ of genus h.*

Proof. The index divides $2g-2$, because $2g-2$ is the degree of the canonical divisor. If the characteristic of k is not 2, then $k(B) \simeq k(C)(\sqrt{f})$ for some $f \in k(C)^*$, and the total degree of the set of points where f has odd valuation must be a multiple of $2I$, since the divisor of f has degree zero; now the Hurwitz formula implies $h \equiv 1 \pmod{I}$. If k has characteristic 2, we have $k(B) \simeq k(C)(z)$, where z satisfies $z^2 + z = f$ for some $f \in k(C)$. A local calculation shows that each point of B occurs with even multiplicity in the different, so the degree of the different is divisible by $2I$, and Hurwitz again implies $h \equiv 1 \pmod{I}$.

Now we prove the converse assertion. Proposition 1.4 handles the case where k is finite, so we assume k is infinite. Let $d = h - 2g + 1$. Then $d \equiv 2 - 2g \equiv 0 \pmod{I}$, so we can choose a divisor D on C of degree d. Since $d \geq 2g+1$, the divisor D is very ample, and therefore determines an embedding $C \to \mathbb{P}^{d-g}$ whose image has degree d. The composition of this embedding with a generically chosen linear projection to $\mathbb{P}^1$ is a degree-d map $f\colon C \to \mathbb{P}^1$. The linear projection may be chosen so as not to kill a chosen tangent vector at some point of C, so we may assume the map f induces a separable extension of function fields. By composing f with an automorphism of $\mathbb{P}^1$, we may further assume that 0 and ∞ are not branch points of f. Now let B be the cover obtained by adjoining to $k(C)$ a root y of $y^2 + y = f$ or $y^2 = f$, according as the characteristic of k equals 2 or not. The different of $B \to C$ has degree $2d$ in each case, so by Hurwitz we have $g(B) = 2g - 1 + d = h$. □

3. Asymptotic lower bounds

In this section we prove Theorem 1.1 and a weakened version of Theorem 1.2. (The full version of Theorem 1.2 will be proved in Section 5.2.) As we noted in the introduction, Serre used class field towers to exhibit a positive lower bound on $A^+(q)$ for every q, and Ihara used Shimura curves to produce a better lower bound for square q. We will briefly recall these constructions, and include some necessary complements. Our theorems will follow from these constructions and Proposition 1.4.

3.1. **Preliminaries.** We begin by relating Proposition 1.4 to rational points.

Proposition 3.1. *Let C be a curve over $\mathbb{F}_q$ of genus g. For every integer $h \geq 4g$, we have $N_q(h) \geq \#C(\mathbb{F}_q)$.*

Proof. By Proposition 1.4, there is a genus-h curve B over $\mathbb{F}_q$ that admits a degree-2 covering map $B \to C$ over $\mathbb{F}_q$. The result follows, since either B or its quadratic twist over C has at least as many $\mathbb{F}_q$-rational points as does C. □

Corollary 3.2. *If $h \geq 4g$ then $N_q(h) \geq N_q(g)$.* □

Now we give a general technique for producing lower bounds for $A^-(q)$. We will call a sequence $\mathcal{C} = \{C_0, C_1, \dots\}$ of curves over $\mathbb{F}_q$ *ascensive* if $\lim_{i\to\infty} g(C_i) = \infty$. If $\mathcal{C}$ is an ascensive sequence of curves, define

$$\gamma(\mathcal{C}) := \liminf_{i\to\infty} \frac{\#C_i(\mathbb{F}_q)}{g(C_{i+1})}.$$

Note that we divide the number of points of each curve in the sequence by the genus of the *next* curve. It is not hard to show that $0 \leq \gamma(\mathcal{C}) \leq A^+(q)$.

Proposition 3.3. *If $\mathcal{C} = \{C_0, C_1, \dots\}$ is an ascensive sequence of curves over $\mathbb{F}_q$, then $A^-(q) \geq \gamma(\mathcal{C})/4$.*

Proof. For any $h \geq 4g(C_0)$, let i be the largest integer for which $h \geq 4g(C_i)$. Proposition 3.1 implies that $N_q(h) \geq \#C_i(\mathbb{F}_q)$; thus,

$$\frac{N_q(h)}{h} \geq \frac{\#C_i(\mathbb{F}_q)}{4g(C_{i+1})},$$

and the desired result follows. □

3.2. **Class field towers.** In this section we prove Theorem 1.1 using Proposition 3.3. To do this, we must produce sequences $\mathcal{C}$ with $\gamma(\mathcal{C}) > 0$. We accomplish this using class field towers.

Let F be the function field of a curve over $\mathbb{F}_q$. Let S be a nonempty set of rational places of F, and let ℓ be a prime number. Let $\overline{F}$ be an algebraic closure of F. Then the (S, ℓ)-*class field tower of F* is the sequence $\mathcal{F} = \{F_0, F_1, \dots\}$ of function fields over $\mathbb{F}_q$ defined inductively as follows. We start with $F_0 = F$. Then for every integer $i \geq 0$ we let F_{i+1} be the maximal unramified abelian extension of F_i in $\overline{F}$, of degree a power of ℓ, in which every place in S splits completely into rational places. The tower is called *infinite* if each extension F_{i+1}/F_i is nontrivial.

The following result demonstrates the utility of curves whose function fields have infinite (S, ℓ)-class field towers.

Lemma 3.4. *Let C be a curve over $\mathbb{F}_q$ of genus $g(C) > 1$, let S be a nonempty set of rational places of $\mathbb{F}_q(C)$, and let ℓ be a prime. Suppose the (S, ℓ)-class field tower of $\mathbb{F}_q(C)$ is infinite. Then there exists an ascensive sequence $\mathcal{C}$ of curves over $\mathbb{F}_q$ such that*

$$\gamma(\mathcal{C}) \geq \frac{\#S}{g(C) - 1} \cdot \frac{1}{\ell}.$$

Proof. Let $\mathcal{F} = \{F_0, F_1, \dots\}$ be the (S,ℓ)-class field tower of $\mathbb{F}_q(C)$. Since each extension F_{i+1}/F_i is Galois of ℓ-power degree, there is a refinement of the tower of fields

$$F_0 \subset F_1 \subset F_2 \subset \cdots$$

to a tower of degree-ℓ field extensions

$$F_0 = \widehat{F}_0 \subset \widehat{F}_1 \subset \widehat{F}_2 \subset \cdots$$

such that each F_i occurs as some $\widehat{F}_j$. Clearly $\widehat{F}_n$ is an unramified extension of F_0 in which every place in S splits completely. Thus, the genus of $\widehat{F}_n$ is $1+\ell^n(g(C)-1)$, and the number of rational places of $\widehat{F}_n$ is at least $\ell^n \cdot \#S$. Let C_n be a curve over $\mathbb{F}_q$ such that $\mathbb{F}_q(C_n) \cong \widehat{F}_n$ and let $\mathcal{C} = \{C_0, C_1, \dots\}$. Then we have

$$\frac{\#C_n(\mathbb{F}_q)}{g(C_{n+1})} \geq \frac{\ell^n \cdot \#S}{1+\ell^{n+1}(g(C)-1)},$$

so that $\mathcal{C}$ is an ascensive sequence satisfying the conclusion of the lemma. □

Theorem 1.1 follows from Lemma 3.4 and Proposition 3.3. Indeed, for every fixed q, Serre has constructed a curve C over $\mathbb{F}_q$ of genus $g > 1$ and a nonempty set S of rational places of $\mathbb{F}_q(C)$, such that the $(S,2)$-class field tower of C is infinite. (The appendix contains a version of Serre's construction.)

Remark. In fact, Serre's construction yields C and S with $\#S > c_1(\log q)^2$ and $g(C) < c_2 \log q$, for some positive constants c_1 and c_2. Let $d = \min(c_1/(8c_2), 1/(2c_2))$. By considering hyperelliptic curves when $g \leq 4c_2 \log q$, and degree-2 covers of the curves from Serre's tower when $g > 4c_2 \log q$, we conclude that $N_q(g) > (d \log q)g$ for all q and g. This justifies the claim we made in the introduction, just before the statement of Theorem 1.2.

For some nonprime q, Serre's proof yields better bounds (as does the method of Zink [27] based on degenerate Shimura surfaces). If q is a square, one gets even better results by using Shimura curves (among other methods — see [5, 6, 7]), as we explain in the following section.

3.3. **Classical modular curves and Shimura curves.** In this section we will prove the following weakened version of Theorem 1.2:

Theorem 3.5. *For every square q, we have $A^-(q) \geq (\sqrt{q}-1)/4$.*

Proof. We first sketch a proof in the special case $q = p^2$ using the classical modular curves $X_0(\ell)$. If $q = p^2$, let $\mathcal{C} = \{X_0(\ell_1), X_0(\ell_2), X_0(\ell_3), \dots\}$, where $\ell_1 < \ell_2 < \dots$ are the primes distinct from p. Then, writing $g_i = g(X_0(\ell_i))$ and $N_i = \#X_0(\ell_i)(\mathbb{F}_q)$, we have

$$N_i \geq (p-1)(\ell_i+1)/12 \qquad \text{and} \qquad g_i = \begin{cases} (\ell_i - 13)/12 & \text{if } \ell_i \equiv 1 \pmod{12} \\ \lfloor (\ell_i+1)/12 \rfloor & \text{otherwise,} \end{cases}$$

where the formula for g_i is classical, and the bound on N_i holds because all supersingular points on $X_0(\ell_i)$ are defined over $\mathbb{F}_{p^2}$ and their number is at least $(p-1)(\ell_i+1)/12$. We compute

$$\gamma(\mathcal{C}) = \liminf_{i\to\infty} \frac{N_i}{g_{i+1}} \geq \liminf_{i\to\infty} \frac{(p-1)(\ell_i+1)}{\ell_{i+1}+1} = p-1.$$

(In fact, using the Drinfel'd-Vlăduţ bound one can show that $\gamma(\mathcal{C}) = p-1$.) Now Proposition 3.3 implies that $A^-(p^2) \geq (p-1)/4$. This proves Theorem 3.5 for the case $q = p^2$.

A different proof for the case $q = p^2$ can be given using the Igusa-Ihara field of modular functions of level n over $\mathbb{F}_{p^2}$, where n ranges over the positive integers coprime to p. (This field is the function field of a twist of $X(n)$ defined over $\mathbb{F}_{p^2}$ such that all its supersingular points are defined over $\mathbb{F}_{p^2}$: an open subset of this twist parameterizes elliptic curves E with a pairing-respecting isomorphism from $E[n]$ to the Galois module $(\mathbb{Z}/n\mathbb{Z})^2$ on which the p^2-Frobenius automorphism acts as multiplication by $-p$.) The relevant facts about these fields were announced in [8] and proved in [9, pp. 166–170] (see also [10]).

For more general square fields, we use Shimura curves. Suppose $q = p^{2m}$ where p is prime and $m \geq 1$. Let F be a totally real number field that has a prime $\mathfrak{p}$ whose norm is p^m. Let $F_{\mathfrak{p}}$ be the completion of F at $\mathfrak{p}$ and let $\mathfrak{o}$ denote the ring of integers of F. Let B be a quaternion algebra over F whose ramification locus contains all but one of the infinite places of F and does not contain $\mathfrak{p}$; standard results of class field theory show that there are infinitely many such B. As is explained in Ihara's survey article [13], associated to the data $(F, \mathfrak{p}, B)$ there is a family of Shimura curves with many points over $\mathbb{F}_q$ — see [24], [11], and [17] for further details. We will show that this family contains enough curves for us to find a subfamily $\mathcal{C}$, indexed by the positive integers, for which $\gamma(\mathcal{C}) = \sqrt{q} - 1$.

Let $N_{B/F}$ denote the reduced norm map of the quaternion algebra B and let $\mathfrak{O}$ be an arbitrary $\mathfrak{o}$-order in B. Let $\mathfrak{o}[\mathfrak{p}^{-1}]$ denote the ring obtained by adjoining to $\mathfrak{o}$ all of the elements of the fractional ideal $\mathfrak{p}^{-1}$, and let $\mathfrak{O}[\mathfrak{p}^{-1}] = \mathfrak{O} \otimes_{\mathfrak{o}} \mathfrak{o}[\mathfrak{p}^{-1}]$. We define the quaternionic arithmetic group

$$\Gamma := \{\, \alpha \in \mathfrak{O}[\mathfrak{p}^{-1}] : N_{B/F}(\alpha) = 1\}/\{\pm 1\},$$

which can be embedded in $\mathrm{PSL}_2(\mathbb{R}) \times \mathrm{PSL}_2(F_{\mathfrak{p}})$ as a discrete subgroup. The group Γ contains a torsion-free subgroup Γ_0 of finite index. Associated to Γ_0 there is a curve X_0 over $\mathbb{F}_q$ and a set S_0 of $\mathbb{F}_q$-places of X_0 such that $\#S_0 \geq (\sqrt{q} - 1)(g_0 - 1)$, where g_0 is the genus of X_0. To every finite-index congruence subgroup $\Gamma_1 \subset \Gamma_0$ there is an associated unramified cover $X_1 \to X_0$ of degree $(\Gamma_0 : \Gamma_1)$, defined over $\mathbb{F}_q$, such that all the places of S_0 split completely. Consequently, to obtain a family of $\mathbb{F}_q$-curves $\mathcal{C}$ with $\gamma(\mathcal{C}) = \sqrt{q} - 1$ it suffices to show that Γ_0 has a sequence of finite-index congruence subgroups such that the index d_i of the ith subgroup tends to infinity and such that $\lim_{i\to\infty} d_{i+1}/d_i = 1$. We will construct such a sequence.

Let $p_1 < p_2 < \cdots$ be the sequence of primes that lie below degree-1 primes $\mathfrak{p}_i$ of F. Chebotarev's density theorem shows that the sequence $\{p_i\}$ is infinite and has positive density in the sequence of prime numbers; in particular, the sequence $(p_{i+1} + 1)/(p_i + 1)$ approaches 1 as i approaches infinity. Throwing away finitely many primes, we may suppose, for each i, that $p_i \neq p$ and that $\mathfrak{O} \otimes_{\mathfrak{o}} (\mathfrak{o}/\mathfrak{p}_i)$ is a central simple algebra. By Wedderburn's theorem, we may choose an isomorphism $\mathfrak{O}[\mathfrak{p}^{-1}] \otimes_{\mathfrak{o}} (\mathfrak{o}/\mathfrak{p}_i) \cong M_2(\mathbb{F}_{p_i})$. Let $U(p_i) \subset \mathrm{PSL}_2(\mathbb{F}_{p_i})$ denote the subgroup of upper-triangular matrices and define $\Gamma_0(\mathfrak{p}_i)$ to be the intersection of Γ_0 with the subgroup

$$\{\, \alpha \in \mathfrak{O}[\mathfrak{p}^{-1}] : N_{B/F}(\alpha) = 1 \text{ and } \overline{\alpha} \in U(p_i)\,\}/\{\pm 1\}$$

of Γ, where $\overline{\alpha}$ denotes the image of α in $M_2(\mathbb{F}_{p_i})$ under the chosen isomorphism.

We claim that the index $d_i := [\Gamma_0 : \Gamma_0(\mathfrak{p}_i)]$ is equal to $p_i + 1$ when i is sufficiently large. To see this, note that for each i the map $\alpha \mapsto \overline{\alpha}$ is a homomorphism $\tau_i \colon \Gamma \to \mathrm{PSL}_2(\mathbb{F}_{p_i})$. A strong approximation theorem [23, (5.12)] applies in this case, and as a consequence τ_i is surjective for every i. When $p_i > 3$ the group $\mathrm{PSL}_2(\mathbb{F}_{p_i})$ is simple with order divisible by p_i and hence has no subgroups of index less than p_i. Thus, for i sufficiently large, the

restriction of τ_i to Γ_0 is surjective as well. It follows that the index d_i is equal to $p_i + 1$, as claimed.

The sequence d_{i+1}/d_i approaches 1. As we noted above, this is enough to prove Theorem 3.5 for the field $\mathbb{F}_q$. □

4. Curves with many points and large n-rank

In our proof of Theorem 1.1 we started with an ascensive sequence of curves with many points and used double covers to produce curves of every sufficiently large genus with many points. In this section we will use the same basic method to prove Theorem 1.3: We will start with an ascensive sequence of curves with many points and large n-rank, and use double covers to produce curves with the same properties in every sufficiently large genus.

Let us begin by introducing some notation. Suppose $\mathcal{C} = \{C_0, C_1, \dots\}$ is an ascensive sequence of curves over $\mathbb{F}_q$. We define $\rho_n(\mathcal{C})$ (for every integer $n > 1$) and $\beta(\mathcal{C})$ by

$$\rho_n(\mathcal{C}) := \liminf_{i\to\infty} \frac{r_n(C_i)}{g(C_{i+1})} \qquad \text{and} \qquad \beta(\mathcal{C}) := \liminf_{i\to\infty} \frac{g(C_i)}{g(C_{i+1})}.$$

Note that in each expression we are dividing an invariant of one curve in the sequence by the genus of the next.

We will prove two lemmas. The first shows how we can obtain ascensive sequences having positive values of ρ_n.

Lemma 4.1. *Suppose $\mathcal{C}$ is an ascensive sequence over $\mathbb{F}_q$. Then for every integer $n > 1$ there is an ascensive sequence $\mathcal{C}_n$ over $\mathbb{F}_q$ such that*

$$\gamma(\mathcal{C}_n) \geq \frac{\min(\gamma(\mathcal{C}), \beta(\mathcal{C}))}{7n} \qquad \textit{and} \qquad \rho_n(\mathcal{C}_n) \geq \frac{\min(\gamma(\mathcal{C}), \beta(\mathcal{C}))}{7n}.$$

The second lemma shows how we can get curves with many points and large n-rank from the sequences produced by Lemma 4.1.

Lemma 4.2. *Suppose $\mathcal{C}$ is an ascensive sequence over $\mathbb{F}_q$. Then for every $\varepsilon > 0$ the following statement holds: For every sufficiently large h there is a curve B of genus h such that*

$$\#B(\mathbb{F}_q) > (1-\varepsilon)\gamma(\mathcal{C})h/4 \qquad \textit{and} \qquad r_n(B) > (1-\varepsilon)\rho_n(\mathcal{C})h/4.$$

Our refined versions of Theorem 1.1 show that there is a constant c such that for every q there are ascensive sequences $\mathcal{C}$ over $\mathbb{F}_q$ with $\beta(\mathcal{C}) = 1$ and $\gamma(\mathcal{C}) > c$. To prove Theorem 1.3 we need merely apply Lemma 4.1 to such a $\mathcal{C}$ and then apply Lemma 4.2 to the resulting sequences $\mathcal{C}_n$.

Proof of Lemma 4.1. We may assume that $\mathcal{C} = \{C_0, C_1, \dots\}$ is an ascensive sequence over $\mathbb{F}_q$ with $\gamma(\mathcal{C}) > 0$ and $\beta(\mathcal{C}) > 0$. By eliminating a finite number of terms from $\mathcal{C}$, if necessary, we may assume that $g(C_i) > 1$ and $\#C_i(\mathbb{F}_q) > 0$ for all i. Now suppose we are given a positive integer n. Our goal is to define a sequence $\mathcal{C}_n = \{B_0, B_1, \dots\}$ satisfying the conclusions of the lemma. For every i, we define B_i as follows.

Let $g = g(C_i)$, let $d = \min(\#C_i(\mathbb{F}_q), g)$, and let S be a subset of $C_i(\mathbb{F}_q)$ with $\#S = d$. Let Q be a place of C_i of degree $2g+1$; such a place exists by Lemma 2.1(ii). The Riemann-Roch theorem, applied to the divisor Q, shows that there is a function $f_Q \in \mathbb{F}_q(C_i)$ whose polar

divisor is Q. For every $P \in S$, Riemann-Roch applied to Q and $P+Q$ shows that there is a function $f_P \in \mathbb{F}_q(C_i)$ with simple poles at P and Q and no other poles. Let

$$f := \sum_{P \in S} f_P,$$

and if f has no pole at Q then replace f with $f + f_Q$. Then f is a function of degree $d+2g+1$ with a simple pole at every $P \in S$.

Write $n = p^e r$ where p is the characteristic of $\mathbb{F}_q$ and $(r, q) = 1$. Let B' be the curve obtained by adjoining a root of $y^r = f$ to $\mathbb{F}_q(C_i)$. If $e = 0$, let $B_i = B'$; otherwise let B_i be the curve obtained by adjoining a root of $z^{p^e} - z = f$ to $\mathbb{F}_q(B')$. We note several facts about the curve B_i: First, if we apply the Hurwitz formula to the covers $B' \to C_i$ and $B_i \to B'$ (the formulas from [25, Cor. III.7.4] and [25, Prop. III.7.10(e)] are helpful here) and apply some easy estimates that depend on the fact that $d \le g$, we find that $g(B_i) < 7ng$. Second, the cover $B_i \to C_i$ is totally ramified at every point in S, so $\#B_i(\mathbb{F}_q) \ge d$. Third, we have $r_n(B_i) \ge d - 2$, as the following argument shows.

Let π be the natural map from B' to C_i. Let G denote the group of degree-zero divisors of B' supported on $S' := \pi^{-1}(S)$, and let G_0 be the subgroup of G consisting of those degree-zero divisors D with $\operatorname{ord}_P D \equiv \operatorname{ord}_{P'} D \pmod r$ for every $P, P' \in S'$. Note that G is a free abelian group of rank $d-1$, that $G_0 \supseteq rG$, and that G_0/rG is naturally isomorphic to a subgroup of $\mathbb{Z}/r\mathbb{Z}$.

We claim that the kernel of the natural map

$$G \to (\operatorname{Jac} B')(\mathbb{F}_q)/\pi^*((\operatorname{Jac} C_i)(\mathbb{F}_q))$$

contains rG and is contained in G_0. Clearly rG is in the kernel, since if $D \in G$ we have $rD = \pi^*\pi_* D$. On the other hand, suppose that $D \in G$ is in the kernel. Then $D = (h) + \pi^* E$ for some $h \in \mathbb{F}_q(B')$ and divisor E on C_i. The function h is preserved up to scalar multiple by the action of $\operatorname{Gal}(B'/C_i)$ (by which we mean the Galois group of the covering of curves over $\overline{\mathbb{F}}_q$), and writing h in terms of the basis $1, y, \dots, y^{r-1}$ shows that $h \in y^j \mathbb{F}_q(C_i)^*$ for some j. It follows that the multiplicities of the points of S' in D are all congruent to each other modulo r, so D is contained in G_0. This proves the claim.

It follows from the previous paragraph that the image of G in the quotient group

$$(\operatorname{Jac} B')(\mathbb{F}_q)/\pi^*((\operatorname{Jac} C_i)(\mathbb{F}_q))$$

contains $(\mathbb{Z}/r\mathbb{Z})^{d-2}$. Group theory then shows that $(\operatorname{Jac} B')(\mathbb{F}_q)$ also contains $(\mathbb{Z}/r\mathbb{Z})^{d-2}$. But since the natural map $B_i \to B'$ has degree coprime to r, the kernel of the natural map $\operatorname{Jac} B' \to \operatorname{Jac} B_i$ has order coprime to r, so $(\operatorname{Jac} B_i)(\mathbb{F}_q)$ also contains a copy of $(\mathbb{Z}/r\mathbb{Z})^{d-2}$.

The same proof shows that $(\operatorname{Jac} B_i)(\mathbb{F}_q)$ contains $(\mathbb{Z}/p^e\mathbb{Z})^{d-2}$. (The only difference in the argument is that now when the action of $\operatorname{Gal}(B_i/B')$ on the analogous h is by scalar multiples, the scalars must be p^e-th roots of 1, hence equal to 1, so h comes from $\mathbb{F}_q(B')$.) Combining this with the previous paragraph and applying the Chinese Remainder Theorem, we find $r_n(B_i) \ge d - 2$, as we had noted above.

Combining the several facts we have noted about the curve B_i, we find that for every $i \ge 0$ we have

$$\frac{\#B_i(\mathbb{F}_q)}{g(B_{i+1})} > \frac{\min(\#C_i(\mathbb{F}_q), g(C_i))}{7ng(C_{i+1})} \qquad \text{and} \qquad \frac{r_n(B_i)}{g(B_{i+1})} > \frac{-2 + \min(\#C_i(\mathbb{F}_q), g(C_i))}{7ng(C_{i+1})}.$$

It follows that

$$\gamma(\mathcal{C}_n) \geq \frac{\min(\gamma(\mathcal{C}), \beta(\mathcal{C}))}{7n} \qquad \text{and} \qquad \rho_n(\mathcal{C}_n) \geq \frac{\min(\gamma(\mathcal{C}), \beta(\mathcal{C}))}{7n}.$$

□

The proof of the second lemma is almost identical to the proof of Proposition 3.3.

Proof of Lemma 4.2. Suppose we are given an ascensive sequence $\mathcal{C} = \{C_0, C_1, \dots\}$ and an $\varepsilon > 0$ as in the statement of the lemma. We may certainly assume that $\varepsilon < 1$. Then there is an integer j such that for all $i > j$ we have

$$\#C_i(\mathbb{F}_q) \geq (1-\varepsilon)\gamma(\mathcal{C})g(C_{i+1}) \qquad \text{and} \qquad r_n(C_i) \geq (1-\varepsilon)\rho_n(\mathcal{C})g(C_{i+1}).$$

Now suppose we are given an integer $h \geq 4g(C_{j+1})$. Let i be the largest integer such that $h \geq 4g(C_i)$. Proposition 1.4 shows that there is a curve B of genus h that is a double cover of C_i. By replacing B with its quadratic twist over C_i, if necessary, we may assume that $\#B(\mathbb{F}_q) \geq \#C_i(\mathbb{F}_q)$. Also, the Hurwitz formula shows that the double cover $B \to C_i$ must be totally ramified at some point, so class field theory for curves shows that the natural map $(\operatorname{Jac} B)(\mathbb{F}_q) \to (\operatorname{Jac} C_i)(\mathbb{F}_q)$ is surjective. It follows that $r_n(B) \geq r_n(C_i)$. Since we also have $h < 4g(C_{i+1})$, we find that

$$\#B(\mathbb{F}_q) \geq \#C_i(\mathbb{F}_q) \geq (1-\varepsilon)\gamma(\mathcal{C})g(C_{i+1}) > (1-\varepsilon)\gamma(\mathcal{C})h/4.$$

Similarly, we have

$$r_n(B) \geq r_n(C_i) \geq (1-\varepsilon)\rho_n(\mathcal{C})g(C_{i+1}) > (1-\varepsilon)\rho_n(\mathcal{C})h/4,$$

as we were to show. □

Remark. The reader who objects to the intrusion of class field theory into the proof of Lemma 4.2 can remove it at the expense of slightly weakening the lemma. Consider the double cover $\pi\colon B \to C_i$ introduced at the end of the proof. We have $\pi_*\pi^* = 2$ on $\operatorname{Jac} C_i$, so $r_n(B) \geq r_{2n}(C_i)$. Thus, *without* class field theory, we can show that for every sufficiently large h there is a curve B of genus h such that $\#B(\mathbb{F}_q) > (1-\varepsilon)\gamma(\mathcal{C})h/4$ and $r_n(B) > (1-\varepsilon)\rho_{2n}(\mathcal{C})h/4$.

Theorem 1.3 has the following consequence for class field towers:

Proposition 4.3. *Fix a prime power q and a prime ℓ. For $g \gg 0$, there exists a genus-g curve C over $\mathbb{F}_q$ with $P \in C(\mathbb{F}_q)$ such that the $(\{P\}, \ell)$-class field tower of $\mathbb{F}_q(C)$ is infinite.*

Proof. Suppose g is at least $5\ell/c$, where c is the constant that appears in Theorem 1.3. Then Theorem 1.3 shows that there is a genus-g curve C over $\mathbb{F}_q$ whose n-rank is greater than 5 and that has at least 5 rational points. Pick $P \in C(\mathbb{F}_q)$ and embed C in its Jacobian J using P as the base point. Let $F \in \operatorname{End} J$ be the q-power Frobenius endomorphism and let D be the inverse image of C under $(1-F)\colon J \to J$. Class field theory for curves shows that D is an irreducible curve and that $D \to C$ is a unramified Galois covering with Galois group $J(\mathbb{F}_q)$, and clearly P splits completely in this covering. By Galois theory, there exists a subcovering $E \to C$ with Galois group $(\mathbb{Z}/\ell\mathbb{Z})^r$, where $r = r_n(C) > 5$. The function field analogue of the Golod-Shafarevich criterion (the lemma in our appendix, with $S = \{P\}$) implies that the $(\{P\}, \ell)$-class field tower of $\mathbb{F}_q(C)$ is infinite. □

5. Quantitative refinements

Our arguments in Section 3 required asymptotic results about special sequences of curves, but the tool we applied to these results — Proposition 1.4 — makes no use of any special properties these curves might have. Indeed, the proposition makes reference only to the genera of the curves it mentions. In this section we will show that we can produce better bounds on $A^-(q)$ by replacing Proposition 1.4 with sharper asymptotic results. At the end of this section we prove Theorem 1.2.

5.1. **Bounding data.** Let $\mathcal{C} = \{C_0, C_1, \dots\}$ be an ascensive sequence of curves over $\mathbb{F}_q$ and let H and M be real numbers. We will say that the pair (H, M) is *bounding data for* $\mathcal{C}$ (*over* $\mathbb{F}_q$) if for every $\varepsilon > 0$ there is an L_ε such that following statement holds:

> If $i > L_\varepsilon$ and h is an integer with $h > (H+\varepsilon)g(C_i)$, then there exists a genus-h curve B over $\mathbb{F}_q$ such that $\#B(\mathbb{F}_q) \geq (M-\varepsilon)\#C_i(\mathbb{F}_q)$.

Bounding data for a sequence $\mathcal{C}$ can be used to give a lower bound on $A^-(\mathcal{C})$, as the following proposition shows.

Proposition 5.1. *If (H, M) is bounding data for an ascensive sequence $\mathcal{C}$ over $\mathbb{F}_q$, then $A^-(q) \geq \gamma(\mathcal{C}) \cdot M/H$.*

Proof. This is a generalization of Proposition 3.3, and the proof is essentially identical to the proof of that result. Indeed, Proposition 3.3 amounts to the observation that $(4, 1)$ is bounding data for every ascensive $\mathcal{C}$, which follows from Proposition 1.4. □

5.2. **Improved bounds on $A^-(q)$ for square q.** In this section we will prove Theorem 1.2 by showing that every ascensive sequence over $\mathbb{F}_q$ has bounding data of the form $(H, 1)$ for an appropriate value of H. To show that $(H, 1)$ is bounding data for $\mathcal{C}$, we must show that for every $\varepsilon > 0$, for every sufficiently large i, if $h > (H+\varepsilon)g(C_i)$ then there is a genus-h curve B with $\#B(\mathbb{F}_q) \geq (1-\varepsilon)\#C_i(\mathbb{F}_q)$. In this section we will restrict ourselves to the case where B is a degree-2 cover of C_i. This restriction entails that $h \geq 2g(C_i) - 1$, so this line of argument cannot possibly work for values of H less than 2.

If $\mathcal{C} = \{C_0, C_1, \dots\}$ is an ascensive sequence over $\mathbb{F}_q$, define

$$R_2(\mathcal{C}) := \limsup_{i\to\infty} \frac{r_2(C_i)}{g(C_i)},$$

where, as before, $r_2(C_i)$ denotes the 2-rank of $(\operatorname{Jac} C_i)(\mathbb{F}_q)$. (Note that we are dividing the 2-rank of each curve in the sequence by *its own* genus, and *not* the genus of the next curve!) Also define

$$H_{\mathcal{C}} := 2 + R_2(\mathcal{C})\frac{\log 2}{\log q}.$$

Proposition 5.2. *If $\mathcal{C}$ is an ascensive sequence over $\mathbb{F}_q$ then $(H_{\mathcal{C}}, 1)$ is bounding data for $\mathcal{C}$.*

Proof. Our proof depends on the parity of q. First suppose that q is odd. Let C be a genus-g curve over $\mathbb{F}_q$. Let J be the Jacobian of C. Let $j = \#(J(\mathbb{F}_q)/2J(\mathbb{F}_q))$. Lemma 2.1(iv) shows that if $g \geq 900$ and $d \geq \log_q(j \log j + 1) + \sqrt{g}$, then $n_d(C) > j$. Since $\log j \leq \log(2^{2g}) = O(g)$, the condition on d can be rewritten as

$$d \geq \log_q j + o(g) = r_2(C)\frac{\log 2}{\log q} + o(g)$$

as $g \to \infty$. Proposition 5.2 (for odd q) follows by applying the argument in the final paragraph of the proof of Proposition 1.4.

Now suppose q is even. Fix a curve $C/\mathbb{F}_q$ of genus g and let d be an arbitrary integer with $d \geq d(C)$, where

$$d(C) := \max\left(r_2(C)\frac{\log 2}{\log q}, \frac{2\log(6g+3)}{\log q}\right).$$

We see from Lemma 2.1(i) that C has a place of degree d, and it follows from Lemma 5.3 (below) that there exists a degree-2 cover $B \to C$ with $g(B) = 2g + d - 1$. As C ranges through the curves in $\mathcal{C}$, we have

$$\limsup \frac{d(C)}{g(C)} = R_2(\mathcal{C})\frac{\log 2}{\log q}.$$

□

Lemma 5.3. *Let q be a power of 2, and let C be a curve over $\mathbb{F}_q$. Suppose C has a place of degree d, where $q^d \geq J[2](\mathbb{F}_q)$. Then there exists a degree-2 cover $B \to C$ such that $g(B) = 2g(C) + d - 1$.*

Proof. Let $\mathfrak{p}$ be a place of degree d on C and let P be a geometric point of C lying in $\mathfrak{p}$, so that $\mathfrak{p}$ consists of the d conjugates of P. Let u be a uniformizing parameter at P. For every integer $m \geq 0$ let S_m be the additive group of functions in $\mathbb{F}_q(C)$ that have no poles outside $\mathfrak{p}$ and whose polar expansions at P are of the form

$$c_m u^{-2^m} + c_{m-1}u^{-2^{m-1}} + \cdots + c_1 u^{-2} + c_0 u^{-1},$$

where the c_i are elements of $\overline{\mathbb{F}}_q$ and where c_m is not necessarily nonzero. A standard Riemann-Roch argument shows that S_m contains nonconstant functions when $m \gg 0$, and in fact it is not hard to see that $\#S_m = q^d \# S_{m-1}$ for $m \gg 0$. For $m > 0$ let $T_m \subseteq S_m$ be the subgroup

$$T_m := \{g^2 + g + c : g \in S_{m-1}, c \in \mathbb{F}_q\}.$$

Then $\#T_m = \#S_{m-1}$, so for $m \gg 0$ we have $\#(S_m/T_m) = q^d$.

Artin-Schreier theory shows the following:

1. If $f \in S_m \setminus T_m$ then the degree-2 cover of C obtained by adjoining a root of $y^2 - y - f$ to $\mathbb{F}_q(C)$ is geometrically irreducible and is ramified at most at $\mathfrak{p}$.
2. If $f, g \in S_m \setminus T_m$ then the degree-2 covers obtained as in (1) from f and g are geometrically isomorphic (as curves *equipped with their maps to C*) if and only if $f - g \in T_m$.

Thus, from the set S_m we obtain $-1 + \#(S_m/T_m)$ geometrically nonisomorphic irreducible degree-2 covers of C. By taking m large enough, we find that there are at least $q^d - 1$ such covers. But the number of geometrically distinct *unramified* degree-2 covers of C is equal to $\#J[2](\mathbb{F}_q) - 1$, so there must be a *ramified* degree-2 cover $B \to C$ over $\mathbb{F}_q$ coming from S_m, and it must be ramified exactly at $\mathfrak{p}$. The Hurwitz formula then shows that $g(B) = 2g(C) + d - 1$. □

Proof of Theorem 1.2. We showed in Section 3.3 that for every square q there exists an ascensive sequence $\mathcal{C}$ of curves over $\mathbb{F}_q$ with $\gamma(\mathcal{C}) = \sqrt{q} - 1$. In light of Propositions 5.1 and 5.2, to prove Theorem 1.2 it will be enough for us to show that

$$R_2(\mathcal{C}) \leq \begin{cases} 1 & \text{when } q \text{ is even;} \\ 2 & \text{when } q \text{ is odd.} \end{cases}$$

But these inequalities follow from the fact that for every curve C over $\mathbb{F}_q$ we have

$$r_2(C) \leq \begin{cases} g(C) & \text{when } q \text{ is even;} \\ 2g(C) & \text{when } q \text{ is odd.} \end{cases}$$

□

6. Variants of our argument

Section 3 gave a lower bound on $A^-(q)$ in terms of the value of $\gamma(\mathcal{C})$ of an ascensive sequence. Section 5.1 gave an improved bound taking into account also the size of q, but the full power of Proposition 5.2 was not used, because we used only the trivial upper bound on $R_2(\mathcal{C})$. It would be extremely interesting to obtain better bounds on $R_2(\mathcal{C})$ when $\mathcal{C}$ is one of the sequences of modular curves or Shimura curves used in Section 3.3. Ideally, one would like to show that $R_2(\mathcal{C}) = 0$ for such an ascensive sequence, so that $(2, 1)$ would be bounding data for $\mathcal{C}$. Theorem 1.3 shows, however, that $R_2(\mathcal{C})$ can be positive, even for sequences of curves with many points. Thus, proving that $R_2(\mathcal{C}) = 0$ for a sequence of Shimura curves would require using special properties of the curves.

It is possible to improve the $4g$ in Proposition 1.4 if we require only that the proposition apply to curves of sufficiently large genus. Indeed, the proof of Proposition 5.2 shows that we can replace the $4g$ with $(2 + (\log 2/\log q))g$ if q is even and with $(2 + (\log 4/\log q))g$ if q is odd. But the following argument limits the possible further improvements we might hope to obtain: Given m and q, there exists a curve C over $\mathbb{F}_q$ such that every place has degree at least m. (For instance, nonsingular plane curves with this property exist [18].) It then follows from Proposition 1.4 that such C exist in every sufficiently large genus. An argument similar to that proving Proposition 2.2 shows that such C do not admit degree-2 covers of any genus $h < 2g + 2m - 1$ except possibly for unramified degree-2 covers of genus $h = 2g - 1$. In particular, we cannot improve the $4g$ in Proposition 1.4 to $2g + s$ for any fixed constant s, even if we ask only that the proposition hold for $g \gg 0$. We do not know whether there always exists a cover of genus $2g + o(g)$.

It is conceivable that $A^-(q) = \sqrt{q} - 1$. In order to prove this using our methods, we would need an ascensive sequence $\mathcal{C}$ with $\gamma(\mathcal{C}) = \sqrt{q} - 1$ for which we could provide bounding data (H, M) with $H/M = 1$. But the smallest ratio H/M that we can possibly attain using degree-2 covers $B \to C$ is 2, unless we can make $M > 1$ by forcing *more* than half of the points in $C(\mathbb{F}_q)$ to split. For $q < 207$, it is in fact possible to show in this way that every ascensive sequence over $\mathbb{F}_q$ has bounding data (H, M) with $H/M < 2$; plugging this into Proposition 5.1 improves the lower bounds on $A^-(q)$. We give the argument below, beginning with the following variant of Proposition 1.4.

Proposition 6.1. *Let q be an odd prime power and let $m = (\log 2/\log q)(\sqrt{q} + 1)$. Fix a positive real ε. Then for all $g \gg 0$, if $C/\mathbb{F}_q$ is a curve of genus g, and if h is an integer with $h \geq (2 + m + \varepsilon)g$, then there exists a genus-h curve $B/\mathbb{F}_q$ that admits a degree-2 covering map $B \to C$ in which every rational place of C splits.*

Proof. Let $d = h - 2g + 1 > (m + \varepsilon)g$. Thus $d > 1$ when $g \gg 0$. As in the proof of Proposition 1.4, let T_d denote the set of places on C of degree d. By Lemma 2.1(i), we have $\#T_d \geq q^d/(2d)$ when $g \gg 0$. Thus $g \gg 0$ implies $\#T_d \geq q^{(m+\varepsilon/2)g}$. Consider the map $T_d \to J(\mathbb{F}_q)/2J(\mathbb{F}_q)$ defined by $P \mapsto [P - P_0]$, where P_0 is any fixed degree-d divisor on C. Since $\#J(\mathbb{F}_q)/2J(\mathbb{F}_q) \leq 2^{2g}$, there exists $x \in J(\mathbb{F}_q)/2J(\mathbb{F}_q)$ having at least

$q^{(m+\varepsilon/2)g}/2^{2g}$ preimages in T_d. Fix one of these preimages P_1. Then for each preimage P of x, fix $f_P \in \mathbb{F}_q(C)$ having divisor $P - P_1 + 2D$ for some D.

Let $K = \mathbb{F}_q(C)$. For each $Q \in C(\mathbb{F}_q)$, let K_Q be the completion of K at Q, and let $\mathcal{O}_Q \subset K_Q$ be the valuation ring. Since $d > 1$, f_P has even valuation at each $Q \in C(\mathbb{F}_q)$. Hence the f_P map into the group

$$S := \prod_{Q \in C(\mathbb{F}_q)} \frac{\mathcal{O}_Q^* K_Q^{*2}}{K_Q^{*2}}$$

of order $2^{\#C(\mathbb{F}_q)}$. The Drinfel'd-Vlăduţ bound gives $\#C(\mathbb{F}_q) < (\sqrt{q} - 1 + \varepsilon/2)g$ for $g \gg 0$, but then the definition of m implies

$$\frac{q^{(m+\varepsilon/2)g}}{2^{2g}} > 2^{(\sqrt{q}-1+\varepsilon/2)g} > \#S,$$

so there exist distinct $P, P' \in T_d$ in the preimage of x such that f_P and $f_{P'}$ have the same image in S. Let $e = f_P/f_{P'}$.

Let B be the curve with $\mathbb{F}_q(B) \simeq \mathbb{F}_q(C)(\sqrt{e})$. The divisor of e has the form $P - P' + 2D$ with $P, P' \in T_d$, so Hurwitz shows that B has genus h. By construction, $e \in K_Q^{*2}$ for all $Q \in C(\mathbb{F}_q)$, so every rational point of C splits in the degree-2 cover $B \to C$. □

Corollary 6.2. *Let q be an odd prime power and let $m = (\log 2/\log q)(\sqrt{q} + 1)$. Let $\mathcal{C}$ be an ascensive sequence over $\mathbb{F}_q$. Then $A^-(q) \geq \gamma(\mathcal{C})/(1 + m/2)$.*

Proof. Proposition 6.1 shows that $\mathcal{C}$ has bounding data $(2+m, 2)$. Now apply Proposition 5.1. □

We have $1 + m/2 < 2$ for all odd prime powers $q < 207$, and $1 + m/2 < 2 + \log 4/\log q$ (the trivial upper bound on $H_{\mathcal{C}}$) for all odd prime powers $q < 417$. We showed in Section 3.3 that, for every square q, there are ascensive sequences $\mathcal{C}$ over $\mathbb{F}_q$ with $\gamma(\mathcal{C}) = \sqrt{q} - 1$. Thus, for odd square q we have $A^-(q) \geq (\sqrt{q} - 1)/(1 + m/2)$, which improves the bound in Theorem 1.2 if $q < 417$. For example, if $q = 9$ then $1 + m/2 < 1.631$, and the ascensive sequence $\{X_0(\ell)\}$ over $\mathbb{F}_9$ gives $A^-(9) > A^+(9)/1.631 = (\sqrt{9} - 1)/1.631 > 1.226$.

Appendix: class field towers

In this appendix we present a version of Serre's proof that $A^+(q) > 0$ for all q. Previously Serre's proof has appeared only in the unpublished lecture notes [22]. The version below uses an idea from [15] at one step to simplify the argument.

As in Section 3.2, it suffices to show that for every q there is a curve C over $\mathbb{F}_q$ of genus $g > 1$ such that for some nonempty set S of rational places on $\mathbb{F}_q(C)$, the $(S, 2)$-class field tower of $\mathbb{F}_q(C)$ is infinite. To do this, we use a function field analogue of the Golod-Shafarevich criterion:

Lemma. *Let C be a curve over $\mathbb{F}_q$, let ℓ be a prime number, and let S be a nonempty set of rational places of $\mathbb{F}_q(C)$. Suppose there is an unramified Galois extension $F/\mathbb{F}_q(C)$, with Galois group $(\mathbb{Z}/\ell\mathbb{Z})^r$, such that every place in S splits completely into $\mathbb{F}_q$-rational places of F. If $r \geq 2$ and*

$$\frac{(r-2)^2}{4} \geq \begin{cases} 1 + \#S & \text{if } \ell \mid (q-1); \\ \#S & \text{otherwise,} \end{cases}$$

then the (S, ℓ)-class field tower of $\mathbb{F}_q(C)$ is infinite.

Proof. See [19]. □

Theorem (Serre)**.** *We have $A^+(q) > 0$ for all prime powers q. In fact, there exists $c > 0$ such that $A^+(q) > c \log q$ for all q.*

Proof. First suppose q is odd. Let $f = f_1 f_2 \dots f_6$, where $f_1, f_2, \dots, f_6$ are distinct monic irreducible polynomials in $\mathbb{F}_q[x]$ having even degrees. Then $\mathbb{F}_q(x, \sqrt{f_1}, \dots, \sqrt{f_6})$ is an unramified Galois extension of $\mathbb{F}_q(x, \sqrt{f})$, with Galois group $(\mathbb{Z}/2\mathbb{Z})^5$, in which both places of $\mathbb{F}_q(x, \sqrt{f})$ which contain $1/x$ are completely split. It follows that $A^+(q) > 0$.

For odd q it remains only to prove the second statement for $q \gg 0$. Let $\alpha_1, \dots, \alpha_{r+1}$ be distinct elements of $\mathbb{F}_q$, and let $f(x) = (x - \alpha_1) \dots (x - \alpha_{r+1})$. Suppose r is even. Then $F := \mathbb{F}_q(\sqrt{x - \alpha_1}, \dots, \sqrt{x - \alpha_{r+1}})$ is an unramified Galois extension of $\mathbb{F}_q(x, \sqrt{f})$, with Galois group $(\mathbb{Z}/2\mathbb{Z})^r$. By Hurwitz, $\mathbb{F}_q(x, \sqrt{f})$ has genus $g := r/2$ and F has genus $1 + 2^r(r/2 - 1)$. By the Weil lower bound, the number of rational places N on F satisfies

$$N \geq q + 1 - 2\sqrt{q} \cdot 2^r(r/2 - 1).$$

Exactly $N/2^r$ rational places of $\mathbb{F}_q(x, \sqrt{f})$ split completely in F. Choose r as the even integer nearest $(\log_2 q)/3$. For $q \gg 0$, we have $r \geq 4$ and $N/2^r \geq (r-2)^2/4 - 1 \geq 0$, so it is possible to choose a subset S of these rational places with $\#S = \lfloor (r-2)^2/4 - 1 \rfloor$. By the lemma, the $(S, 2)$-class field tower is infinite, so a proof similar to that of Lemma 3.4 shows that

$$A^+(q) \geq \frac{\#S}{g - 1} = \frac{r}{2} + O(1) = c' \log q + O(1)$$

as $q \to \infty$, for some $c' > 0$.

The case of even q can be treated in a completely analogous manner, using Artin-Schreier covers. □

The proof of the theorem shows that there exists $c > 0$ such that for every q, there exists a curve C over $\mathbb{F}_q$ with $g(C) > 1$ and a set S of rational places on $\mathbb{F}_q(C)$ such that $\#S > (c \log q) \cdot (g(C) - 1)$ and such that the $(S, 2)$-class field tower of $\mathbb{F}_q(C)$ is infinite. As in Section 3.2, it follows that for every q we have $A^-(q) \geq (c/4) \log q$. We do not know whether this bound can be improved significantly when q is prime.

References

[1] J. Csirik, J. Wetherell, and M. Zieve, *On the genera of $X_0(N)$*, J. Number Theory (to appear). arXiv:math.NT/0006096.

[2] V. G. Drinfel'd and S. G. Vlăduţ, *The number of points of an algebraic curve*, Funktsional. Anal. i Prilozhen. **17** (1983), 68–69. [Funct. Anal. Appl. **17** (1983), 53–54.]

[3] N. D. Elkies, *Explicit modular towers*, in: Proceedings of the Thirty-Fifth [1997] Annual Allerton Conference on Communication, Control and Computing (T. Başar and A. Vardy, eds.), Univ. of Illinois at Urbana-Champaign, 1998, 23–32.

[4] N. D. Elkies, *Explicit towers of Drinfeld modular curves*, in: European Congress of Mathematics (Barcelona, 2000), Vol. II (C. Casacuberta et al., eds.), Birkhauser, Basel, 2001, 189–198. arXiv:math.NT/0005140.

[5] A. Garcia and H. Stichtenoth, *A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound*, Invent. Math. **121** (1995), 211–222.

[6] A. Garcia and H. Stichtenoth, *On the asymptotic behavior of some towers of function fields over finite fields*, J. Number Theory **61** (1996), 248–273.

[7] A. Garcia, H. Stichtenoth, and M. Thomas, *On towers and composita of towers of function fields over finite fields*, Finite Fields Appl. **3** (1997), 257–274.
[8] Y. Ihara, *Algebraic curves mod* $\mathfrak{p}$ *and arithmetic groups*, in: Algebraic Groups and Discontinuous Subgroups (A. Borel and G. D. Mostow, eds.), American Mathematical Society, Providence, 1966, 265–271.
[9] Y. Ihara, On Congruence Monodromy Problems. Vol. 2, Department of Mathematics, University of Tokyo, 1969.
[10] Y. Ihara, *On modular curves over finite fields*, in: Discrete Subgroups of Lie Groups and Applications to Moduli (Internat. Colloq., Bombay, 1973) Oxford Univ. Press, Bombay, 1975, 161–202.
[11] Y. Ihara, *Congruence relations and Shimūra curves*, in: Automorphic Forms, Representations, and L-functions. Part 2 (A. Borel and W. Casselman, eds.), American Mathematical Society, Providence, 1979, 291–311.
[12] 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.
[13] Y. Ihara, *Shimura curves over finite fields and their rational points*, in: Applications of Curves over Finite Fields (M. Fried, ed.), American Mathematical Society, Providence, 1999, 15–23.
[14] A. Kresch, J. Wetherell, and M. Zieve, *Curves of every genus with many points, I: Abelian and toric families*, J. Algebra **250** (2002), 353–370. arXiv:math.AG/9912069.
[15] W.-C. W. Li and H. Maharaj, *Coverings of curves with asymptotically many rational points*, J. Number Theory (to appear). arXiv:math.NT/9908152.
[16] Y. I. Manin, *What is the maximum number of points on a curve over* $\mathbb{F}_2$?, J. Fac. Sci. Univ. Tokyo **28** (1981), 715–720.
[17] Y. Morita, *Reduction modulo* $\mathfrak{P}$ *of Shimura curves*, Hokkaido Math. J. **10** (1981), 209–238.
[18] B. Poonen, *Bertini theorems over finite fields*, arXiv:math.AG/0204002.
[19] R. Schoof, *Algebraic curves over* $\mathbb{F}_2$ *with many rational points*, J. Number Theory **41** (1992), 6–14.
[20] J.-P. Serre, *Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini*, C. R. Acad. Sci. Paris **296** (1983), 397–402; = Œuvres [128].
[21] J.-P. Serre, *Nombres de points des courbes algébriques sur* $\mathbb{F}_q$, Sém. Théor. Nombres Bordeaux (1982–1983), exp. 22; = Œuvres [129].
[22] J.-P. Serre, *Rational points on curves over finite fields*, unpublished lecture notes by F. Q. Gouvêa, Harvard University, 1985.
[23] G. Shimura, *Arithmetic of unitary groups*, Ann. of Math. (2) **79** (1964), 369–409.
[24] G. Shimura, *On canonical models of arithmetic quotients of bounded symmetric domains*, Ann. of Math. (2) **91** (1970), 144–222.
[25] H. Stichtenoth, Algebraic Function Fields and Codes, Springer Verlag, Berlin, 1993.
[26] A. Weil, Variétés abéliennes et courbes algébriques, Hermann, Paris, 1948.
[27] Th. Zink, *Degeneration of Shimura surfaces and a problem in coding theory*, in: Fundamentals of Computation Theory (L. Budach, ed.), Springer-Verlag, New York, 1985, 503–511.

Department of Mathematics, Harvard University, Cambridge, MA 02138–2901
E-mail address: elkies@math.harvard.edu

Center for Communications Research, 4320 Westerra Court, San Diego, CA 92121–1967
E-mail address: however@alumni.caltech.edu

Department of Mathematics, University of Pennsylvania, Philadelphia, PA 19104–6395
E-mail address: kresch@math.upenn.edu

Department of Mathematics, University of California, Berkeley, CA 94720–3840
E-mail address: poonen@math.berkeley.edu

Department of Mathematics, University of Southern California, Los Angeles, CA 90089–1113
Current address: Center for Communications Research, 4320 Westerra Court, San Diego, CA 92121–1967
E-mail address: jlwether@alum.mit.edu

Center for Communications Research, 805 Bunn Drive, Princeton, NJ 08540
E-mail address: zieve@idaccr.org