JOURNAL OF NUMBER THEORY 41, 6–14 (1992)

Algebraic Curves over $\mathbf{F}_2$ with Many Rational Points

RENÉ SCHOOF

Dipartimento di Matematica, Università degli Studi di Trento, I-38050 Povo (Trento) Italy

Communicated by D. Goss

Received November 15, 1990; revised May 29, 1991

A smooth, projective, absolutely irreducible curve of genus 19 over $\mathbf{F}_2$ admitting an infinite S-class field tower is presented. Here S is a set of four $\mathbf{F}_2$-rational points on the curve. This is shown to imply that $A(2) = \limsup \#X(\mathbf{F}_2)/g(X) \geqslant 4/(19-1) \approx 0.222$. Here the limit is taken over curves X over $\mathbf{F}_2$ of genus $g(X) \to \infty$. © 1992 Academic Press, Inc.

1. INTRODUCTION

Let q be a power of a prime p and let $\mathbf{F}_q$ denote a field with q elements. André Weil [15] showed that for a smooth projective absolutely irreducible curve X of genus g over $\mathbf{F}_q$ the cardinality of the set $X(\mathbf{F}_q)$ satisfies

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

When the genus g of X is small with respect to q, this inequality says that the number of $\mathbf{F}_q$-rational points of X is approximately $q+1$, the number of $\mathbf{F}_q$-rational points on a projective line, with an error of the order $\sqrt{q}$. When g is very large, however, the situation is quite different [7]. In this case the interesting part of the inequality is

$$\#X(\mathbf{F}_q) \leqslant q + 1 + 2g\sqrt{q},$$

where, this time, the $2g\sqrt{q}$ term dominates. Following Ihara [6] we define

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

where the limit is taken over smooth, projective, absolutely irreducible curves X of genus g_X tending to ∞. Weil's result implies that

$$A(q) \leqslant 2\sqrt{q}.$$

0022-314X/92 $5.00

Copyright © 1992 by Academic Press, Inc.
All rights of reproduction in any form reserved.

Using Weil's estimate for finite extensions of $\mathbf{F}_q$ as well, Drinfeld and Vlădut [3, 12] showed that one has, in fact, the stronger estimate

$$A(q) \leqslant \sqrt{q} - 1.$$

For $q = 2$ this new bound is approximately 0.414, which is a dramatic improvement over $2\sqrt{2} \approx 2.82$ which follows from Weil's estimate.

The situation is not so satisfactory for lower bounds for $A(q)$. It was shown by Ihara [6] and Zink *et al.* [14] that the bound is sharp when q is a square:

$$A(q) = \sqrt{q} - 1 \qquad \text{for } q \text{ a square.}$$

Later Zink [16] showed that

$$A(p^3) \geqslant \frac{2(p^2-1)}{p+2} \qquad \text{for } p \text{ prime.}$$

Both these estimates were obtained by exhibiting a suitable family of "modular" curves. Using the modular interpretation one can count the rational points on the curves and establish a lower bound for $A(q)$.

Another method was employed by Serre [11–13]. He used infinite class field towers and showed that there exists a positive constant c for which

$$A(q) \geqslant c \log q \qquad \text{for all } q.$$

Using the same method Perret [8] obtained better lower bounds for $A(q^l)$ when q^l is a proper power of q. He showed, for instance, that for prime l and $q \equiv 1 \pmod{l}$ one has that

$$A(q^l) \geqslant \frac{\sqrt{l(q-1)} - 2l}{l-1}.$$

In this paper we study the case $q = 2$. This case is especially interesting because of the connections between algebraic curves over $\mathbf{F}_2$ and binary error-correcting codes. We already remarked that we have the upper bound $A(2) \leqslant \sqrt{2} - 1 \approx 0.414$. The main result of this paper is the following lower bound.

THEOREM 1.1. *One has*

$$A(2) \geqslant \tfrac{2}{9}.$$

The bound $\frac{2}{9} \approx 0.222$ is slightly better than the bound $\frac{8}{39}$ which appears in [11]. The present bound will also be established using an infinite class field tower of a suitable curve over $\mathbf{F}_2$. After I found this example I learned

that Serre had found in 1985 that $A(2) \geqslant \frac{2}{9}$. He had done so by means of an infinite class field tower as well. His example is different from mine.

In Section 2 we discuss infinite class field towers and show how they can be used to obtain lower bounds for $A(q)$. In Section 3 we exhibit one special tower by means of which Theorem 1.1 will be proved. For the cohomology theory and class field theory of curves that we will use we refer the reader to [1, 2, 9, 10].

2. Infinite Class Field Towers

In this section we discuss class field towers of function fields of curves over finite fields. The main result is Theorem 2.3: a sufficient criterion for a function field to have an infinite (l, S)-class field tower. The principal ingredients are class field theory and the following group theoretical result due to Golod and Shafarevič [4; 2, Chap. 9].

THEOREM 2.1. *Let l be a prime and let G be a non-trivial finite l-group that can be presented by means of d independent generators and r relations. Then one has that*

$$r > \tfrac{1}{4} d^2.$$

We recall that the number of independent generators d and the number of independent relations r of an l-group G can be given as dimensions of certain homology groups [2, Chap. 9],

$$\begin{aligned} d &= \dim_{\mathbf{F}_l} H_1(G, \mathbf{Z}/l\mathbf{Z}), \\ r &= \dim_{\mathbf{F}_l} H_2(G, \mathbf{Z}/l\mathbf{Z}). \end{aligned} \tag{1}$$

In order to explain how Theorem 2.1 is employed we introduce some notation. Let q be a power of a prime p and let $\mathbf{F}_q$ be a field with q elements. Let X be a smooth, projective, absolutely irreducible curve or "curve," for short, over $\mathbf{F}_q$. By K we denote its function field and by $\mathbf{A}_K$ its adèle ring. The idèle class group $\mathbf{A}_K^*/K^*$ is denoted by C_K.

Let S denote a non-empty set of *places* of X. Note that a "place" is not quite a point. It is a Galois conjugacy class of points. A place is called rational if it consists of one point only. This point is then necessarily defined over $\mathbf{F}_q$. For any S we let U_S denote the group of idèles that are units at all the places outside S. By means of the valuation maps at the places outside S we obtain an exact sequence

$$0 \to U_S \to \mathbf{A}_K^* \to \bigoplus_{v \notin S} \mathbf{Z} \to 0.$$

Here $\bigoplus_{v \notin S} \mathbf{Z}$ is called the *S-divisor group*. By O_S we denote the subring of functions of K that have no poles outisde S. The intersection of U_S and K^* is precisely O_S^*; it is called the group of *S-units*. By Dirichlet's Unit Theorem we have the following isomorphism of groups:

$$O_S^* \cong \mathbf{F}_q^* \times \mathbf{Z}^{\#S-1}.$$

Finally, we introduce the *S-divisor class group* Cl_S. It is the quotient of the S-divisor group by its subgroup P_S of principal divisors, i.e., by the subgroup of divisors of functions in K^*. All the groups we have defined so far fit into the following commutative diagram with exact rows and columns:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & O_S^* & \longrightarrow & K^* & \longrightarrow & P_S & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & U_S & \longrightarrow & \mathbf{A}_K^* & \longrightarrow & \bigoplus_{v \notin S} \mathbf{Z} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & U_S/O_S^* & \longrightarrow & C_K & \longrightarrow & Cl_S & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array} \tag{2}$$

Let $\bar{K}$ denote a fixed separable closure of K. The S-Hilbert class field H_S of K is defined to be the maximal abelian unramified extension of K inside $\bar{K}$ in which all places in S are totally split. It is known that H_S is a finite extension of K, its Galois group being isomorphic to the S-divisor class group Cl_S of X. One can now repeat this construction: put $K_1 = H_S$ and S_1 the collection of places of K_1 that lie over places in S. Let K_2 be the S_1-Hilbert class field of K_1, etcetera. In this way we obtain a sequence of fields

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots,$$

which is called the S-class field tower of K. The class field tower is called finite if the sequence stabilizes, i.e., when there is an index i such that $K_n = K_i$ for all $n \geqslant i$ and infinite otherwise.

To each field K_i in the tower there corresponds a smooth projective absolutely irreducible curve X_i over $\mathbf{F}_q$ with function field K_i and an unramified morphism $X_i \to X$. We will say that the curve X admits an

infinite S-class field tower when its function field K has an infinite S-class field tower.

We recall that $A(q) = \limsup_X \# X(\mathbf{F}_q)/g_X$, where the limit is taken over curves X over $\mathbf{F}_q$ with genus g_X tending to ∞. One can exploit infinite class field towers to obtain lower bounds for $A(q)$ as follows:

PROPOSITION 2.2. *Let X be a curve of genus $g > 1$ over $\mathbf{F}_q$ and let S be a non-empty set of rational places of X. If X admits an infinite S-class field tower, then*

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

Proof. Consider a curve X_i corresponding to a field K_i in the class field tower of the function field K of X. Since X_i is unramified over X the Hurwitz–Zeuthen formula [5, p. 301] for its genus g_i gives that

$$2g_i - 2 = [K_i : K](2g-2).$$

On the other hand, since all places are rational and totally split in X_i, we have that

$$\# X_i(\mathbf{F}_q) \geqslant \# S_i = [K_i : K] \# S.$$

Since the tower is infinite, we conclude that

$$A(q) \geqslant \lim \frac{\# S_i}{g_i} = \frac{\# S}{g-1},$$

as required.

Similarly, we consider for every prime l the (l, S)-*class field tower* of K. It is defined in an analogous way: The (l, S)-Hilbert class field $H_{S,l}$ of K is defined to be the maximal abelian unramified l-extension of K inside $\bar{K}$ in which all places in S are totally split. One can repeat this process as before and we obtain a sequence of fields

$$K = K_{0,l} \subset K_{1,l} \subset K_{2,l} \subset \cdots,$$

which we call the (l, S)-class field tower of K. The tower is called finite if the sequence stabilizes. In this case the Galois group of $\bigcup_i K_{i,l}$ over K is a finite l-group. It is easy to see that K admits an infinite S-class field tower once it admits an infinite (l, S)-class field tower for some prime l. The next theorem gives a sufficient condition for a curve to have an infinite (l, S)-class field tower.

For any abelian group A we denote by $d_l A$ the l-rank of A, the $\mathbf{F}_l$-dimension of $A \otimes \mathbf{Z}/l\mathbf{Z}$.

THEOREM 2.3. *Let X be a curve over $\mathbf{F}_q$ and let S be a set of places of X. Let l be a prime. If*

$$d_l Cl_S \geqslant 2 + 2\sqrt{d_l O_S^* + 1}$$

then X admits an infinite (l, S)-class field tower.

Proof. Suppose that the function field K of X has a *finite* (l, S)-class field tower. Let L denote the union of the fields in the tower; it is a Galois extension of K with Galois group G a finite l-group. Let d and r denote the minimal number of generators and relations, respectively, of G. From the long G-homology sequence of the exact sequence

$$0 \to \mathbf{Z} \to \mathbf{Z} \to \mathbf{Z}/l\mathbf{Z} \to 0$$

and (1) and (2) above we deduce that $d = d_l H_1(G, \mathbf{Z})$ and $r - d = d_l H_2(G, \mathbf{Z})$.

Since $H_1(G, \mathbf{Z})$ is isomorphic to the maximal abelian quotient $G/[G, G]$ of G, we conclude that

$$d = d_l Cl_S. \tag{3}$$

To compute the group $H_2(G, \mathbf{Z})$ we will use some class field theory [2]. We have

$$H_2(G, \mathbf{Z}) = \hat{H}^{-3}(G, \mathbf{Z}) \cong \hat{H}^{-1}(G, C_L).$$

Let T denote the set of places of L lying over S. Since L is unramified over K and since all places in S are totally split in L over K the module U_T is cohomologically trivial. Since L is at the *top* of the (l, S)-class field tower of K one has that Cl_T has order prime to l. Therefore it is a cohomologically trivial module as well. Looking at diagram (2) with L and T instead of K and S we conclude that

$$\hat{H}^{-1}(G, C_L) \cong \hat{H}^{-1}(G, U_T/O_T^*) \cong \hat{H}^0(G, O_T^*).$$

Since $\hat{H}^0(G, O_T^*)$ is a quotient of the group of S-units O_S^* we see that

$$r - d \leqslant d_l O_S^*. \tag{4}$$

It now follows from (3), (4), and Theorem 2.1 that $d_l Cl_S < 2 + 2\sqrt{d_l O_S^* + 1}$ and this implies the theorem at once.

In order to apply Theorem 2.3 it is necessary to have good lower bounds for the l-rank $d_l Cl_S$ of the S-divisor class group of X. These are provided by "genus theory."

PROPOSITION 2.4. *Let X be a curve over $\mathbf{F}_q$ and let S be a finite set of places of X. Suppose that the function field K of X is a cyclic extension of prime degree l of a field k and that S is stable under the action of the Galois group of K over k. Then*

$$d_l Cl_S \geqslant \rho - 1 - d_l O_{S'}^*.$$

Here S' denotes the set of places of k over which S lies and ρ denotes the number of places of k that are ramified in K.

Proof. Let $\Delta = \mathrm{Gal}(K/k)$. From the long Δ-cohomology sequences associated to diagram (2) we obtain

$$\begin{aligned} d_l Cl_S &\geqslant d_l \hat{H}^{-1}(\Delta, Cl_S) \geqslant d_l \hat{H}^0(\Delta, U_S/O_S^*) - d_l \hat{H}^0(\Delta, C_K) \\ &\geqslant d_l \hat{H}^0(\Delta, U_S) - d_l \hat{H}^0(\Delta, O_S^*) - d_l \hat{H}^0(\Delta, C_K). \end{aligned}$$

By global class field theory $\hat{H}^0(\Delta, C_K) \cong \hat{H}^{-2}(\Delta, \mathbf{Z}) \cong \Delta$ is cyclic of order l. By local class field theory $d_l \hat{H}^0(\Delta, U_S) \geqslant \rho$. From this the result follows easily.

3. AN EXAMPLE

In this section we exhibit a curve X over $\mathbf{F}_2$ and a set of rational points S on it such that X admits an infinite S-class field tower. As a result we can prove Theorem 1.1.

We start with $\mathbf{P}^1$, the projective line over $\mathbf{F}_2$. Its function field is just the field of rational functions $\mathbf{F}_2(T)$. There are three rational points which we will, according to the values of the function T, denote by 0, 1, and ∞. We will realize our curve X as a covering of degree 8 of $\mathbf{P}^1$. The set S will consist of the points of X lying over ∞. We will proceed in three steps.

First we consider two quadratic extensions of $\mathbf{F}_2(T)$: one of conductor $4(\infty)$ in which the points 0 and 1 are split and one of conductor $2(0)+2(1)$ in which the point over ∞ is split. We will call the corresponding smooth curves E and E', respectively. The Existence Theorem of class field theory implies that these quadratic extensions actually exist. We will discuss the extension of conductor $4(\infty)$ as an example.

Every abelian extension of $\mathbf{F}_2(T)$ of conductor dividing $4(\infty)$ has a Galois group a quotient of a certain group A which sits in an exact sequence [9]

$$0 \to (\mathbf{F}_2[u]/u^4\mathbf{F}_2[u])^* \to A \to \mathbf{Z} \to 0,$$

where $u = T^{-1}$ is a uniformizing element at ∞. An extension in which moreover the points 0 and 1 of $\mathbf{P}^1$ are split has its Galois group isomorphic

to A modulo the two *cyclic* inertia groups of 0 and 1. Since $(\mathbf{F}_2[u]/(1+u^4\mathbf{F}_2[u])^* \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$ it follows that such an extension does exist. The genus g_E of E can be computed using the conductor–discriminant–product formula. One finds that g_E is at most 1. Since E has five rational points, the genus must be equal to 1 and the quadratic extension must have its conductor equal to $4(\infty)$. In a similar way it can be shown that E' exists, that is has four rational points, and that it has genus 1 as well.

It is actually very easy to give explicit equations for E and E': the curve E can be given by $Y^2+Y=T^3+1$ and E' by $Y^2+uY=u^3+1$, where, as above, $uT=1$ in $\mathbf{F}_2(T)$.

The curve E has the largest possible number of points a curve of genus 1 over $\mathbf{F}_2$ can have. It does not have any points of degree 2 or 3, but it has points of higher degree. Let P denote a point of degree 5. We let Y denote the quadratic cover of E of conductor $2(P)$ in which all five rational points of E are split. As above, it can be verified that Y exists. It has genus 6 and $2 \cdot 5 = 10$ rational points. This is the maximal number of points a curve of genus 6 can have [6]. The set S' of points on Y over ∞ has cardinality 2.

Let k denote the function field of Y and let K be the composite of k and $\mathbf{F}_2(E')$. It is a quadratic extension of k. By X we denote the corresponding smooth curve. By construction the points on Y that are in S' are split in X. Therefore the set S of points on X over ∞ has cardinality 4. The other eight rational points of Y are ramified in X.

$$\begin{array}{ccc} Y & \longleftarrow & X \\ \downarrow & & \downarrow \\ E & \longleftarrow & Z \\ \downarrow & & \downarrow \\ \mathbf{P}^1 & \longleftarrow & E' \end{array}$$

Here Z denotes the curve corresponding to the composite of the function fields of E and E'. All arrows in the diagram are 2 to 1 mappings.

Proof of Theorem 1.1. Consider the cover $X \to Y$ and the corresponding quadratic extension of function fields $k \subset K$. We have that $\# S' = 2$ and hence that $O_{S'}^* \cong \mathbf{Z}$. All eight points of Y not in S' are ramified in X. It follows therefore from Proposition 2.4 with $l=2$ that

$$d_2 Cl_S \geqslant 8-1-1=6.$$

Since $\# S = 4$ we have that $d_2 O_S^* = 3$. We conclude from Theorem 2.3 that X admits an infinite $(2, S)$-class field tower.

The genus g_X of X can be computed using the conductor–discriminant–product formula: the conductor of X over Y is equal to $\sum 2(Q)$, where the sum runs over all eight points Q over 0 and 1. Since the genus of Y is 6 we get that $2g_X - 2 = 2(2 \cdot 6 - 2) + 2 \cdot 8$ and hence that $g_X = 19$. Since $\#S = 4$ we conclude from Proposition 2.2 that $A(2) \geqslant 4/(19-1) = \frac{2}{9}$, as required.

ACKNOWLEDGMENTS

Most of the work for this paper was done during a stay at the National Mathematical Centre in Abuja, Nigeria. I thank Professor Ezeilo and the Institute for a pleasant stay.

REFERENCES

1. E. ARTIN AND J. T. TATE, "Class Field Theory," Benjamin, New York, 1967.
2. J. W. S. CASSELS AND A. FRÖHLICH, "Algebraic Number Theory," Academic Press, London, 1967.
3. V. G. DRINFELD AND S. G. VLĂDUT, The number of points on an algebraic curve, *Funktsional. Anal. i Prilozhen* **17** (1983), 68–69. [*Functional Anal. Appl.* **17** (1983), 53–54]
4. E. S. GOLOD AND I. R. SHAFAREVIČ, On class field towers, *Izv. Akad. Nauk SSSR Ser. Mat.* **28**, 261–272. [*Amer. Math. Soc. Transl. Ser. 2* **48** (1965), 91–102]
5. R. HARTSHORNE, "Algebraic Geometry," Graduate Texts in Mathematics, Vol. 52, Springer-Verlag, New York, 1977.
6. Y. IHARA, Some remarks on the number of rational points of algebraic curves over finite fields, *J. Fac. Sci. Tokyo* **28** (1981), 721–724.
7. YU. I. MANIN, What is the maximum number of points on a curve over $\mathbf{F}_2$? *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **28** (1981), 715–720.
8. M. PERRET, Sur le nombre de points d'une courbe sur un corps fini; application aux codes correcteurs d'erreurs, *C. R. Acad. Sci. Paris* **309** (1989), 177–182.
9. J.-P. SERRE, "Groupes algébriques et corps de classes," Hermann, Paris, 1959.
10. J.-P. SERRE, "Corps locaux," Hermann, Paris, 1962.
11. J.-P. SERRE, Nombres de points des courbes algébriques sur $\mathbf{F}_q$, *Sém. Théor. de Nombres Bordeaux* (1982–1983), exp. 22.
12. 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.
13. J.-P. SERRE, Résumé des cours de 1983–1984, *in* "Annuaire du Collège de France, 1984," pp. 79–83.
14. M. A. TSFASMAN, S. G. VLĂDUT, AND TH. ZINK, Modular curves, Shimura curves and Goppa codes better than the Varschamov–Gilbert bound, *Math. Nachr.* **109** (1982), 21–28.
15. A. WEIL, "Variétés abéliennes et courbes algébriques," Hermann, Paris, 1948.
16. TH. ZINK, Degeneration of Shimura surfaces and a problem in coding theory, *in* "Proceedings, Fundamentals of Computation Theory, Corrbus, Germany, 1985" (L. Budach, Ed.), Lecture Notes in Computer Science, Vol. 199, Springer-Verlag, Berlin, 1986.