ACTA ARITHMETICA
160.2 (2013)

An upper bound for the minimum genus of a curve without points of small degree

by

Claudio Stirpe (Roma)

1. Introduction. Let X be a smooth, projective, absolutely irreducible curve over the finite field $\mathbb{F}_q$ and let K be the function field of X. For any integer $n > 0$ let a_n denote the number of places of K of degree n. Then $N_n = \sum_{d|n} da_d$ is the number of rational points over the constant field extension $K\mathbb{F}_{q^n}$. The Weil inequality (see [12]) states that

$$|N_n - q^n - 1| \leq 2g\sqrt{q^n},$$

where g is the genus of the curve. A search for curves with many points, motivated by applications in coding theory, showed that this bound is optimal when the genus g is small compared to q (see [3] for further details). When g is large compared to q sharper estimates hold (see for example [6] for an asymptotic result or also [10, Chapter V, Section 3]). A similar problem arises when looking for curves without points of degree n when n is a positive integer. In particular when X has no points over $\mathbb{F}_{q^n}$ then $g \geq (q^n + 1)/(2\sqrt{q^n})$. The genus 2 case was already considered in [7]. Moreover in a recent paper, E. Howe, K. Lauter and J. Top [5] show that the previous bound is not always sharp when $n = 1$ and $g = 3$ or 4. In the same paper they cite an unpublished result of P. Clark and N. Elkies that states that for every fixed prime p there is a constant $C_p > 0$ such that for any integer $n > 0$, there is a projective curve over $\mathbb{F}_p$ of genus $g \leq C_p np^n$ without places of degree smaller than n.

In this paper we prove that this bound is not optimal. In fact we prove the following result.

Theorem 1.1. *For any prime p there is a constant $C_p > 0$ such that for any $n > 0$ and for any power q of p there is a projective curve over $\mathbb{F}_q$ of genus $g \leq C_pq^n$ without points of degree strictly smaller than n.*

2010 *Mathematics Subject Classification*: Primary 11G05; Secondary 11R37.
Key words and phrases: rational points, class field theory.

DOI: 10.4064/aa160-2-2

We show the existence of such curves by means of class field theory. The basic relevant facts and definitions are recalled in the next section. In the third section we generalize a result of [1] about the number of ray class field extensions with given conductor $\mathfrak{m}$ and we prove some consequences concerning cyclic extensions. In Section 4 the estimate of Theorem 1.1 is proved.

We do not know if the estimate of Theorem 1.1 is asymptotically optimal. A table of examples for $q = 2$ and $n < 20$ is given at the end of the paper.

2. Background and notation. Throughout the paper we consider the function fields associated to the projective, nonsingular, geometrically irreducible curves over the finite field $\mathbb{F}_q$ of characteristic p.

The set of places of the function field K is denoted by $\mathcal{P}_K$ and the set of divisors of K is denoted by $\mathcal{D}_K$. The degree zero divisors are denoted by $\mathcal{D}_K^0$. We can associate to a nonzero element $z \in K$ its principal divisor $(z) \in \mathcal{D}_K^0$. The set of principal divisors is denoted by $\mathrm{Prin}(K)$. The number $h_K = |\mathcal{D}_K^0/\mathrm{Prin}(K)|$ is finite and it is called the *divisor class number* of K.

The completion of K at the place P is denoted by $\hat{K}_P$, and the unit group $\hat{U}_P$ is the set of nonzero elements of $\hat{K}_P$ with evaluation zero. We denote by J_K and C_K the idele group and the class group of K (see [9, Chapter 2]).

In what follows, we use ray class fields to construct curves. Let S be a finite nonempty set of places of K and let $\mathfrak{m} = \sum n_P P$ be an effective divisor of the function field K with support disjoint from S. The *S-congruence subgroup modulo* $\mathfrak{m}$ is the subgroup

$$J_S^{\mathfrak{m}} = \prod_{P \in S} \hat{K}_P^* \times \prod_{P \notin S} \hat{U}_P^{(n_P)}$$

of J_K, where $\hat{U}_P^{(n_P)}$ is the n_Pth unit group

$$\hat{U}_P^{(n_P)} = \{x \in \hat{U}_P \mid v_P(x-1) \geq n_P\},$$

when $n_P > 0$ and $\hat{U}_P^{(0)}$ is the unit group $\hat{U}_P$.

Definition 2.1. A *ray class group* is a subgroup $C_S^{\mathfrak{m}}$ of C_K of the form

$$C_S^{\mathfrak{m}} = (K^* J_S^{\mathfrak{m}})/K^*$$

where $J_S^{\mathfrak{m}}$ is the S-congruence subgroup modulo $\mathfrak{m}$.

The index of $C_S^{\mathfrak{m}}$ in C_K is finite and we denote by $K_S^{\mathfrak{m}}$ the function field associated to the subgroup $C_S^{\mathfrak{m}}$ by the Artin map (see [9, Chapter 2]). We call $K_S^{\mathfrak{m}}$ a *ray class field*.

The following result summarizes many useful formulas for the genus of a ray class field.

THEOREM 2.2. *Let K be a function field over the constant field $\mathbb{F}_q$ of genus g_K and let h_K be the divisor class number of K. Let $S = \{P\}$ be a set of a single place P of K of degree d and $\mathfrak{m} = \sum_{i=1}^{k} m_i P_i$ be an effective divisor of K where P_i are distinct places of degree n_i for $i = 1, \ldots, k$ such that $P \notin \mathrm{Supp}(\mathfrak{m})$ and $k \geq 1$ is a nonnegative integer. Then the ray class field $K_S^{\mathfrak{m}}$ is a function field over $\mathbb{F}_{q^d}$. The degree $[K_S^{\mathfrak{m}} : K]$ is equal to*

$$h_K d \prod_{i=1}^{k} \frac{(q^{n_i} - 1) q^{(m_i - 1) n_i}}{q - 1}.$$

The genus $g_{K_S^{\mathfrak{m}}}$ of $K_S^{\mathfrak{m}}$ is given by

$$g_{K_S^{\mathfrak{m}}} = 1 + \frac{h_K \prod_i (q^{n_i} - 1)}{2(q - 1)} \left(2g_K - 2 + \deg(\mathfrak{m}) - \sum_i \frac{\deg(P_i) q^{(m_i - 1) n_i}}{q^{n_i} - 1} \right). \tag{2.1}$$

Proof. See [2, Example 1.5]. ∎

3. Ray class fields. Let $h = h_K$ be the divisor class number of K. Then h is the degree of every maximal unramified abelian extension of K with constant field $\mathbb{F}_q$. There are exactly h such extensions of K (see [1, Chapter 8.3]). We denote them by $K_1^0, \ldots, K_h^0$.

A similar result also holds concerning ramified extensions.

THEOREM 3.1. *Let $\mathfrak{m} = \sum_{i=1}^{t} m_i P_i$ be an effective divisor and let n_i be the degree of P_i for $i = 1, \ldots, t$. Set $\mathfrak{m} = 0$ if $t = 0$. Set also*

$$d = \frac{h_K}{q - 1} \prod_{i=1}^{t} (q^{n_i} - 1) q^{(m_i - 1) n_i} \quad \text{if } t > 0 \quad \text{and} \quad d = h_K \quad \text{otherwise.}$$

Then there are exactly d abelian extensions of K of degree d with conductor $\mathfrak{m}$ and constant field $\mathbb{F}_q$.

As before, we denote such extensions by $K_1^{\mathfrak{m}}, \ldots, K_d^{\mathfrak{m}}$. There is no conflict with the previous notation because the result concerning unramified extensions can be seen as a special case of the previous theorem.

Proof of Theorem 3.1. In order to apply the Artin Reciprocity Theorem we construct suitable subgroups of the class group C_K.

Let U_0 be the subset of J_K given by

$$U_0 = \{(x_P)_{P \in \mathcal{P}_K} \in J_K \mid x_P \in \hat{U}_P^* \text{ for all places } P \in \mathcal{P}_K\}$$

and let $U_{\mathfrak{m}}$ be the subset of U_0 given by

$$U_{\mathfrak{m}} = \{(x_P)_{P \in \mathcal{P}_K} \in U_0 \mid x_P \equiv 1 \bmod t_i^{m_i} \text{ for all } i = 1, \ldots, t\},$$

where t_i is a uniformizer parameter at P_i. As before we set $U_{\mathfrak{m}} = U_0$ if $\mathfrak{m} = 0$. The field K^* is canonically embedded in J_K and we denote it again by K^* as in the previous section. Let $C_{\mathfrak{m}} = U_{\mathfrak{m}}/(K^* \cap U_{\mathfrak{m}})$ be the classes of $U_{\mathfrak{m}}$ in C_K.

Let D_0 be the subgroup of C_K of classes of ideles $x = (x_P)_{P\in\mathcal{P}_K}$ such that the divisor

$$\mathrm{Div}(x) = \sum_{P\in\mathcal{P}_K} v_P(x_P)P$$

has degree 0. The subgroup D_0 is well-defined because the principal divisors have degree 0. Moreover $U_0 \subseteq D_0$ and $|D_0/C_{\mathfrak{m}}| = d$.

The following sequence is exact (see [1, Chapter 8.3]):

$$0 \to D_0 \to C_K \to \mathbb{Z} \to 0, \tag{3.1}$$

where the map $C_K \to \mathbb{Z}$ is the degree of the divisor and it is surjective by the Schmidt Theorem (see [10, Corollary V.1.11]). Let D be a divisor of degree 1 and let $x \in J_K$ be an idele such that $\mathrm{Div}(x) = D$. Let $[x] \in C_K$ be the class of x in C_K. The subgroup generated by $C_{\mathfrak{m}} \cup [x]$ in C_K has finite index d because $|D_0/C_{\mathfrak{m}}| = d$. Let $a_1, \dots, a_d$ be representatives of the cosets of $C_{\mathfrak{m}}$ in D_0. Then the subgroups B_i of C_K generated by $C_{\mathfrak{m}} \cup ([x] + a_i)$ for $i \in \{1, \dots, d\}$ are d distinct subgroups of C_K of index d such that the image under the evaluation map in (3.1) is $\mathbb{Z}$.

Let $K_1^{\mathfrak{m}}, \dots, K_d^{\mathfrak{m}}$ be the function fields corresponding to the subgroups $B_1, \dots, B_d$ by the Artin map. We prove that these function fields are all the abelian extensions of K satisfying the hypothesis of the Theorem.

Let K' be an abelian extension of K with conductor $\mathfrak{m}$, degree d and constant field $\mathbb{F}_q$. Then $C_{K'} \subset C_K$ by the Artin map. Let $x' \in J_{K'}$ be an idele such that the divisor $D' = \mathrm{Div}(x')$ has degree 1. Then $[x'] - [x] \in D_0$ and so $[x'] - [x] \in C_{\mathfrak{m}} + a_i$ for a certain $i \in \{1, \dots, d\}$. It follows that $[x'] \in B_i$ and $K' = K_i^{\mathfrak{m}}$ because the degree over K is d. ∎

Remark 3.2. The proof of the previous theorem shows that the extensions $K_1^{\mathfrak{m}}, \dots, K_d^{\mathfrak{m}}$ of K are all contained in the constant field extension of degree d of any one of them, say $K_1^{\mathfrak{m}}\mathbb{F}_{q^d}$. In fact the compositum of the function fields $K_i^{\mathfrak{m}}K_j^{\mathfrak{m}}$ corresponds to the intersection $B_{i,j} = B_i \cap B_j$ in C_K by the Artin reciprocity map for $i, j \in \{1, \dots, d\}$. The image of the valuation of $B_{i,j}$ under the degree map in (3.1) is a subgroup of $\mathbb{Z}$ of finite index $d' \mid d$. In particular $K_i^{\mathfrak{m}}K_j^{\mathfrak{m}} = K_i^{\mathfrak{m}}\mathbb{F}_{q^{d'}}$.

Remark 3.3. When the quotient group $D_0/C_{\mathfrak{m}}$ is cyclic we can say something more about the subextensions of $K_i^{\mathfrak{m}}$ containing K for $i = 1, \dots, d$. In fact, let l be a divisor of d. Then there is only one subgroup G of $D_0/C_{\mathfrak{m}}$ of index l. Let $g_1, \dots, g_l$ be the coset representatives of G in $D_0/C_{\mathfrak{m}}$. We denote by F_i the fields corresponding by the Artin reciprocity map to the subgroups G_i of C_K generated by $G \cup ([x] + g_i)$ for $i = 1, \dots, l$. The field extensions F_i/K are all the abelian extensions of degree l unramified outside $\mathfrak{m}$ with constant field $\mathbb{F}_q$ for $i = 1, \dots, l$.

COROLLARY 3.4. *Let $\mathfrak{m}$ and d be as in Theorem 3.1. Let P be an unramified place of K and denote its degree by d'. Let l be the positive integer* $\gcd(d, d')$ *and $P_i|P$ be a place of $K_i^{\mathfrak{m}}$ over P for $i \in \{1, \dots, d\}$. If $D_0/C_{\mathfrak{m}}$ is a cyclic group then $f(P_i|P) = 1$ in at most l such extensions $K_i^{\mathfrak{m}}/K$.*

Proof. Assume that the place P is totally split in $K_i^{\mathfrak{m}}/K$ for at least one $i \le d$, otherwise the proof would be trivial. Then P is split in $K_j^{\mathfrak{m}}/K$ for $j \ne i$ if and only if P is totally split in the compositum $K_i^{\mathfrak{m}} K_j^{\mathfrak{m}}/K$. But $K_i^{\mathfrak{m}} K_j^{\mathfrak{m}} = K_i^{\mathfrak{m}} \mathbb{F}_{q^a}$ for a suitable integer $a \mid d$ by Remark 3.2. By the properties of the constant field extensions this is possible only when $a \mid d'$ and so $a \mid l$ and $K_j^{\mathfrak{m}} \subseteq K_i^{\mathfrak{m}} \mathbb{F}_{q^l}$.

It follows from Remark 3.3 that

$$l \cdot ([x] + a_i) \subseteq B_j$$

and so $l \cdot (a_i - a_j) \in C_{\mathfrak{m}}$ and the class of $l \cdot a_j$ in the quotient group $D_0/C_{\mathfrak{m}}$ is the class of $l \cdot a_i$. When $D_0/C_{\mathfrak{m}}$ is a cyclic group there are at most l such classes $a_j \in D_0/C_{\mathfrak{m}}$ and so there are at most l corresponding fields extensions by the Artin map. ∎

The previous corollary can be generalized as in the following result.

COROLLARY 3.5. *Assume the quotient group $D_0/C_{\mathfrak{m}}$ is a cyclic group of order d as in Corollary 3.4. Let s be a prime dividing d and let t be the maximal power of s dividing d. Let F_i/K be the extensions of degree t for $i = 1, \dots, t$ as in Remark 3.3. Let P be a place of K of degree d' and $P_i|P$ be a place of F_i over P. Let l be the* $\gcd(d', t)$ *and let $c \ge 0$ be the exponent such that $t/l = s^c$. Assume $c \ge 1$. Then for all integers $j = 1, \dots, c$, the integer s^j divides $f(P_i|P)$ in at least $l(s^c - s^{j-1})$ such extensions F_i/K.*

Proof. Let j' denote the number $ls^{c-(j-1)}$ and $E_1/K, \dots, E_{j'}/K$ be the extensions of K unramified outside $\mathfrak{m}$ of degree j' over K by Corollary 3.4. If $s^j \nmid f(P_i|P)$ for a certain $i \in \{1, \dots, t\}$ then the Frobenius automorphism $\mathrm{Frob}(P)$ of P in F_i/K has order dividing s^{j-1}. Let $E_{i'}/K$ be the only subfield of F_i of degree j' over K and let $P'_{i'}$ be the place under P_i in $E_{i'}$. Then $\mathrm{Frob}(P'_{i'}) = \mathrm{Frob}(P_i)^{j-1} = 1$ so $f(P'_{i'}|P) = 1$. By Corollary 3.4 there are at most l extensions E_i/K such that $f(P'_i|P) = 1$, say, $E_1/K, \dots, E_l/K$. There are exactly s^{j-1} extensions F_i/K over each $E_{i'}$ so $s^j \nmid f(P_i|P)$ in at most ls^{j-1} extensions F_i/K, and the corollary follows. ∎

REMARK 3.6. There are at most t/s extensions F_i/K as in Corollary 3.5 such that t/l does not divide $f(P_i|P)$.

4. A refinement of the Clark–Elkies bound. In the following we denote by K the rational function field over $\mathbb{F}_q$. The number of places of degree t of K is denoted by a_t, for any integer $t > 0$.

LEMMA 4.1. *Let $n \geq 1$ be an integer. The number of places of degree smaller than n is bounded by*

$$\sum_{d<n} a_d \leq q \cdot \frac{q^n}{n}. \tag{4.1}$$

Proof. We prove this by induction over n. The proof is trivial for $n = 1$ and $n = 2$.

If $n = 3$ then $a_1 + a_2 = q + 1 + \frac{q^2-q}{2} \leq q \cdot \frac{q^3}{3}$ for all $q \geq 2$.

Assume that $\sum_{d<n} a_d < q \cdot \frac{q^n}{n}$ for a certain $n \geq 3$. Then

$$\sum_{d<n+1} a_d < q \cdot \frac{q^n}{n} + a_n < q \cdot \frac{q^n}{n} + \frac{q^n}{n} \leq q \cdot \frac{q^{n+1}}{n+1},$$

and the lemma follows. ∎

We will use the following well-known lemma and an easy consequence.

LEMMA 4.2. *Let s and m be distinct, odd prime numbers and let q be a prime power such that $s \mid \frac{q^m-1}{q-1}$ but $s \nmid q-1$. Then $s = 2am+1$ for a suitable integer $a > 0$. In particular $s > 2m$.*

Proof. By hypothesis $q^m \equiv 1 \bmod s$ but $q \not\equiv 1 \bmod s$ because $s \nmid q-1$, so q has order m in $\mathbb{Z}^*/(s)$. By the Lagrange Theorem $m \mid s-1$, but m is odd and $s-1$ is even, so $2m \mid s-1$. ∎

COROLLARY 4.3. *There is a constant $c_q > 0$ such that when $m > c_q$ is a prime then there are at most m distinct primes dividing $(q^m-1)/(q-1)$ and these primes are all greater than $2m$.*

The next lemma shows that there are many function fields without places of small degree when we consider ray class field extensions of K.

LEMMA 4.4. *Let $C_1, C_2 > 0$ be positive real constants (not depending on n) with $C_2 < 1$. Let m be a prime number with $m \geq \log_q(n) + 1$ and let α be a positive integer such that $\alpha \leq a_m$. Let $\mathfrak{q}_1, \ldots, \mathfrak{q}_\alpha$ be distinct places of K of degree m and let $\mathfrak{m}$ be the divisor $\sum_{i=1}^{\alpha} \mathfrak{q}_i$. Set $d = (q^m-1)^\alpha/(q-1)$. Let $K_1^{\mathfrak{m}}, \ldots, K_d^{\mathfrak{m}}$ be the abelian extensions of degree d unramified outside $\mathfrak{m}$ as in Theorem 3.1. Then there is a constant n_0 such that when $n > n_0$ and $\alpha > C_1 n/\log_q(n)$ then there are at least $C_2 d$ function field extensions $K_i^{\mathfrak{m}}$ of K such that the inertia index $f(P_i|P)$ is greater than $n/\deg(P)$ whenever P is a place of K of degree $\deg(P) < n/\log_q(n)$ and P_i is a place of $K_i^{\mathfrak{m}}$ over P.*

Proof. Let i be an element in $\{1,\ldots,d\}$ such that $K_i^{\mathfrak{m}}/K$ is a function field extension with $f(P_i|P) < n/\deg(P)$ for at least one place P of K of degree d' with $d' < n/\log_q(n)$. We estimate the number of such extensions.

Let k be the integer $(q^m-1)/(q-1)$. Let j be an integer in $\{1,\ldots,\alpha\}$ and let t be a power of a prime number s such that t divides k. Consider the subextensions of $K_i^{\mathfrak{q}_j} \subseteq K_i^{\mathfrak{m}}$ totally ramified in $\mathfrak{q}_j$ of degree t for $j \in \{1,\ldots,\alpha\}$. Let $P_{i,j}$ be the place of $K_i^{\mathfrak{q}_j}$ under P_i. Let l be the integer $\gcd(t,d')$.

Assume first that for every prime power divisor t of k the number t/l divides $f(P_{i,j}|P)$ for at least one $j \leq \alpha$. Then

$$k \mid f(P_i|P)\gcd(k,d')$$

and so

$$f(P_i|P) \geq n/d',$$

because $k \geq n$ and $d' \geq \gcd(k,d')$. It follows that if $f(P_i|P) < n/\deg(P)$ then there is at least one prime power t dividing k such that $t/l \nmid f(P_{i,j}|P)$ for all $j \in \{1,\ldots,\alpha\}$. For this reason, given a prime power t dividing k, it will be enough to estimate only the number of extensions $K_i^{\mathfrak{m}}/K$ such that $t/l \nmid f(P_{i,j}|P)$ for all $j \in \{1,\ldots,\alpha\}$.

The extensions $K_i^{\mathfrak{q}_j}/K$ are cyclic for all $j \in \{1,\ldots,\alpha\}$ (see [9, Proposition 3.2.4]). By Remark 3.6 there are at most t/s distinct extensions $K_i^{\mathfrak{q}_j}/K$ of degree t totally ramified in $\mathfrak{q}_j$ such that $t/l \nmid f(P_{i,j}|P)$. It follows that there are at most $(k/s)^\alpha$ different extensions $K_i^{\mathfrak{q}_1}\cdots K_i^{\mathfrak{q}_\alpha}$ of K such that $t/l \nmid f(P_i|P)$ when P is unramified. So we see that there are at most d/s^α extensions $K_i^{\mathfrak{m}}/K$ with a place P_i such that $f(P_i|P) < n/d'$ for a certain place P of K of degree $d' < n/\log_q(n)$.

Now we consider the case where $P = \mathfrak{q}_h$, for a certain $h \in \{1,\ldots,\alpha\}$, is a ramified place. We consider $\mathfrak{m}' = \mathfrak{m} - P$. For a similar reasoning as above we get at most

$$\frac{(q^m-1)^{\alpha-1}}{(q-1)s^{\alpha-1}}$$

extensions $K_j^{\mathfrak{m}'}$ for $j \in \{1,\ldots,(q^m-1)^{\alpha-1}/q-1\}$ such that $f(P_j'|P) < n/\deg(P)$, where P_j' is a place of $K_j^{\mathfrak{m}'}$ over P. But $K_j^{\mathfrak{m}'} \subseteq K_i^{\mathfrak{m}}$ for q^m-1 suitable $i \in \{1,\ldots,d\}$ and $f(P_j'|P) \leq f(P_i|P)$ so there are at most $d/s^{\alpha-1}$ extensions $K_i^{\mathfrak{m}}/K$ of K with $f(P_i|P) < n/\deg(P)$ when $P \in \mathrm{Supp}(\mathfrak{m})$ is ramified.

Now we sum the number of all such extensions for all the places P of K, ramified or not, of degree smaller than $n/\log_q(n)$ and for all prime $s \mid k$. This yields

$$\sum_{s|k}\sum_{i=1}^{\alpha}\frac{d}{s^{\alpha-1}}+\sum_{\deg(P)<n/\log_q(n)}\sum_{s|k}\frac{d}{s^{\alpha}}<(1-C_2)d, \tag{4.2}$$

where P runs over the unramified places of K of degree smaller than $n/\log_q(n)$. The left hand side in (4.2) is bounded by

$$m\alpha\frac{d}{(2m)^{\alpha-1}}+mq\cdot q^{n/\log_q(n)}\frac{d}{(2m)^{\alpha}}$$

by (4.1), Lemma 4.2 and Corollary 4.3. So

$$(2m)^{\alpha}>\frac{qm}{1-C_2}(2m\alpha+q^{n/\log_q(n)}),$$

or

$$\alpha\log_q(2m)>\log_q(q^{n/\log_q(n)}+2m\alpha)+\log_q\left(\frac{m}{1-C_2}\right)+1. \tag{4.3}$$

The right hand side in the last inequality is smaller than

$$\frac{n}{\log_q(n)}+\log_q(2m\alpha)+\log_q\left(\frac{m}{1-C_2}\right)+1,$$

because the logarithm is subadditive and so (4.3) holds when n is large because $\alpha>C_1n/\log_q(n)$ by hypothesis. ∎

Lemma 4.5. *Let $\mathfrak{q}_1,\dots,\mathfrak{q}_a$ be distinct places of K of degree $t_1,\dots,t_a$ respectively. Let $p_1,\dots,p_a$ be positive integers such that $p_i \mid \frac{q^{t_i}-1}{q-1}$ for $i=1,\dots,a$. Let F_i/K be ray class field extensions over $\mathbb{F}_q$ of degree p_i totally ramified in $\mathfrak{q}_i$ for $i=1,\dots,a$. Let g_L be the genus of the compositum field $L=F_1\cdots F_a$. Then*

$$g_L\le\frac{1}{2}\sum_{i=1}^{a}t_i\prod_{j=1}^{a}p_j.$$

Proof. This follows by induction over a. When $a=1$ the assertion follows from the Hurwitz genus formula (see [10, Theorem III.4.12]).

Let L' be the compositum field $F_1\cdots F_{a-1}$ and assume

$$g_{L'}\le\frac{1}{2}\sum_{i=1}^{a-1}t_i\prod_{j=1}^{a-1}p_j.$$

Consider the extension L/L'. The degree of the different is $(p_a-1)t_a\prod_{j=1}^{a-1}p_j$ (see [10, Theorem III.5.1]), so

$$g_L\le p_ag_{L'}+\frac{1}{2}t_a\prod_{j=1}^{a}p_j$$

by the Hurwitz genus formula, and the lemma follows. ∎

Proposition 4.6. *Let m and l be distinct prime numbers greater than $3\log_q(n)$ and let α and β be positive integers with $\alpha \le a_m$ and $\beta \le a_l$. Let $C_1 > 0$ be a real constant and let $C_2 > 0$ be a real constant with $C_2 < 1$ as in Proposition 4.4. Let $\mathfrak{q}_1, \ldots, \mathfrak{q}_\alpha$ (resp. $\mathfrak{p}_1, \ldots, \mathfrak{p}_\beta$) be distinct places of K of degree m (resp. l) with $\alpha > C_1 n/\log_q(n)$. Let $\mathfrak{m}$ be the effective divisor $\sum_{i=1}^{\alpha} \mathfrak{q}_i + \sum_{j=1}^{\beta} \mathfrak{p}_j$. Let*

$$k_1 = \frac{q^m - 1}{q - 1}, \qquad k_2 = \frac{q^l - 1}{q - 1},$$

and set

$$d = \frac{(q^m - 1)^\alpha (q^l - 1)^\beta}{q - 1}.$$

Assume that k_1 and k_2 are both prime to $q-1$. Then there is an integer n_0 such that when $n > n_0$ and

$$\frac{C_2}{2} d > \frac{q \cdot q^n}{n},$$

there is a function field extension $K_i^{\mathfrak{m}}/K$ for a certain $i \in \{1, \ldots, d\}$ without places of degree smaller than n.

Proof. We may assume that l and m are smaller than $n/\log_q(n)$, as otherwise the proof would be easier. By Lemma 4.4 there are at least $C_2 d$ function field extensions $K_i^{\mathfrak{m}}/K$ for $i = 1, \ldots, d$ such that $\deg(P) f(P_i|P) \ge n$ whenever P is a place of K of degree $\deg(P) < n/\log_q(n)$ and P_i is a place over P. In one of these field extensions $K_i^{\mathfrak{m}}$ of K there is a place of degree smaller than n only if there is a place P of K of degree $d' < n$ with $d' \ge n/\log_q(n)$ such that P is totally split in $K_i^{\mathfrak{q}_j}/K$ for all $j \in \{1, \ldots, \alpha\}$ and in $K_i^{\mathfrak{p}_h}/K$ for all $h \in \{1, \ldots, \beta\}$ by Lemma 4.2, where $K_i^{\mathfrak{q}_j}$ and $K_i^{\mathfrak{p}_h}$ are the ray class fields of K with conductor $\mathfrak{q}_j$ and $\mathfrak{p}_h$, respectively, contained in $K_i^{\mathfrak{m}}$. We are going to estimate the number of such function field extensions $K_i^{\mathfrak{m}}/K$.

For a fixed $j \le \alpha$ we consider $K_i^{\mathfrak{q}_j}/K$ for $i \in \{1, \ldots, k_1\}$. There are at most $d_1 = \gcd(d', k_1)$ function field extensions $K_i^{\mathfrak{q}_j}/K$ such that P is totally split by Corollary 3.4. Similarly for a fixed $h \le \beta$ there are at most $d_2 = \gcd(d', k_2)$ function field extensions $K_i^{\mathfrak{q}_h}/K$ with $i \in \{1, \ldots, k_2\}$ such that P is totally split. We denote by d'' the greatest common divisor $\gcd(q-1, d')$. It follows that there are at most $d_1^\alpha d_2^\beta d''^{\alpha+\beta-1}$ extensions $K_i^{\mathfrak{m}}/K$ with $i \in \{1, \ldots, d\}$ such that P is totally split. We are going to estimate the number of such places P.

Let $A_{d_1,d_2,d'}$ be the number of places of K of degree d' totally split in all the subextensions of degree $d_1 d''$ (resp. $d_2 d''$) of the ray class fields $K_i^{\mathfrak{q}_j}$ for $i \in \{1, \ldots, k_1\}$ and $j \in \{1, \ldots, \alpha\}$ (resp. $K_i^{\mathfrak{p}_h}$ for $i \in \{1, \ldots, k_2\}$ and

$h \in \{1, \ldots, \beta\}$). Then

$$A_{d_1,d_2,d'} \le \frac{q^{d'}}{d' d_1^{\alpha} d_2^{\beta} d''^{\alpha+\beta-1}} + 2\frac{g_L}{d_1^{\alpha} d_2^{\beta} d''^{\alpha+\beta-1}}\sqrt{q^{d'}} + \deg(\mathfrak{m})$$

by the Chebotarev Theorem (see [8]), where L is the compositum of the subextensions of degree d_1 and d_2 of $K_i^{\mathfrak{q}_j}$ and $K_i^{\mathfrak{p}_h}$. By Lemma 4.5 we get

$$g_L \le \tfrac{1}{2} d_1^{\alpha} d_2^{\beta} d''^{\alpha+\beta-1}(m\alpha + l\beta)$$

and so

$$A_{d_1,d_2,d'} \le \frac{q^{d'}}{d' d_1^{\alpha} d_2^{\beta} d''^{\alpha+\beta-1}} + (\sqrt{q^{d'}} + 1)(m\alpha + l\beta).$$

It follows that the number of distinct extensions $K_i^{\mathfrak{m}}/K$ with at least one totally split place of K of degree d' with $n/\log_q(n) < d' < n$ is bounded by

$$\sum_{d'=[n/\log_q(n)]}^{n-1} A_{d_1,d_2,d'} d_1^{\alpha} d_2^{\beta} d''^{\alpha+\beta-1}$$

$$\le \sum_{d'=[n/\log_q(n)]}^{n-1} \frac{q^{d'}}{d'} + (\sqrt{q^{d'}} + 1)(\alpha m + \beta l) d_1^{\alpha} d_2^{\beta} d''^{\alpha+\beta-1}.$$

But $d_1 d'' \le d' < n < k_1^{1/3}$, and similarly $d_2 d'' < k_2^{1/3}$. So

$$d_1^{\alpha} d_2^{\beta} d''^{\alpha+\beta} < (k_1^{\alpha} k_2^{\beta})^{1/3} \le d^{1/3}.$$

Moreover $\alpha m + \beta l < 2\log_q(d)$. It follows that there are at most

$$q\frac{q^n}{n} + 2n\sqrt{q^n}\log_q(d) d^{1/3} \tag{4.4}$$

extensions $K_i^{\mathfrak{m}}/K$ with at least one totally split place of K of degree $d' < n$.

By Lemma 4.4 there are at least $C_2 d$ extensions $K_i^{\mathfrak{m}}/K$ such that $f(Q|P) > n/\deg(P)$ for all the places Q over the place P of K with $\deg(P) < n/\log_q(n)$. We prove that at least one of these function fields has no places of degree smaller than n. In fact, the number showed in (4.4) is smaller than $C_2 d$ if

$$\frac{q \cdot q^n}{n} < \frac{C_2}{2} d \quad \text{and} \quad 2n\sqrt{q^n}\log_q(d) < \frac{C_2}{2} d^{2/3}.$$

The first condition holds by hypothesis, the second one holds when n is large because $d > (2q/C_2)(q^n/n)$, so there is at least one function field extension $K_i^{\mathfrak{m}}/K$ without places of degree smaller than n. ∎

In order to prove Theorem 1.1 we choose suitable α and β such that the integer $d = (q^m - 1)^{\alpha}(q^l - 1)^{\beta}/(q - 1)$ is greater than a certain real number r but smaller than rq. In the next lemma we see a sufficient condition for the existence of such integers α and β.

LEMMA 4.7. *Let l and m be coprime integers with $l < m < 2l$. Then there is a constant l_0 such that when $l > l_0$ then for any real number r greater than q^{2m^3} there are two positive integers α and β such that*

$$r < \frac{(q^m - 1)^\alpha (q^l - 1)^\beta}{q - 1} < rq. \tag{4.5}$$

Proof. Let R be the real number $\log_q(rq) + \log_q(q-1)$. Taking logarithms of both sides in (4.5) we get the equivalent condition

$$R - 1 < \alpha q_m + \beta q_l < R,$$

where q_m and q_l denote the real numbers $\log_q(q^m - 1)$ and $\log_q(q^l - 1)$.

By means of the Farey series of order m (see [4, Chapter III]) we can find positive integers h and k with $0 < h < k < m$ such that the real number

$$v = kq_l - hq_m$$

satisfies $1/2 < v < 1$. In fact h/k is the rational number preceding l/m in the Farey series, and $h/k < q_l/q_m < l/m$ when l is large compared to q (see [11, formula (5.10)]). In particular $v < kl - hm$. But $kl - hm = 1$ by an elementary property of the Farey series (see [4, Theorem 28]), so $v < 1$. Moreover $v > 1/2$, since otherwise

$$\frac{q_l}{q_m} - \frac{h}{k} = \frac{v}{kq_m} < \frac{1}{2kq_m},$$

so

$$\frac{l}{m} - \frac{q_l}{q_m} + \frac{1}{2kq_m} > \frac{l}{m} - \frac{h}{k} = \frac{1}{km},$$

and so

$$\frac{l}{m} - \frac{q_l}{q_m} > \frac{1}{km} - \frac{1}{2kq_m} > \frac{1}{4m(m-1)},$$

and we get a contradiction because

$$\frac{l}{m} - \frac{q_l}{q_m} < \frac{1}{4m(m-1)}$$

when l is large (see [11, formula (5.10)]).

Let c be the integer $[R/q_m]$ and let z be the real number cq_m. If $z > R-1$ then we choose $\alpha = c$ and $\beta = 0$, and the lemma follows. Otherwise we define the succession $z_i = z + iv$ for all integers $i \geq 0$. Let j be the minimum integer such that $z_j > R - 1$. Then $z_j < R$ because $v < 1$ and so $j < c/h$, as otherwise $jv > q_m$ and z_j would be greater than R, because $v > 1/2$ and $R > 2m^3$, and this is not the case. We choose $\alpha = c - jh$ and $\beta = jk$, and the lemma follows. ∎

Proof of Theorem 1.1. We assume first that $q = p$ is a prime.

We choose a prime number l greater than $3\log_p(n)$. By the Bertrand postulate we can choose l smaller than $6\log_p(n)$. Moreover there is another prime m greater than l but smaller than $2l$. We set $r = 4p \cdot p^n/n$. We can apply Lemma 4.7 when n is large because l and m are smaller than $12\log_p(n)$ so there are two positive integers α and β satisfying (4.5). The conditions $\alpha < a_m$ and $\beta < a_l$ hold if l and m are greater than $3\log_p(n)$, as otherwise $p^{m\alpha+l\beta}$ would be greater than p^{n^3} and it would not satisfy (4.5). In a similar way we see that α or β is greater than, say,

$$\frac{1}{48}\,\frac{n}{\log_p(n)},$$

otherwise $p^{m\alpha+l\beta}$ would be smaller than $p^{n/2}$ in contrast with (4.5). So we can apply Proposition 4.6 with $C_1 = 1/48$ and $C_2 = 1/2$ and we get a ray class field extension of degree d over the rational function field without places of degree smaller than n whenever n is greater than a suitable constant n_0. The degree of the conductor is smaller than n, and

$$d < 4p^2 \cdot p^n/n,$$

so the genus of such a function field is smaller than $2p^2p^n$ by (2.1). Let C_p be the constant $2p^{n_0+2}$. Then there is a function field with constant field $\mathbb{F}_p$ without places of degree smaller than n of genus smaller than C_pp^n for all integer $n > 0$.

Now let $q = p^c$ be a prime power of p. By the previous case there is a function field K of genus $g_K \le C_pp^{cn} = C_pq^n$ over $\mathbb{F}_p$ without places of degree smaller than cn. The constant field extension $K\mathbb{F}_q$ is a function field over $\mathbb{F}_q$ with the same genus without places of degree smaller than n. This concludes the proof. ∎

5. Table. In the table opposite we list examples of curves over $\mathbb{F}_q$ without points of degree d' such that $d' \le n$ when $q = 2$ and $n < 20$.

The integer d in the table is the degree of a function field extension $K/\mathbb{F}_q(x)$ of the rational function field with genus g and constant field $\mathbb{F}_q$. In this table the field K is a subfield of the ray class field $K_S^{\mathfrak{m}}$ of conductor $\mathfrak{m}$. The irreducible polynomials in the fourth column correspond to the places in the support of $\mathfrak{m}$ with multiplicity. The polynomial in $\mathbb{F}_q(x)$ corresponding to the place S totally split in $K_S^{\mathfrak{m}}/\mathbb{F}_q(x)$ is shown in the last column.

Acknowledgements. This research is part of my Phd thesis at the Università di Roma 'Sapienza'. I am grateful to Prof. René Schoof, Università di Roma 'Tor Vergata', for his patience and support. Part of this work was done when I was a visiting student at the Mathematical Institute at Leiden University.

Pointless curves for $q = 2$

n	g	d	$\mathfrak{m}$	S
1	2	2	$(x^3+x+1)^2$	(x^3+x^2+1)
2	3	7	(x^3+x+1)	(x^4+x+1)
3	4	5	(x^4+x+1)	(x^7+x^4+1)
5	12	7	$(x^6+x^4+x^3+x+1)$	$(x^8+x^5+x^3+x^2+1)$
7	48	17	$(x^8+x^7+x^6+x+1)$	$(x^9+x^7+x^5+x^2+1)$
8	78	$7\cdot 7$	(x^3+x^2+1, x^3+x+1)	$(x^9+x^7+x^2+x+1)$
9	120	31	$(x^{10}+x^3+1)$	$(x^{11}+x^9+x^7+x^2+1)$
11	362	$15\cdot 7$	$(x^4+x+1, x^6+x^5+x^3+x^2+1)$	$(x^{13}+x^8+x^5+x^3+1)$
12	588	$31\cdot 7$	(x^5+x^2+1, x^3+x+1)	$(x^{13}+x^{12}+x^{10}+x^7+x^4+x+1)$
13	1480	$31\cdot 15$	(x^5+x^2+1, x^4+x+1)	$(x^{14}+x^{13}+x^5+x^4+x^3+x^2+1)$
14	3342	$127\cdot 7$	(x^7+x+1, x^3+x+1)	$(x^{15}+x^{14}+x^{13}+x^7+x^6+x^4+x^2+x+1)$
15	8940	$73\cdot 17$	$(x^9+x^4+1, x^8+x^5+x^3+x^2+1)$	$(x^{16}+x^{14}+x^{13}+x^{11}+x^{10}+x^7+x^4+x+1)$
16	19861	$23\cdot 89$	$(x^{11}+x^6+x^5+x^2+1, x^{11}+x^9+1)$	$(x^{18}+x^{17}+x^{11}+x^9+x^7+x^4+1)$
17	41440	$89\cdot 63$	$(x^{11}+x^9+1, x^6+x+1)$	$(x^{18}+x^{17}+x^{16}+x^{11}+x^9+x^4+1)$
18	89415	$127\cdot 89$	$(x^7+x+1, x^{11}+x^9+1)$	$(x^{19}+x^{18}+x^{15}+x^{14}+x^{11}+x^7+x^3+x+1)$
19	95886	$127\cdot 127$	(x^7+x+1, x^7+x^6+1)	$(x^{20}+x^{19}+x^{15}+x^{14}+x^{13}+x^2+1)$

References

[1] E. Artin and J. Tate, *Class Field Theory*, W. A. Benjamin, New York, 1967.
[2] R. Auer, *Ray class fields of global function fields with many rational places*, Acta Arith. 95 (2000), 97–122.
[3] R. Fuhrmann and F. Torres, *The genus of curves over finite fields with many rational points*, Manuscripta Math. 89 (1996), 103–106.
[4] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford Sci. Publ., Clarendon, 1938.
[5] E. W. Howe, K. Lauter and J. Top, *Pointless curves of genus three and four*, in: Arithmetic, Geometry and Coding Theory, Sémin. Congr. 11, Soc. Math. France, 2005, 125–141.
[6] 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.
[7] D. Maisner and E. Nart, *Abelian surfaces over finite fields as Jacobians* (with an appendix by E. W. Howe), Experiment. Math. 11 (2002), 321–337.
[8] V. K. Murty and J. Scherk, *Effective versions of the Chebotarev density theorem for function fields*, C. R. Acad. Sci. Paris Sér. I Math. 319 (1994), 523–528.
[9] H. Niederreiter and C. Xing, *Rational Points on Curves over Finite Fields: Theory and Applications*, Cambridge Univ. Press, Cambridge, 2001.
[10] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, Berlin, 1993.
[11] C. Stirpe, *An upper bound for the genus of a curve without points of small degree*, Phd Thesis at Università di Roma 'Sapienza', http://padis.uniroma1.it/bitstream/10805/1371/1/tesi.pdf, 2011.
[12] A. Weil, *Courbes algébriques et variétés abéliennes*, Hermann, Paris, 1971.

Claudio Stirpe
Dipartimento di Matematica
Università di Roma 'Sapienza'
Via Castello 35
03029 Veroli (FR), Italy
E-mail: clast@inwind.it

Received on 24.5.2012
and in revised form on 26.2.2013 (7043)