



Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt



Imaginary quadratic function fields

Javier Diaz-Vargas*, Carlos Pompeyo-Gutiérrez

Facultad de Matemáticas, Universidad Autónoma de Yucatán, Anillo Periférico Norte Tablaje 13615, Mérida, Yucatán, Mexico

ARTICLE INFO

Article history:

Received 5 February 2008

Revised 9 September 2009

Communicated by David Goss

Keywords:

Function fields

Divisor class group

Ideal class group

Class number

ABSTRACT

In Bautista-Ancona and Diaz-Vargas (2006) [B-D] a characterization and complete listing is given of the imaginary quadratic extensions K of $k(x)$, where k is a finite field, in which the ideal class group has exponent two and the infinite prime of $k(x)$ ramifies. The objective of this work is to give a characterization and list of these kind of extensions but now considering the case in which the infinite prime of $k(x)$ is inert in K . Thus, we get all the imaginary quadratic extensions of $k(x)$, in which the ideal class group has exponent two.

© 2009 Elsevier Inc. All rights reserved.

1. Introduction

An algebraic function field of one variable over k is an extension field $k \subseteq K$ such that K is a finite extension of $k(x)$ for some $x \in K$ transcendental over k . Emil Artin studied the arithmetic and analytic theory of the quadratic extensions of $k(x)$, where k is a field of prime order. He viewed these topics as an analogue of the theory of quadratic number fields, and for this reason he divided these extensions in two classes, real and imaginary according to the decomposition of the infinite prime of $k(x)$ in the extension. In the study Artin made on quadratic extensions of $k(x)$, he discussed the problem of classifying all the extensions of $k(x)$ in which the ideal class group has exponent two. He showed that for such fields we have $|k| = q = 3, 5$ or 7 and the genus is bound. Madden eliminated the assumption that k is of prime order and improved the bounds on the genus. However, in his work Madden considered only imaginary extensions in which the infinite prime of $k(x)$ ramifies. This is the motivation and starting point of our work: to establish and prove a similar result assuming now that the infinite prime is inert in K .

Consider $k[x]$ inside $k(x)$. Let K be a quadratic extension of $k(x)$, and A the ring of integers of K over $k[x]$. Recall that h_K is the divisor (null) class number of K , so the class number h , the order of

* Corresponding author.

E-mail address: jdvargas@uady.mx (J. Diaz-Vargas).

the ideal class group of A as a Dedekind domain, is $h = f_\infty h_K$, where f_∞ is the inertia degree of the infinite prime of $k(x)$.

The study of the congruent function fields with exponent two ideal class group is made by considering fields with exponent two null class group (or group of divisor classes of degree zero) C_K^0 , whose order is h_K . If K is an imaginary quadratic extension of $k(x)$ in which the ideal class group has exponent 2, since the null class group of an imaginary extension is a subgroup of the ideal class group, the null class group must have exponent 2 or have order one. Madan and Queen [M2] have shown that there are only two cases in which a quadratic extension of $k(x)$ has class number 1 and genus $g > 1$. In both cases $q = 2$ and $g = 2$. If the infinite prime of $k(x)$ ramifies, the connection is even simpler since the null class group and the ideal class group are identical. Unfortunately, this is not the case if the infinite prime of $k(x)$ is inert in K , and for this reason, we will restrict ourselves, to begin with, to considerations of the null class group.

Recall that by definition, K is an imaginary extension of $k(x)$ if there is only one prime of K that lies over the infinite prime of $k(x)$. A field K is said to be a totally imaginary extension of $k(x)$ if no prime of degree one in $k(x)$ splits in K . Notice that if K is an extension of $k(x)$ any prime of $k(x)$ of degree one may act as the infinite prime since

$$k(x) = k\left(\frac{1}{x+a}\right), \quad \text{for any } a \in k.$$

Therefore, if we set $L = k(x)$ and K is a totally imaginary extension of L then K is an imaginary extension of L no matter which degree one prime of L we take as the infinite prime. Given an arbitrary quadratic extension with exponent two null class group, two things can happen. If some prime of degree one ramifies then we can choose this prime as the infinite prime. Then the extension is imaginary, and in this case we can find what type of extension we have in [B-D]. If there is no prime of degree one ramifying, then the genus of K is greater than 1. As the exponent of the null class group is 2, then according to Theorem 2 in [M3] we have that K is a totally imaginary extension of $k(x)$. Therefore all the degree one primes are inert. These considerations justify our assumption that all primes of degree one in $k(x)$ are inert in K , instead of only the prime at infinity.

If $h_K = 1$, since $f_\infty = 2$, $h = 2$ and then, of course, the ideal class group has exponent two. This situation has already been discussed before and the only function field found is given by (see [L1, page 118]):

$$y^2 + y = \frac{x^3 + x^2 + 1}{x^3 + x + 1}. \quad (1)$$

So, we focus on the case $h_K > 1$. We show that there is no imaginary quadratic function field whose null class group has exponent two and all degree one primes are inert, obtaining in this way the main theorem of this paper that we state in the following.

Theorem 1.1. *Let K be an imaginary quadratic extension of $k(x)$ with genus g , where k is a finite field of order q , in which all the primes of degree one of $k(x)$ are inert in K , and with exponent 2 ideal class group. Then $K = k(x, y)$ with $q = 2$ and $g = 2$, where*

$$y^2 + y = \frac{x^3 + x^2 + 1}{x^3 + x + 1}.$$

Also, the ideal class group has order 2.

For general background on function fields, see the book [S1]. Also see the books [R2] and [VS1].

For the rest of this work, each time we say K/k is a function field, we mean that K/k is an algebraic function field of one variable over k .

2. Preliminaries

In this section we provide a brief introduction to the theory needed to develop the next sections.

We begin by giving an estimate of the minimal degree of a prime of $k(x)$ which splits in K , a geometric extension of degree 2 of $k(x)$. This result is a specialization of the mentioned case, of Theorem 6 in [M1].

Theorem 2.1. *If K is a geometric quadratic extension of $k(x)$, then there is a prime divisor in $k(x)$ which splits in K with degree less than or equal to m_0 , for any odd integer m_0 satisfying*

$$q^{m_0} - 2gq^{m_0/2} + 1 > m_0 R$$

where g is the genus of K , $|k| = q$ and R is the number of primes of $k(x)$ ramifying in K .

By using this result we can show

Theorem 2.2. *Let K/k be a congruence function field with constant field k , such that $[K : k(x)] = 2$ and having exponent 2 null class group. Assume that all the degree 1 primes of $k(x)$ are inert in K and the genus g of K is greater than 1. Let*

$$\lambda = \left\lceil \frac{g}{2} \right\rceil,$$

the greater integer less than or equal to $g/2$. Then, if λ is odd we have

$$q^\lambda - 2gq^{\lambda/2} + 1 \leq \lambda R,$$

and if λ is even then

$$q^{\lambda-1} - 2gq^{(\lambda-1)/2} + 1 \leq (\lambda-1)R$$

where R is the number of primes of $k(x)$ ramifying in K .

Proof. Since all the primes of degree 1 are inert in K , we have $f_\infty = f(\mathfrak{P}_\infty | P_{1/x}) = 2$, and by the corollary to Theorem 4 in [M3] (that needs the hypothesis about the null class group) we have that no prime of degree $g/2$ or less can split in K . Now we will consider the case in which λ is odd. If we had

$$q^\lambda - 2gq^{\lambda/2} + 1 > \lambda R$$

then by Theorem 2.1 there is a prime divisor P of $k(x)$ totally split in K and such that

$$\deg(P) \leq \lambda = \left\lceil \frac{g}{2} \right\rceil \leq \frac{g}{2}$$

which is absurd. Therefore

$$q^\lambda - 2gq^{\lambda/2} + 1 \leq \lambda R.$$

Now, if λ is even, then $\lambda - 1$ is odd and again Theorem 2.1 gives us

$$q^{\lambda-1} - 2gq^{(\lambda-1)/2} + 1 \leq (\lambda - 1)R,$$

as we wanted. \square

3. A first approximation

First we need to note the following. A function field K/k (where k is the constant field of K) is said to be *elliptic* if the following conditions are held:

1. the genus g of K/k is 1, and
2. there is a divisor $A \in D_K$ with $\deg(A) = 1$.

Observe that condition 2 is always true if k is a finite field, and in this case we have that K/k is an elliptic function field if and only if $g = 1$. Via the Riemann–Roch theorem is standard to prove that if K/k is a function field of genus 1, then there is a prime of degree 1 which ramifies in K and therefore, without loss of generality, the infinite prime of $k(x)$ ramifies in K . In this way, if K is a quadratic extension of $k(x)$ in which all primes of degree 1 of $k(x)$ are inert in K , then $g \geq 2$.

Now we give the first approximation for the bounds. We need to consider only $q < 6$. See [M3, last page].

Theorem 3.1. *Let K be a quadratic extension of $k(x)$ with exponent 2 null class group. Assume that all primes of degree 1 of $k(x)$ are inert in K . If $|k| = q$ and g is the genus of K then*

1. $q = 5, 2 \leq g \leq 9$;
2. $q = 4, 2 \leq g \leq 9$;
3. $q = 3, 2 \leq g \leq 13$;
4. $q = 2, 2 \leq g \leq 25$.

Proof. The main idea of this proof is to use Theorem 2.2 since $g \geq 2$. If we define

$$\lambda = \left\lfloor \frac{g}{2} \right\rfloor,$$

then

$$g = \begin{cases} 2\lambda & \text{if } g \text{ is even,} \\ 2\lambda + 1 & \text{if } g \text{ is odd.} \end{cases}$$

Moreover, the condition of all primes of degree 1 being inert in K implies that $R \leq g + 1$, where R is the number of primes of $k(x)$ ramifying in K . This is because the assumption implies that K has no primes of degree one. Then by the assumption, and Riemann–Hurwitz we have

$$2g + 2 = \deg(\text{Diff}(K/k(x))) = \sum_{i=1}^R \deg(\mathfrak{P}_i) \geq 2R.$$

Case $q = 5$. First suppose λ is odd. If g is even, then $g = 2\lambda$, therefore $\lambda = 1$ or 3, for if $\lambda = 5$ then $g = 10$ and

$$q^\lambda - 2gq^{\lambda/2} + 1 - \lambda R \geq q^\lambda - 2gq^{\lambda/2} + 1 - \lambda(g + 1) > 1952 > 0$$

that is to say

$$q^\lambda - 2gq^{\lambda/2} + 1 > \lambda R$$

which is absurd. Therefore $\lambda = 1$ or 3 and $g = 2$ or 6 .

If g is odd then $g = 2\lambda + 1$ and necessarily $\lambda = 1$ or 3 for if $\lambda = 5$ then $g = 11$ and

$$q^\lambda - 2gq^{\lambda/2} + 1 - \lambda(g + 1) > 1836 > 0$$

which again gives us a contradiction. Therefore $\lambda = 1$ or 3 and $g = 3$ or 7 .

Now suppose λ is even. If g is even, we have $g = 2\lambda$ and then $\lambda = 2$ or 4 , for if $\lambda = 6$, $g = 12$ and

$$q^{\lambda-1} - 2gq^{(\lambda-1)/2} + 1 - (\lambda - 1)R \geq q^{\lambda-1} - 2gq^{(\lambda-1)/2} + 1 - (\lambda - 1)(g + 1) > 1719$$

implying

$$q^{\lambda-1} - 2gq^{(\lambda-1)/2} + 1 > (\lambda - 1)R$$

which is impossible. Therefore $\lambda = 2$ or 4 and $g = 4$ or 8 .

Finally, if g is odd, we have $g = 2\lambda + 1$. If $\lambda = 6$ then $g = 13$ and

$$q^{\lambda-1} - 2gq^{(\lambda-1)/2} + 1 - (\lambda - 1)(g + 1) > 1602$$

which is contradictory. Therefore $\lambda = 2$ or 4 and $g = 5$ or 9 .

In conclusion, if $q = 5$ we have $2 \leq g \leq 9$.

Case $q = 4$. In this case we are going to see that we can improve the bound for R . By the rule (12) of Theorem 8 in [M1] we have that if P_i is a prime of $k(x)$ which ramifies in K then $d(\mathfrak{P}_i | P_i) = (\lambda_i + 1)(2 - 1) \geq 2$. Here we are assuming that $K = k(x, y)$ where

$$y^2 - y = f(x) = \frac{q(x)}{p_1(x)^{\lambda_1} p_2(x)^{\lambda_2} \cdots p_R(x)^{\lambda_R}}.$$

Using this we see that

$$2g + 2 = \deg(\text{Diff}(K/k(x))) = \sum_{i=1}^R d(\mathfrak{P}_i | P_i) \deg(\mathfrak{P}_i) \geq 2 \sum_{i=1}^R \deg(\mathfrak{P}_i) \geq 4R$$

and consequently

$$R \leq \frac{g + 1}{2}.$$

Now, suppose λ is odd. If g is even then $g = 2\lambda$, and for this reason if $\lambda = 5$ we must have $g = 10$ and

$$q^\lambda - 2gq^{\lambda/2} + 1 - \lambda R \geq q^\lambda - 2gq^{\lambda/2} + 1 - \lambda \cdot \frac{g + 1}{2} > 357$$

implying

$$q^\lambda - 2gq^{\lambda/2} + 1 > \lambda R$$

which is absurd. Therefore $\lambda = 1$ or 3 and from this it follows that $g = 2$ or 6 .

If g is odd, we have $g = 2\lambda + 1$. If $\lambda = 5$ then $g = 11$ and

$$q^\lambda - 2gq^{\lambda/2} + 1 - \lambda R \geq q^\lambda - 2gq^{\lambda/2} + 1 - \lambda \cdot \frac{g+1}{2} \geq 291$$

which gives us a contradiction. Consequently, $\lambda = 1$ or 3 and $g = 3$ or 7 .

Now consider λ is even. If g is even, $g = 2\lambda$, in this way if $\lambda = 6$, $g = 12$ and

$$q^{\lambda-1} - 2gq^{(\lambda-1)/2} + 1 - (\lambda-1)R \geq q^{\lambda-1} - 2gq^{(\lambda-1)/2} + 1 - (\lambda-1) \left(\frac{g+1}{2} \right) > 224$$

which is absurd. Therefore $\lambda = 2$ or 4 and then $g = 4$ or 8 .

Finally, if g is odd then $g = 2\lambda + 1$, therefore if $\lambda = 6$ then $g = 13$ and

$$q^{\lambda-1} - 2gq^{(\lambda-1)/2} + 1 - (\lambda-1)R \geq q^{\lambda-1} - 2gq^{(\lambda-1)/2} + 1 - (\lambda-1) \left(\frac{g+1}{2} \right) \geq 158$$

which is impossible. Therefore $\lambda = 2$ or 4 and $g = 5$ or 9 .

To conclude, if $q = 4$ then $2 \leq g \leq 9$.

Case $q = 3$. Now we adjust the upper bound for R . If $P \in \mathbb{P}_{k(x)}$ ramifies in K , then $\text{Conorm}(P) = \mathfrak{P}^2$ for some $\mathfrak{P} \in \mathbb{P}_K$, and we have $f(\mathfrak{P}|P) = 1$, which gives us $\deg(\mathfrak{P}) = \deg(P)$. Besides if $P_1, \dots, P_R \in \mathbb{P}_{k(x)}$ are the primes of $k(x)$ ramifying in K , and $\mathfrak{P}_i \in \mathbb{P}_K$ is such that $\mathfrak{P}_i|P_i$, then we have

$$\text{Diff}(K/k(x)) = \prod_{i=1}^R \mathfrak{P}_i^{d(\mathfrak{P}_i|P_i)},$$

but by Theorem 2 in [M1], $d(\mathfrak{P}_i|P_i) = e(\mathfrak{P}_i|P_i) - 1 = 2 - 1 = 1$, and then

$$\text{Diff}(K/k(x)) = \prod_{i=1}^R \mathfrak{P}_i,$$

and by taking degrees

$$\deg(\text{Diff}(K/k(x))) = \sum_{i=1}^R \deg(\mathfrak{P}_i) = \sum_{i=1}^R \deg(P_i).$$

Now, for each $j \in \mathbb{N}$, let R_j be the number of primes of degree j of $k(x)$ ramifying in K . We then have

$$\deg(\text{Diff}(K/k(x))) = \sum_{i=1}^R \deg(P_i) = \sum_{j=1}^{\infty} jR_j, \quad R = \sum_{j=1}^{\infty} R_j.$$

This lets us give an upper bound for R if we consider the fact that R increases as each R_j does, and since the degree of the Different is fixed for a fixed genus, the greatest possible values for R_j are reached for small values of j . Besides, if $P \in \mathbb{P}_{k(x)}$ ramifies in K , let us say $P = P_{p(x)}$ for some monic irreducible polynomial $p(x) \in k[x]$, then $\deg(P) = \deg(p(x))$. Therefore if we count the number of monic irreducible polynomials of the same degree as we have in $k[x]$ we will know how many

places of certain degree we have. Recall that if $N_q(j)$ is the number of monic irreducible polynomials of degree j in $\mathbb{F}_q[x]$, then

$$N_q(j) = \frac{1}{j} \sum_{d|j} \mu\left(\frac{j}{d}\right) q^d = \frac{1}{j} \sum_{d|j} \mu(d) q^{j/d},$$

where μ is the Möbius function.

Since no prime of degree 1 ramifies, we start counting from the primes of degree 2. Then we have $N_3(2) = 3$ and $N_3(3) = 8$.

Suppose λ is odd. For $\lambda = 7$ we have that if g is even, then $g = 14$ and $\deg(\text{Diff}(K/k(x))) = 30$. Since $2N_3(2) + 3N_3(3) = 30$, we see that the greatest value for R_2 is $N_3(2)$ and the greatest possible value for R_3 is $N_3(3)$, therefore $R \leq 3 + 8 = 11$. Nevertheless

$$q^\lambda - 2gq^{\lambda/2} + 1 - \lambda R \geq 3^7 - 28 \cdot 3^{7/2} + 1 - 7 \cdot 11 > 801$$

which is absurd. If g is odd, $g = 15$ and $\deg(\text{Diff}(K/k(x))) = 32$. Since $2N_3(2) + 3N_3(3) < 32$, we need to involve primes with degree 4, and because of this we calculate $N_3(4) = 18$. We are interested then in the possible integral solutions of the equation

$$2\alpha + 3\beta + 4\gamma = 32$$

where $0 \leq \alpha \leq 3$, $0 \leq \beta \leq 8$, $0 \leq \gamma \leq 18$. We also want those solutions providing the greatest possible value for $\alpha + \beta + \gamma$. It is not hard to see that the greatest possible value for $\alpha + \beta + \gamma$ is 11, and we can reach this value by taking either $(\alpha, \beta, \gamma) = (2, 8, 1)$ or $(\alpha, \beta, \gamma) = (3, 6, 2)$. So, $R \leq 11$ and

$$q^\lambda - 2gq^{\lambda/2} + 1 - \lambda R \geq 3^7 - 30 \cdot 3^{7/2} + 1 - 7 \cdot 11 > 708$$

which leads us to a contradiction. Therefore if λ is odd, then $\lambda = 1, 3$ or 5 and consequently $g = 2, 3, 6, 7, 10$ or 11 .

Now consider the case when λ is even. Suppose $\lambda = 8$. If g is even, then $g = 16$ and $\deg(\text{Diff}(K/k(x))) = 34$. Again, we want the integral solutions of the equation

$$2\alpha + 3\beta + 4\gamma = 34$$

with $0 \leq \alpha \leq 3$, $0 \leq \beta \leq 8$, $0 \leq \gamma \leq 18$, and such that $\alpha + \beta + \gamma$ reaches its greatest possible value. In this case, the solutions satisfying these conditions are $(\alpha, \beta, \gamma) = (3, 8, 1)$ and $\alpha + \beta + \gamma = 12$. Therefore $R \leq 12$ and

$$q^{\lambda-1} - 2gq^{(\lambda-1)/2} + 1 - (\lambda-1)R \geq 3^7 - 32 \cdot 3^{7/2} + 1 - 7 \cdot 12 > 607$$

which is absurd. If g is odd, then $g = 17$ and $\deg(\text{Diff}(K/k(x))) = 36$. If we solve $2\alpha + 3\beta + 4\gamma = 36$ as before, we obtain that the maximum value for $\alpha + \beta + \gamma$ is 12 and it is reached if $(\alpha, \beta, \gamma) = (2, 8, 2)$ or $(3, 6, 3)$. In this way, $R \leq 12$ and

$$q^{\lambda-1} - 2gq^{(\lambda-1)/2} + 1 - (\lambda-1)R \geq 3^7 - 34 \cdot 3^{7/2} + 1 - 7 \cdot 12 > 513$$

which is impossible. Therefore, if λ is even, we have $\lambda = 2, 4$ or 6 and consequently $g = 4, 5, 8, 9, 12$ or 13 .

To conclude, if $q = 3$, then $2 \leq g \leq 13$.

Case $q = 2$. In a similar way as in the case $q = 4$, we have $R \leq (g + 1)/2$.

Assume that λ is odd. If g is even and $\lambda = 13$, we have $g = 26$ and

$$q^\lambda - 2gq^{\lambda/2} + 1 - \lambda R \geq 2^{13} - 52 \cdot 2^{13/2} + 1 - 13 \cdot \frac{27}{2} > 3310.$$

Now, if g is odd and $\lambda = 7$, then $g = 27$ and

$$q^\lambda - 2gq^{\lambda/2} + 1 - \lambda R \geq 2^{13} - 54 \cdot 2^{13/2} + 1 - 13 \cdot \frac{28}{2} > 3123.$$

Therefore, $\lambda = 1, 3, 5, 7, 9$ or 11 and $g = 2, 3, 6, 7, 10, 11, 14, 15, 18, 19, 22$ or 23 .

Suppose that λ is even. If g is even and $\lambda = 14$, $g = 28$ and

$$q^{\lambda-1} - 2gq^{(\lambda-1)/2} + 1 - (\lambda - 1)R \geq 2^{13} - 56 \cdot 2^{13/2} + 1 - 13 \cdot \frac{29}{2} > 2935.$$

If g is odd and $\lambda = 14$, then $g = 29$ and

$$q^{\lambda-1} - 2gq^{(\lambda-1)/2} + 1 - (\lambda - 1)R \geq 2^{13} - 58 \cdot 2^{13/2} + 1 - 13 \cdot \frac{30}{2} > 2748.$$

In this way $\lambda = 2, 4, 6, 8, 10$ or 12 and $g = 4, 5, 8, 9, 12, 13, 16, 17, 20, 21, 24$, or 25 .

To conclude, if $q = 2$, $2 \leq g \leq 25$. \square

Notice that we do not involve the class number in the preceding theorem; by doing so we can improve the bounds, as we will see in the following theorems.

In order to do this, we are going to show that the class number has the following restriction.

Theorem 3.2. Let K/k be a congruence function field and let $q = |k|$ and g be the order of the field and the genus of K/k respectively. Define

$$S(a) := (q - 1)(q^{2g-1} + 1 - 2gq^{(2g-1)/2}) - a(q^g - 1)(2g - 1).$$

If $S(a) > 0$, then $h_K > a$, where h_K is the class number of K .

Proof. Let K'/k' be a degree $2g - 1$ constant field extension of K/k . Then K'/k' has the same genus as K/k . By the Riemann hypothesis we have

$$|N'_1 - (|k'| + 1)| \leq 2g|k'|^{1/2}$$

where N'_1 is the number of primes of degree one of K' , so

$$N'_1 \geq q^{2g-1} + 1 - 2gq^{(2g-1)/2}. \quad (2)$$

A prime of degree d of K splits in K' as $(d, 2g - 1)$ primes of degree $\frac{d}{(d, 2g-1)}$. Therefore, the primes of degree one of K' are over primes of K with degree a divisor of $2g - 1$. Let P be a prime of degree d dividing $2g - 1$. Then $P \rightarrow \frac{2g-1}{d}P$ is a one-to-one map from the set of such primes to the set of integral divisors of degree $2g - 1$. So, if N is the number of integral divisors of degree $2g - 1$ of K and N_d the number of primes of degree d of K ,

$$N \geq \sum_{d|2g-1} N_d$$

and then

$$(2g-1)N \geq \sum_{d|2g-1} (2g-1)N_d \geq \sum_{d|2g-1} dN_d = N'_1.$$

By using (2) it follows that K has at least

$$\frac{q^{2g-1} + 1 - 2gq^{(2g-1)/2}}{2g-1} \quad (3)$$

integral divisors of degree $2g-1$. On the other hand, the total number of integral divisors of degree $2g-1$ is $\frac{h_K}{q-1} \cdot (q^g - 1)$ [S1, page 160]. From here,

$$\frac{h_K}{q-1} \cdot (q^g - 1) \geq \frac{q^{2g-1} + 1 - 2gq^{(2g-1)/2}}{2g-1},$$

or equivalently

$$h_K \geq \frac{(q-1)(q^{2g-1} + 1 - 2gq^{(2g-1)/2})}{(q^g - 1)(2g-1)}.$$

In this way, if $S(a) > 0$, then

$$h_K \geq \frac{(q-1)(q^{2g-1} + 1 - 2gq^{(2g-1)/2})}{(q^g - 1)(2g-1)} > a,$$

as we wanted. \square

Now we will give a refinement of Theorem 3.1.

Theorem 3.3. *Let K be a quadratic extension of $k(x)$ with exponent 2 null class group. Suppose that all primes of degree one of $k(x)$ are inert in K . If $|k| = q$ and g are the order of the field and the genus of K respectively then the class number h_K of K/k is a power of 2 and*

1. $q = 5$,

$g = 2$	$h_K = 8$ or 16
$g = 3$	$h_K = 32$ or 64
$g = 4$	$h_K = 128$ or 256
$g = 5$	$h_K = 512$ or 1024
$g = 6$	$h_K = 2048$ or 4096
$g = 7$	$h_K = 8192$ or 16384
$g = 8$	$h_K = 32768$ or 65536
$g = 9$	$h_K = 131072$ or 262144

2. $q = 4$,

$g = 2$	$h_K = 4$
$g = 3$	$h_K = 8$

3. $q = 3$,

$g = 2$	$2 \leq h_K \leq 16$
$g = 3$	$4 \leq h_K \leq 64$
$g = 4$	$8 \leq h_K \leq 256$
$g = 5$	$32 \leq h_K \leq 1024$
$g = 6$	$64 \leq h_K \leq 4096$
$g = 7$	$128 \leq h_K \leq 16384$
$g = 8$	$512 \leq h_K \leq 65536$
$g = 9$	$1024 \leq h_K \leq 262144$
$g = 10$	$4096 \leq h_K \leq 1048576$
$g = 11$	$8192 \leq h_K \leq 4194304$
$g = 12$	$16384 \leq h_K \leq 16777216$
$g = 13$	$65536 \leq h_K \leq 67108864$

4. $q = 2$,

$g = 2$	$h_K = 2$ or 4
$g = 3$	$2 \leq h_K \leq 8$
$g = 4$	$2 \leq h_K \leq 16$
$g = 5$	$2 \leq h_K \leq 32$
$g = 6$	$4 \leq h_K \leq 64$
$g = 7$	$8 \leq h_K \leq 128$
$g = 8$	$8 \leq h_K \leq 256$
$g = 9$	$16 \leq h_K \leq 512$
$g = 10$	$32 \leq h_K \leq 1024$
$g = 11$	$64 \leq h_K \leq 2048$
$g = 12$	$128 \leq h_K \leq 4096$
$g = 13$	$256 \leq h_K \leq 8192$
$g = 14$	$512 \leq h_K \leq 16384$
$g = 15$	$1024 \leq h_K \leq 32768$
$g = 16$	$2048 \leq h_K \leq 65536$
$g = 17$	$2048 \leq h_K \leq 131072$
$g = 18$	$4096 \leq h_K \leq 262144$
$g = 19$	$8192 \leq h_K \leq 524288$
$g = 20$	$16384 \leq h_K \leq 1048576$
$g = 21$	$32768 \leq h_K \leq 2097152$
$g = 22$	$65536 \leq h_K \leq 4194304$
$g = 23$	$131072 \leq h_K \leq 8388608$
$g = 24$	$262144 \leq h_K \leq 16777216$
$g = 25$	$524288 \leq h_K \leq 33554432$

Proof. If k has an odd characteristic then $h_K \leq 2^{2g}$ and this gives us the upper bounds for h_K depending on the genus when $q = 5$ or 3 . If $\text{char}(k) = 2$ then $h_K \leq 2^g$, which gives us the upper bounds for h_K depending on the genus where $q = 4$ or 2 . Both inequalities follow from the theory of the Jacobian (see [M5]). Furthermore, it is clear that h is a power of 2 , since the null class group has exponent 2 . Let $S(q, g, a) := (q-1)(q^{2g-1} + 1 - 2gq^{(2g-1)/2}) - a(q^g - 1)(2g-1)$. Theorem 3.2 gives us that for q and g fixed, if $S(q, g, a) > 0$ then $h_K > a$. This allows us to find the lower bounds for h_K considering that the power of 2 appearing in the table as a lower bound for the class number for given values of q and g , let us say 2^n satisfies that n is the greatest integer for which $S(q, g, 2^{n-1}) > 0$. Finally, for the case $q = 4$, Theorem 3.1 gives us $g \leq 9$. Nevertheless, if $g = 4$, then $h_K \leq 16$. If we use the function S we obtain $S(4, 4, 16) > 0$, and therefore $h_K > 16$, which is absurd and we do not have a function field satisfying such conditions. The same types of contradictions happen if $q = 4$ and $g = 5, 6, 7, 8$ or 9 , and for this reason we have to reduce the list for this case. \square

Now we will estimate the class number by using a different method from the one used in the preceding theorem. For this we need to introduce some new concepts.

Definition 3.1. Let K/k be a function field of one variable over k and let L be a finite Galois extension of K having the same constant field as K . Let P_1, P_2, \dots, P_R be the primes of K ramifying in L . Define $\delta(L/K)$ by

$$\delta(L/K) = \left(n, \frac{n}{e_1} \deg_K(P_1), \dots, \frac{n}{e_R} \deg_K(P_R) \right),$$

where e_i is the ramification index of P_i for $i = 1, \dots, R$ and $n = [L : K]$.

Definition 3.2. Let L and K be as in the previous definition. Let \deg_L be the degree map on C_L^G , where C_L^G is the group of ambiguous divisor classes of L and $G = \text{Gal}(L/K)$. We define $d(L/K)$ as the positive generator of the ideal $\deg_L(C_L^G)$.

The following theorem given by Rosen in [R1] gives us a way to calculate the ambiguous class number for a cyclic extension of prime degree.

Theorem 3.4. Let L, K, k and R be as in Definition 3.1. Suppose L/K is a cyclic extension of degree p , p prime. If J_L^G is the group of ambiguous divisors classes of degree zero then:

1. If $\delta(L/K) = 1$ and $q \not\equiv 1 \pmod{p}$, then $|J_L^G| = h_K p^{R-1}$.
2. If $\delta(L/K) = 1$ and $q \equiv 1 \pmod{p}$, then $|J_L^G| = h_K p^{R-2}$.
3. If $\delta(L/K) = p$, then $|J_L^G| = h_K p^{R-\epsilon}$, where $\epsilon = 1$ if $d(L/K) = 1$ and $\epsilon = 0$ if $d(L/K) = p$.

We are going to use Theorem 3.4 in the following form.

Theorem 3.5. Let K be a quadratic extension of $k(x)$, where k is a finite field with order q , let h_K be its class number and R be the number of primes of $k(x)$ ramifying in K . Suppose the null class group has exponent 2 and all the degree one primes of $k(x)$ are inert in K . Then we have:

1. If there is some $P \in \mathbb{P}_{k(x)}$ with an odd degree ramifying in K , then $h_K = 2^{R-1}$ or $h_K = 2^{R-2}$ if $q \equiv 0 \pmod{2}$ or $q \equiv 1 \pmod{2}$ respectively.
2. If all the primes of $k(x)$ ramifying in K have even degree then $h_K = 2^{R-1}$.

Proof. In a quadratic extension K of $k(x)$, in which the null class group has exponent two, all the classes in this group are ambiguous, that is to say, all are fixed by the Galois group of $K/k(x)$. In this way the class number of K is equal to the ambiguous class number $|J_K^G|$. By the preceding theorem, we have that, if there is a ramified prime of odd degree, then $\delta(K/k(x)) = 1$ and

$$\begin{aligned} q \equiv 0 \pmod{2} &\Rightarrow |J_K^G| = h_{k(x)} 2^{R-1}, \\ q \equiv 1 \pmod{2} &\Rightarrow |J_K^G| = h_{k(x)} 2^{R-2}. \end{aligned}$$

Since $|J_K^G| = h_K$ and $h_{k(x)} = 1$, the result follows in this case. Now consider the case in which all ramified primes have even degree. Then we have $\delta(K/k(x)) = 2$ and the preceding theorem gives us again:

$$|J_K^G| = h_{k(x)} 2^{R-\epsilon}, \quad \epsilon = 0 \text{ or } 1,$$

and for this $h_K = 2^{R-\epsilon}$ with $\epsilon = 0$ or 1 . Nevertheless, there is a well-known theorem due to Schmidt (see [M4, page 69]) that can be used to calculate the ambiguous class number of K . In particular, since K is a geometric quadratic extension of $k(x)$ with the null class group of exponent two and in which all primes of degree one of $k(x)$ are inert, $|J_K^G| \leq 2^{R-1}$, and it follows that $h_K = 2^{R-1}$. \square

We will also need a formula that will let us relate the genus g of the quadratic extension K with the ramified primes of $k(x)$ and its degrees. When $\text{char}(k) = 2$, K/k is an Artin–Schreier extension and such relation is given by the equality

$$g = \frac{1}{2} \left(-2 + \sum_{i=1}^l (\lambda_i + 1) \deg(P_i) \right)$$

where $P_i = P_{p_i(x)} \in k(x)$ (see Theorem III.7.8 in [S1, page 115]). Since $\deg(p_i(x)) = \deg(P_i)$ the last equality becomes

$$g = \frac{1}{2} \left(-2 + \sum_{i=1}^l (\lambda_i + 1) \deg(p_i(x)) \right)$$

or equivalently

$$\sum_{i=1}^l (\lambda_i + 1) \deg(p_i(x)) = 2g + 2. \quad (4)$$

If we suppose $0 < \text{char}(k) \neq 2$, then K is a Kummer extension of $k(x)$ and the equality we have according to the standard form of the generating equation is

$$g = -1 + \frac{1}{2} \sum_{i=1}^l \deg(P_i)$$

(see Theorem III.7.3 in [S1, page 110]) or equivalently

$$\sum_{i=1}^l \deg(p_i(x)) = 2g + 2. \quad (5)$$

Now we can give a new approximation for the bounds.

Theorem 3.6. *Let K be a quadratic extension of $k(x)$, where k is a finite field with order q , let h_K be its class number and $\delta = \delta(K/k(x))$. If the null class group has exponent 2 and all the degree one primes of $k(x)$ are inert, then we have:*

1. We do not have function fields satisfying these conditions if $q = 5$.
2. We do not have function fields satisfying these conditions if $q = 4$.
3. $q = 3$,

$g = 2$	$h_K = 2$ or 4	$\delta = 2$
$g = 3$	$h_K = 4$ or 8	$\delta = 2$
$g = 4$	$h_K = 8$ or 16	$\delta = 2$
$g = 5$	$h_K = 32$	$\delta = 2$
$g = 6$	$h_K = 64$	$\delta = 2$
$g = 7$	$h_K = 128$	$\delta = 2$

4. $q = 2$,

$g = 3$	$h_K = 2$	$\delta = 2$
$g = 4$	$h_K = 2$	$\delta = 1$ or 2
$g = 5$	$h_K = 2$	$\delta = 1$ or 2
	$h_K = 4$	$\delta = 2$
$g = 6$	$h_K = 4$	$\delta = 1$ or 2
$g = 7$	$h_K = 8$	$\delta = 2$
$g = 8$	$h_K = 8$	$\delta = 1$ or 2
$g = 9$	$h_K = 16$	$\delta = 2$

Proof. Recall that, since all primes of degree one of $k(x)$ are inert in K , $R \leq g + 1$, where R is the number of primes of $k(x)$ ramifying in K .

Case $q = 5$. Theorem 3.3 asserts that $2 \leq g \leq 9$. Suppose there is a prime of $k(x)$ with an odd degree ramifying in K . Since $5 \equiv 1 \pmod{2}$, because of Theorem 3.5 we have $h_K = 2^{R-2} \leq 2^{g-1} \leq 256$. Therefore, again by Theorem 3.3 we have that $g \leq 4$. If P is a prime of $k(x)$ with an odd degree ramifying in K , then $\deg(P) \geq 3$ since no degree one prime ramifies. We can assume, without loss of generality that $\deg(P_1) \geq 3$. Then by using (5) we obtain

$$3 + \sum_{i=2}^R \deg(p_i(x)) \leq \sum_{i=1}^R \deg(p_i(x)) = 2g + 2$$

and for this

$$2(R - 1) \leq \sum_{i=2}^R \deg(p_i(x)) \leq 2g - 1$$

or equivalently

$$R - 2 \leq g - \frac{3}{2}.$$

In this way, for $g = 2$ we have $h_K = 2^{R-2} \leq 2^{1/2} \leq 1.42$, which contradicts Theorem 3.3 and therefore $g \neq 2$. If $g = 3$, then $h_K \leq 2$ and if $g = 4$, $h_K \leq 5$ which also gives us contradictions to Theorem 3.3. Consequently, in this case we obtain $g \leq 1$, which is absurd.

Now suppose that all primes of $k(x)$ ramifying have an even degree. Then because of Theorem 3.5 $h_K = 2^{R-1} \leq 2^g \leq 512$. Therefore, using Theorem 3.3 we see that $g \leq 5$. If $g = 2$, then $h_K = 2^{R-1} \leq 4$ which gives us a contradiction to Theorem 3.3 and consequently $g \neq 2$. For $g = 3, 4$ and 5 we obtain $h_K \leq 8, 16$ and 32 respectively and Theorem 3.3 gives us again that this is impossible. Therefore $g \leq 1$, and from here it follows that there are no function fields in this case.

In conclusion if $q = 5$, there are no function fields satisfying the conditions established in the theorem.

Case $q = 4$. Because of Theorem 3.3, we have $2 \leq g \leq 3$. As in the proof of Theorem 3.1, we have

$$R \leq \frac{g+1}{2},$$

and in this way, because of Theorem 3.5, $h_K \leq 2^{R-1} \leq 2^{(g-1)/2} \leq 2$. Therefore, it follows from Theorem 3.3 that there are no function fields satisfying the given conditions.

Case $q = 3$. In this case, $2 \leq g \leq 13$. Suppose there is a prime of $k(x)$ with an odd degree ramifying in K . Since $3 \equiv 1 \pmod{2}$, we have $h_K = 2^{R-2}$. In the same way as in the case $q = 5$, we can see that

$$R - 2 \leq g - \frac{3}{2},$$

implying $h_K \leq 2^{(2g-3)/2}$ and

if $g =$	then $h_K \leq$
2	1
3	2
4	5
5	11
6	22
7	45
8	90
9	181
10	362
11	724
12	1448
13	2896

and by comparing this table with the corresponding table in Theorem 3.3 we see that g cannot be greater than 1. Therefore, there are no function fields with these characteristics.

Now suppose that all ramified primes of $k(x)$ have an even degree. Then $h_K = 2^{R-1} \leq 2^g$. In this way

if $g =$	then $h_K \leq$
2	4
3	8
4	16
5	32
6	64
7	128
8	256
9	512
10	1024
11	2048
12	4096
13	8192

and by comparing this table with the one in Theorem 3.3 we see that

$g = 2$	$h_K = 2$ or 4
$g = 3$	$h_K = 4$ or 8
$g = 4$	$h_K = 8$ or 16
$g = 5$	$h_K = 32$
$g = 6$	$h_K = 64$
$g = 7$	$h_K = 128$

which gives us the desired result for $q = 3$.

Case $q = 2$. In this case we have $2 \leq g \leq 25$ and in the same way as in the case $q = 4$ we also have

$$R \leq \frac{g+1}{2},$$

implying $h_K \leq 2^{R-1} \leq 2^{(g-1)/2} \leq 4096$ and because of Theorem 3.3, $g \leq 18$. Suppose there is a prime of $k(x)$ with an odd degree ramifying in K . Since $2 \equiv 0 \pmod{2}$, we have $h_K = 2^{R-1}$. Suppose that $\deg(P_1) \geq 3$. Then by using (4) we see that

$$2 \left(3 + \sum_{i=2}^R \deg(p_i(x)) \right) \leq \sum_{i=1}^R (\lambda_i + 1) \deg(p_i(x)) = 2g + 2$$

which gives us

$$2(R-1) \leq \sum_{i=2}^R \deg(p_i(x)) \leq g-2$$

or equivalently

$$R-1 \leq \frac{g-2}{2},$$

and therefore $h_K = 2^{R-1} \leq 2^{(g-2)/2}$. In this way we obtain

if $g =$	then $h_K \leq$
2	1
3	1
4	2
5	2
6	4
7	4
8	8
9	8
10	16
11	16
12	32
13	32
14	64
15	64
16	128
17	128
18	256

and by comparing with Theorem 3.3 we see that

$g = 4$	$h_K = 2$
$g = 5$	$h_K = 2$
$g = 6$	$h_K = 4$
$g = 8$	$h_K = 8$

Now suppose that all ramified primes of $k(x)$ have an even degree. Then $h_K = 2^{R-1}$. Therefore

$$h_K = 2^{R-1} \leq 2^{(g-1)/2}.$$

In this way

if $g =$	then $h_K \leq$
2	1
3	2
4	2
5	4
6	4
7	8
8	8
9	16
10	16
11	32
12	32
13	64
14	64
15	128
16	128
17	256
18	256

If we compare with Theorem 3.3 we see that

$g = 3$	$h_K = 2$
$g = 4$	$h_K = 2$
$g = 5$	$h_K = 2$ or 4
$g = 6$	$h_K = 4$
$g = 7$	$h_K = 8$
$g = 8$	$h_K = 8$
$g = 9$	$h_K = 16$

and with this we finish the proof of Theorem 3.6. \square

Finally we obtain the result involving the ideal class group.

Theorem 3.7. *If K is a quadratic extension of $k(x)$ with genus g , where k is a finite field with order q , in which all primes of degree one of $k(x)$ are inert in K , and if the ideal class group has exponent two and order h , then:*

1. *There are no function fields of this type if $q = 5$.*
2. *There are no function fields of this type if $q = 4$.*
3. $q = 3$,

$g = 2$	$h = 4$ or 8	$\delta = 2$
$g = 3$	$h = 8$ or 16	$\delta = 2$
$g = 4$	$h = 16$ or 32	$\delta = 2$
$g = 5$	$h = 64$	$\delta = 2$
$g = 6$	$h = 128$	$\delta = 2$
$g = 7$	$h = 256$	$\delta = 2$

4. $q = 2$,

$g = 2$	$h = 2$	$\delta = 1$
$g = 3$	$h = 4$	$\delta = 2$
$g = 4$	$h = 4$	$\delta = 1$ or 2
$g = 5$	$h = 4$	$\delta = 1$ or 2
	$h = 8$	$\delta = 2$
$g = 6$	$h = 8$	$\delta = 1$ or 2
$g = 7$	$h = 16$	$\delta = 2$
$g = 8$	$h = 16$	$\delta = 1$ or 2
$g = 9$	$h = 32$	$\delta = 2$

Proof. Since the null class group in an imaginary extension is a subgroup of the ideal class group, the null class group must have an exponent of 2 or be of order 1. Let h_K be the order of C_K^0 . Then $h = f_\infty h_K$ where f_∞ is the inertia degree of the infinite prime of $k(x)$. Madan and Queen have shown that there are only two cases in which a quadratic extension of $k(x)$ has class number 1 and genus $g > 1$. In both cases $q = 2$ and $g = 2$; therefore if $q = 2$ and $g = 2$, then $h = 2$. Nevertheless, only one example satisfies the condition of all the degree one primes being inert, namely, $K = \mathbb{F}_2(x, y)$ where

$$y^2 + y = \frac{x^3 + x^2 + 1}{x^3 + x + 1}.$$

Now, if C_K^0 has an exponent of 2, the result follows from the preceding theorem. \square

4. Further analysis of the cases

Next we will make a proposition establishing the form of the extensions under the conditions considered in this work.

Proposition 4.1. Let K be a quadratic extension of $k(x)$, where k is a finite field with order q , let h_K be its class number and g its genus. If the null class group has exponent 2 and all primes of degree one of $k(x)$ are inert, then:

1. For $q = 3$,

- If $g = 2$ and $h_K = 2$ then $K = k(x, y)$ with generating equation

$$y^2 = p_1(x)p_2(x),$$

where $p_1(x)$ is a polynomial of degree 2 and $p_2(x)$ is a polynomial of degree 4, both being monic and irreducible over $\mathbb{F}_3[x]$. If $h_K = 4$ then $K = k(x, y)$ with generating equation

$$y^2 = (x^2 + 1)(x^2 + x + 2)(x^2 + 2x + 2).$$

- If $g = 3$ and $h_K = 4$ then $K = k(x, y)$ with generating equation

$$y^2 = p_1(x)p_2(x)p_3(x),$$

where $p_1(x), p_2(x)$ are distinct polynomials of degree 2 and $p_3(x)$ is a polynomial of degree 4, all being monic and irreducible over $\mathbb{F}_3[x]$.

- If $g = 4$ then $K = k(x, y)$ with generating equation

$$y^2 = (x^2 + 1)(x^2 + x + 2)(x^2 + 2x + 2)p(x),$$

for a monic polynomial $p(x)$ of degree 4 being irreducible over $\mathbb{F}_3[x]$.

- For $g = 5, 6$ and 7 there are no examples satisfying the hypothesis.

2. For $q = 2$,

- If $g = 4$ then $K = k(x, y)$ with generating equation

$$y^2 + y = \frac{q(x)}{(x^2 + x + 1)p(x)},$$

where $q(x)$ is a polynomial of degree 5 and $p(x)$ is a polynomial of degree 3, both being irreducible over $\mathbb{F}_2[x]$, and satisfying also

$$(q(x), (x^2 + x + 1)p(x)) = 1.$$

- If $g = 5$ and $h_K = 2$ then $K = k(x, y)$ with generating equation given either by

$$y^2 + y = \frac{q(x)}{(x^2 + x + 1)p(x)},$$

where $q(x)$ is a polynomial of degree 6 and $p(x)$ is a polynomial of degree 4, both being irreducible over $\mathbb{F}_2[x]$, satisfying the additional condition

$$(q(x), (x^2 + x + 1)p(x)) = 1;$$

or, with generating equation

$$y^2 + y = \frac{q(x)}{(x^3 + x + 1)(x^3 + x^2 + 1)},$$

where $q(x)$ is a polynomial of degree 6 being irreducible over $\mathbb{F}_2[x]$, satisfying also

$$(q(x), (x^3 + x + 1)(x^3 + x^2 + 1)) = 1.$$

If $h_K = 4$ there are no examples satisfying the given hypothesis.

- For $g = 3, 6, 7, 8$ and 9 there are no examples satisfying the given hypothesis.

Proof. In this proof we use equalities (4) and (5).

Case $q = 3$. Since $\delta = 2$ independently of the genus (see Theorem 3.6), we have that all primes ramifying have an even degree. Furthermore, from Theorem 3.5 we have $h_K = 2^{R-1}$, where R is the number of primes of $k(x)$ ramifying in K .

For $g = 2$, we have then by using Theorem 3.6 that $h_K = 2$ or 4 . If $h_K = 2$ then $R = 2$ and from (5) we have

$$\deg(p_1(x)) + \deg(p_2(x)) = 6$$

and in this way, the only possibility is that $\deg(p_1(x)) = 2$ and $\deg(p_2(x)) = 4$. Now, if $h_K = 4$ then $R = 3$ and again it follows from (5) that

$$\deg(p_1(x)) + \deg(p_2(x)) + \deg(p_3(x)) = 6,$$

and the only possible solution to the last equality is given by $\deg(p_1(x)) = \deg(p_2(x)) = \deg(p_3(x)) = 2$. Therefore, the proposition is proved in this case. The analysis of the cases in which the genus is equal to 3 and 4 is completely analogous, considering the fact that there are only three monic polynomials of degree 2 being irreducible over $\mathbb{F}_3[x]$, namely $x^2 + 1$, $x^2 + x + 2$ and $x^2 + 2x + 2$, which gives us the reason why the generating equation has the described form when $g = 4$.

Now, when $g = 5, 6$ and 7 , the solution to the equality (5) formulated in each case involves more than three monic polynomials of degree 2 being irreducible over $\mathbb{F}_3[x]$, which is impossible because as we just said we only have three of such polynomials. Therefore, in these cases we cannot find examples satisfying the given hypothesis.

Case $q = 2$. Because of Theorem 3.5 we have $h_K = 2^{R-1}$ for any value of δ and g .

For $g = 3$, Theorem 3.6 gives us that $h_K = 2$, and from this $R = 2$. In this way Eq. (4) becomes

$$(\lambda_1 + 1) \deg(p_1(x)) + (\lambda_2 + 1) \deg(p_2(x)) = 8$$

for which the only possible solution is given by $\lambda_1 = \lambda_2 = 1$ and $\deg(p_1(x)) = \deg(p_2(x)) = 2$. Nevertheless, there is only one monic polynomial of degree 2 being irreducible over $\mathbb{F}_2[x]$, so we cannot find examples in this case.

For $g = 4$, we have $h_K = 2$ and $R = 2$. Eq. (4) becomes

$$(\lambda_1 + 1) \deg(p_1(x)) + (\lambda_2 + 1) \deg(p_2(x)) = 10.$$

In order to solve this equality we use the fact that $0 < \lambda_i \leq g$, $(\lambda_i, 2) = 1$ (see Theorem 8 in [M1]), therefore λ_i is odd and $2 \leq \deg(p_i(x)) \leq g + 1$. With these restrictions we have that the only possible solutions to the equality are $(\lambda_1, \deg(p_1(x)), \lambda_2, \deg(p_2(x))) = (1, 2, 1, 3)$ and $(1, 2, 2, 2)$. Nevertheless, we see again that the solution $(1, 2, 2, 2)$ is not possible since it requires the existence of two monic polynomials of degree 2 being irreducible over $\mathbb{F}_2[x]$. In this way the generating equation has the form

$$y^2 + y = \frac{q(x)}{(x^2 + x + 1)p(x)},$$

where $q(x)$ is a polynomial with a certain degree which we are going to calculate and $p(x)$ is a polynomial of degree 3, both being irreducible over $\mathbb{F}_2[x]$, satisfying also the condition

$$(q(x), (x^2 + x + 1)p(x)) = 1.$$

In order to calculate the degree of $q(x)$ we are going to use Proposition 2.10 in [L1], which asserts that if K/k ($\text{char}(k) = 2$) is a hyperelliptic function field with genus g such that $K/k(x)$ is an imaginary quadratic extension, and if the infinite prime is inert then

$$\deg(q(x)) = 2g + 2 - \sum_{i=1}^R \lambda_i \deg(p_i(x)).$$

From this, $\deg(q(x)) = 5$, which gives us the desired result in this case.

The analysis for the remaining cases for $q = 2$ is analogous to the two cases discussed. \square

It is important to note that this proposition does not give us a sufficiency condition. Therefore, although we have established which *should* be the form of a particular quadratic extension, this is not a guarantee that such an extension satisfies the conditions given in the hypothesis.

This proposition lets us have a better idea of the form of the extension we are considering. Besides having a model for the generating equation, we can check if the extension described by such an equation satisfies the hypothesis conditions as we will see in the next section.

5. Computational analysis

To make the computational analysis we used the free software KASH, version 2.5, available at <http://www.math.tu-berlin.de/~kant/kash.html>, allowing us to define function fields of one variable and calculate some of its associated invariants such as the genus, class number, among others.

We start by explaining the instructions used to define the function fields and to calculate their class numbers. First, we have to define the finite field in which we are going to work. To do this we use the instruction

```
kash > k := FF(p, n);
```

which defines k as a finite field with order p^n . Then we use the instruction

```
kash > AlffInit(k, "x", "y");
```

which establishes k as the constant field, defines the variables x and y and the polynomial ring $k[x]$, the field $k(x)$ and the ring $k[x][y]$. If we save the generating equation in the variable f in the following way

```
kash > f := φ(x, y);
```

then we can define the function field $K = k(x, y)$ with generating equation $\varphi(x, y) = 0$ ($\varphi(x, y) \in k[x, y]$) by means of the instruction

```
kash > AlffOrders(f);
```

which defines the variable F as K . We can then calculate the genus of K using

$$\text{kash} > \text{AlffGenus}(F);$$

or we can calculate the class number and the decomposition of the null class group in the following way

$$\text{AlffClassGroup}(F);$$

which gives us an answer in the form

$$[h_K, [c_1, \dots, c_s]]$$

where h_K is the class number of the function field and the integers satisfy the equality

$$C_K^0 \cong \mathbb{Z}/c_1\mathbb{Z} \times \dots \times \mathbb{Z}/c_s\mathbb{Z}.$$

We can then analyze all the generating equations in Proposition 4.1. For the case $q = 3$ this can be done in a direct way, for example when $g = 2$, $h_K = 4$ we have that the generating equation must have the form

$$y^2 - (x^2 + 1)(x^2 + x + 2)(x^2 + 2x + 2) = 0$$

so we define $f := y^2 - (x^2 + 1)(x^2 + x + 2)(x^2 + 2x + 2)$ and we do the computing in KASH. By using the instruction `AlffClassGroup` we obtain

$$[36, [6, 6]]$$

which means that $h_K = 36$ and $C_K^0 \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, that is to say, there is no example satisfying such hypothesis. If we do the same calculation with all the generating equations obtained in Proposition 4.1 for $q = 3$, we see that there is no example of an imaginary quadratic extension $K/\mathbb{F}_3(x)$ such that the null class group has an exponent of 2 and all primes of degree one being inert.

Now, for $q = 2$ we need to modify the generating equation so we can do the calculations, since the instruction `AlffOrders` use a polynomial $\varphi(x, y) \in k[x, y]$ as an input. In order to do this, if the generating equation is given by

$$y^2 + y + \frac{q(x)}{d(x)} = 0,$$

we use the change of variable $y' = d(x)y$. In this way, the generating equation becomes the equivalent equation $(y')^2 + d(x)y' + d(x)q(x) = 0$. Now we can define $f := y'^2 + d(x)y' + d(x)q(x)$ and do the calculations. For example, for $g = 4$ and $h_K = 2$ a generating equation is given by

$$y^2 + y = \frac{x^5}{(x^2 + x + 1)(x^3 + x + 1)}$$

which, under the change of the variable described before becomes

$$y^2 + (x^2 + x + 1)(x^3 + x + 1)y + (x^2 + x + 1)(x^3 + x + 1)x^5 = 0.$$

In this way we can define $f := y^2 + (x^2 + x + 1)(x^3 + x + 1)y + (x^2 + x + 1)(x^3 + x + 1)x^5$ and do the calculations. By using the instruction `AlffClassGroup` we obtain

$$[10, [10]]$$

and from this we can conclude that $h_K = 10$ and $C_K^0 \cong \mathbb{Z}/10\mathbb{Z}$. If we analyze the remaining candidates for generating equations for this case we see that no function field defined by such equations has class number $h_K = 2$, so we do not have examples in this case. Furthermore, when we do the same calculation for the remaining cases described in Proposition 4.1, we see that we cannot find an example of an imaginary quadratic extension $K/\mathbb{F}_2(x)$ in which the null class group has exponent 2 and in which all the degree one primes of $\mathbb{F}_2(x)$ are inert in K .

6. Conclusions

In the computational analysis described in the preceding section we could not find any examples. This suggests a new version of Theorem 3.7, which we enunciated in the Introduction in the form of Theorem 1.1.

This result, together with the ones appearing in [B-D] would give the complete classification of all the imaginary quadratic extensions of $k(x)$ with the exponent two ideal class group, as we explained in the Introduction.

The results obtained in the preceding section seem to suggest

Theorem 6.1. *If K is an imaginary quadratic extension of $k(x)$, where k is a finite field with order $q > 2$, in which the null class group has exponent 2, there is a prime of degree one of $k(x)$ ramifying in K .*

Acknowledgments

We thank Dinesh Thakur for his help and suggestions, and we also want to thank the referee for his patience reading this article, corrections and the suggestion of two nice proofs for some of the facts stated in the paper.

References

- [B-D] V. Bautista-Ancona, J. Diaz-Vargas, Quadratic function fields with exponent two ideal class group, *J. Number Theory* 116 (2006) 21–41.
- [L1] D. Le Brigand, Quadratic algebraic function fields with ideal class number two, in: *Arithmetic, Geometry and Coding Theory*, Luminy, 1993, de Gruyter, Berlin, 1996, pp. 105–126.
- [M1] M. Madan, D. Madden, The exponent of class groups in congruence function fields, *Acta Arith.* XXXII (1977) 183–205.
- [M2] M. Madan, C. Queen, Algebraic function fields of class number one, *Acta Arith.* XX (1972) 423–432.
- [M3] D. Madden, Quadratic function fields with invariant class group, *J. Number Theory* 9 (2) (1977) 218–228.
- [M4] M. Moriya, Rein arithmetisch-algebraischer Aufbau der Klassenkörper theorie über algebraischen Funktionenkörpern einer Unbestimmten mit endlichem Konstantenkörper, *Jpn. J. Math.* 15 (1938) 67–84.
- [M5] D. Mumford, *Abelian Varieties*, 2nd edition, Oxford University Press, Oxford, 1974.
- [R1] M. Rosen, Ambiguous divisor classes in function fields, *J. Number Theory* 9 (1977) 160–174.
- [R2] M. Rosen, *Number Theory in Function Fields*, Springer-Verlag, New York, 2002.
- [S1] H. Stichtenoth, *Algebraic Function Fields and Codes*, Universitext, Springer-Verlag, New York, 1993.
- [VS1] G. Villa Salvador, *Topics in the Theory of Algebraic Function Fields*, Birkhäuser, Boston, 2006.