ACTA ARITHMETICA
139.2 (2009)

Function fields with 3-rank at least 2

by

ALLISON M. PACELLI (Williamstown, MA)

1. Introduction. It is well known that there are infinitely many quadratic number fields and function fields with class number divisible by a given integer n (see Nagell [15] (1922) for imaginary number fields, Yamamoto [22] (1969) and Weinberger [21] (1973) for real number fields, and Friesen [6] (1990) for function fields). A related question concerns the n-rank of the field, that is, the greatest integer r for which the class group contains a subgroup isomorphic to $(\mathbb{Z}/n\mathbb{Z})^r$. In [22], Yamamoto showed that infinitely many imaginary quadratic number fields have n-rank at least 2 for any positive integer $n \geq 2$. In 1978, Diaz y Diaz [3] developed an algorithm for generating imaginary quadratic fields with 3-rank 2, and Craig [2] showed in 1973 that there are infinitely many real quadratic number fields with 3-rank at least 2 and infinitely many imaginary quadratic number fields with 3-rank at least 3. A few examples of higher 3-rank have also been found (see for instance Llorente and Quer [14, 18] who found three imaginary quadratic number fields with 3-rank 6 in 1987/1988). In a recent paper [4], Erickson, Kaplan, Mendoza, Shayler, and the author gave infinite, simply parameterized families of real and imaginary quadratic fields with 3-rank 2. Here we give a function field analogue.

Note that Bauer, Jacobson, Lee, and Scheidler [1] have given algorithms which yield imaginary quadratic function fields with 3-rank at least 2 and a possibly empty set of imaginary quadratic function fields with 3-rank at least 3. The construction below yields infinitely many quadratic function fields, of any given signature, with 3-rank at least 2. See [9], [11], [12], [16], and [17] for constructions of function fields of arbitrary degree m with large n-rank for general n.

Throughout we let q be a power of an odd prime, $q \equiv 1 \pmod 3$. We use $\operatorname{sgn}(f)$ to denote the leading coefficient of a polynomial $f \in \mathbb{F}_q[T]$, and we let $|f| = q^{\deg(f)}$ for $f \in \mathbb{F}_q[T]$. The main result is as follows.

2000 *Mathematics Subject Classification*: 11R29, 11R58.
Key words and phrases: 3-rank, class number, class group, quadratic field, function field.

DOI: 10.4064/aa139-2-1

THEOREM 1. *Let $\mathfrak{p}_1$ and $\mathfrak{p}_2$ be any irreducible polynomials over $\mathbb{F}_q[T]$. Let p be any irreducible polynomial of even degree in $\mathbb{F}_q[T]$ such that $2(p^2-1)$ is not a cube modulo $\mathfrak{p}_1$ and $2p(p^2-1)$ is not a cube modulo $\mathfrak{p}_2$. If c and w are any polynomials in $\mathbb{F}_q[T]$ such that*

$$w \equiv \begin{cases} 0 \pmod{p}, \\ 0 \pmod{\mathfrak{p}_1}, \\ -18c \pmod{\mathfrak{p}_2}, \end{cases}$$

$c \equiv 0 \pmod{p^2-1}$, *and* $c \not\equiv 0 \pmod{\mathfrak{p}_1\mathfrak{p}_2}$, *and*

(i) $\deg(w) > \deg(c)$,
(ii) $(-2^{10}3^6c^6)^{(|p|-1)/3} \not\equiv 1 \pmod{p}$,

then

$$\mathbb{F}_q(T)(\sqrt{8c(w^2+18cw+108c^2)[4w^3(p^2-1)-216c(w^2+18cw+108c^2)]})$$

has 3*-rank at least* 2.

We show in Lemma 1 that it is always possible to choose such primes $\mathfrak{p}_1, \mathfrak{p}_2$, and p. As in [4], the idea of the proof is to construct, for each d of the prescribed form, two distinct, unramified, cyclic, cubic extensions of $\mathbb{F}_q(\sqrt{d})$. By class field theory, then, the field has 3-rank at least 2.

2. 3-Rank 2. Recall that the Hilbert class field of a global function field K is the maximal unramified abelian extension of K in which the prime at infinity splits completely, and that $\mathrm{Gal}(H/K) \cong Cl_K$, where Cl_K denotes the ideal class group of K (see [20] for further details about explicit class field theory in function fields). It follows that the class number of K is divisible by 3 if and only if there is a cyclic, cubic, unramified extension of K in which the prime at infinity splits completely. In fact, if K is a quadratic field, then K has 3-rank n if and only if there are exactly $(3^n-1)/2$ such extensions of K ([7]). To prove that a quadratic field K has 3-rank at least 2, therefore, it suffices to show that K has two distinct cyclic, cubic, unramified extensions in which the infinite prime splits completely.

First, notice that we may assume that c and w are relatively prime, because the quadratic field parameterized by c and w is the same as the field parameterized by $c/(c,w)$ and $w/(c,w)$.

In [8], Kishi and Miyake give a characterization of all quadratic number fields with class number divisible by 3. The following is a function field analogue of Kishi and Miyake's result. A proof (of an alternative statement of the theorem) can be found in [10]. A proof of the version below can be found in [5]. The proof is very similar to the number field case, and uses a function field version of a result of Llorente and Nart [13] which gives the decomposition of a prime $P \in \mathbb{F}_q(T)$ in the cubic extension generated by a root of an irreducible cubic polynomial $g(Z) \in \mathbb{F}_q(T)$.

Theorem 2. *Let u and w be relatively prime polynomials in $\mathbb{F}_q[T]$ with leading coefficients α and β, respectively. Suppose that the following conditions hold.*

(i) $d = 4uw^3 - 27u^2$ *is not a square in* $\mathbb{F}_q[T]$.
(ii) $g(Z) = Z^3 - uwZ - u^2$ *is irreducible over* $\mathbb{F}_q[T]$.
(iii) *One of the following conditions holds*:
  (1) $\frac{3}{2}\deg(uw) > \deg(u^2)$.
  (2) $\frac{3}{2}\deg(uw) = \deg(u^2)$ *and* $x^3 - \alpha x + \beta$ *has three distinct roots in* $\mathbb{F}_q$.
  (3) $\frac{3}{2}\deg(uw) < \deg(u^2)$, $3 \mid \deg(u^2)$, *and one of the following*:
    (a) $3 \nmid (q-1)$,
    (b) $3 \mid (q-1)$ *and* $-\beta$ *is a cube in* $\mathbb{F}_q$.

Let θ be any root of $g(Z)$. Then the normal closure L of $\mathbb{F}_q(T)(\theta)$ is a cyclic, cubic, unramified extension of $\mathbb{F}_q(T)(\sqrt{d})$ in which the prime at infinity splits completely; in particular, then, $k = \mathbb{F}_q(T)(\sqrt{d})$ has class number divisible by 3. *Conversely, every quadratic function field k with class number divisible by* 3 *and every unramified cyclic cubic extension of k in which infinity splits is given by a suitable choice of polynomials u and w.*

Let p, $\mathfrak{p}_1$, and $\mathfrak{p}_2$ be as in the statement of Theorem 1; Lemma 1 below shows that such polynomials must exist. Given polynomials c and w, we define polynomials u, x, and y so that the two pairs, u, w and x, y, each satisfy the conditions of Theorem 2 and the cubic fields have discriminants with the same square-free part as

$$d = 8c(w^2 + 18cw + 108c^2)[4w^3(p^2-1) - 216c(w^2 + 18cw + 108c^2)].$$

By Theorem 2, then, $\mathbb{F}_q(T)(\sqrt{d})$ has two cyclic, cubic, unramified extensions L_1 and L_2 in which the prime at infinity splits completely. We show that L_1 and L_2 are distinct by showing that the prime p splits differently in each. It then follows that $\mathbb{F}_q(T)(\sqrt{d})$ has 3-rank at least 2.

Lemma 1. *There exist irreducible polynomials $p, \mathfrak{p}_1, \mathfrak{p}_2 \in \mathbb{F}_q[T]$ such that $2(p^2-1)$ is not a cube modulo $\mathfrak{p}_1$ and $2p(p^2-1)$ is not a cube modulo $\mathfrak{p}_2$.*

Proof. Consider the elliptic curves given by

$$E_1: \ 2(y^2-1) = x^3, \qquad E_2: \ 2y(y^2-1) = x^3.$$

To see that E_2 is, in fact, an elliptic curve, it is enough to show that it is nonsingular, since then the genus is given by $(d-1)(d-2)/2$; since $d = 3$ here, the genus is 1. In homogeneous coordinates, E_2 is given by

$$f(x,y,z) = 2(y^3 - yz^2) - x^3.$$

The derivatives are:

$$\frac{\partial f}{\partial x} = -3x^2, \qquad \frac{\partial f}{\partial y} = 6y^2 - 2z^2, \qquad \frac{\partial f}{\partial z} = -4yz.$$

It is not hard to see that there are no nonzero values for x, y, z with the partial derivatives simultaneously zero, so E_2 is nonsingular.

We just need to show for $i = 1, 2$, that there exists $\beta_i \in \mathbb{F}_q[T]$ for which there is no $\alpha_i \in \mathbb{F}_q[T]$ with $(\alpha_i, \beta_i) \in E_i \pmod{\mathfrak{p}_i}$; choosing an irreducible polynomial $p \in \mathbb{F}_q[T]$ with $p \equiv \beta_i \pmod{\mathfrak{p}_i}$ gives the desired result. Notice that E_1 and E_2 are both constant elliptic curves since the coefficients are in $\mathbb{F}_q$ rather than $\mathbb{F}_q[T]$. Let P_i be an irreducible polynomial in $\mathbb{F}_q[T]$ of degree d_i. Then the zeta function for E_i is

$$\zeta_{\mathbb{F}}(E_i) = \frac{(1 - \pi_i q^{-s})(1 - \overline{\pi}_i q^{-s})}{(1 - q^{-s})(1 - q^{1-s})},$$

where $|\pi_i| = \sqrt{q}$ and $\overline{\pi}_i$ denotes the complex conjugate of π_i. The number of points on E_i over $\mathbb{F}_q$ is given by

$$N_i = q + 1 - \pi_i - \overline{\pi}_i = q + 1 - 2\sqrt{q}\cos(\theta_i),$$

where θ_i is defined by $\pi_i/\overline{\pi}_i = e^{i\theta_i}$. For $E_i \pmod{\mathfrak{p}_i}$, there exists π_{d_i} with $|\pi_{d_i}| = q^{d_i/2}$ and zeta function

$$\zeta_{\mathbb{F}_{q^{d_i}}}(E_i) = \frac{(1 - \pi_{d_i} q^{-d_i s})(1 - \overline{\pi}_{d_i} q^{-d_i s})}{(1 - q^{-ds})(1 - q^{d_i(1-s)})}.$$

The number of points on E_i modulo $\mathfrak{p}_i$ then is given by

$$N_{d_i} = q^{d_i} + 1 - \pi_{d_i} - \overline{\pi}_{d_i} = q^{d_i} + 1 - 2q^{d_i/2}\cos(\Theta_i),$$

where Θ_i is defined by $\pi_{d_i}/\overline{\pi}_{d_i} = e^{i\Theta_i}$. We claim that we can choose $\mathfrak{p}_i$ so that $\cos(\Theta_i)$ is sufficiently large to guarantee that $N_{d_i} < q^{d_i}$. The result follows; if for all $\alpha \in E_i \pmod{\mathfrak{p}_i}$, there exists at least one $\beta \in E_i \pmod{\mathfrak{p}_i}$ for which (α, β) is a point on the curve, then $N_{d_i} \geq q^{d_i}$, a contradiction.

Since E_i is a constant curve, we have $\pi_{d_i} = \pi_i^{d_i}$. Thus $\Theta_i = d_i\theta_i$. It remains to show that we can choose d_i so that $\cos(\Theta_i)$ is sufficiently large. If not, then θ_i/π is a rational number, say m/n for some integers m and n. Then $\theta_i = m\pi/n$, so $e^{i\theta_i}$ is a $2n$th root of unity. We claim this is impossible.

Write $\pi_{d_i} = \sqrt{q}\, e^{i\Theta_i}$. Raising both sides to the $2n$th power, we get $\pi_{d_i}^{2n} = q^n$, so $q \mid \pi_{d_i}^{2n}$. Notice that E_1 and E_2 both have complex multiplication by $\mathbb{Q}(\zeta_3)$, where ζ_3 is a complex cube root of unity. Since $q \equiv 1 \pmod 3$, it follows that E_i is supersingular modulo q, and so there is a point of order q on E_i over $\overline{\mathbb{F}}_q$, and hence a point of order q on E_i over $\mathbb{F}_{q^s}$ for some positive integer s. Then the number of points on E_i over $\mathbb{F}_{q^{2ns}}$ is

$$N_{q^{2ns}} = q^{2ns} + 1 - \pi_{d_i}^{2ns} - \overline{\pi}_{d_i}^{2ns}.$$

This implies that $q \nmid N_{q^{2ns}}$ since $q \nmid 1$, so E_i does not have a point of order q over $\mathbb{F}_{q^{2ns}}$, a contradiction since $\mathbb{E}(\mathbb{F}_{q^s}) \subset \mathbb{E}(\mathbb{F}_{q^{2ns}})$.

Thus, $e^{i\theta_i}$ is not a root of unity, so θ_i is commensurable with 2π. We can therefore choose irreducible primes $\mathfrak{p}_1, \mathfrak{p}_2$ of degrees d_1 and d_2 with $N_{d_i} < q^{d_i}$, as desired. ∎

Lemma 2. *Choose $c, w \in \mathbb{F}_q[T]$ such that*

$$w \equiv \begin{cases} 0 \pmod{p}, \\ 0 \pmod{\mathfrak{p}_1}, \\ -18c \pmod{\mathfrak{p}_2}, \end{cases}$$

$c \equiv 0 \pmod{p^2 - 1}$, $c \not\equiv 0 \pmod{\mathfrak{p}_1\mathfrak{p}_2}$, *and* $\deg(w) > \deg(c)$. *If*

$$u = \frac{8c}{p^2-1}\,(w^2 + 18cw + 108c^2), \qquad x = p^2u, \qquad y = w + 18c,$$

then the pairs u, w and x, y each satisfy the hypotheses of Theorem 2; *that is*, $\mathbb{F}_q(T)(\sqrt{4uw^3 - 27u^2})$ *and* $\mathbb{F}_q(T)(\sqrt{4xy^3 - 27x^2})$ *each admit cyclic*, *cubic*, *unramified extensions in which the prime at infinity splits completely.*

Proof. First we show that u and w are relatively prime. If any prime $\mathfrak{q}$ divides both u and w, then we must have $\mathfrak{q} \mid 864^3$, contradicting the fact that c and w are relatively prime. If a prime $\mathfrak{q}$ divides both x and y, then first notice that $\mathfrak{q} \neq p$. Otherwise, since $p \mid w$ and $p \mid y$, it would follow that $p \mid c$, again contradicting the fact that c and w are relatively prime. Now

$$\begin{aligned} x &= \frac{8p^2c}{p^2-1}\,(w^2 + 18cw + 108c^2) = \frac{8p^2cw(w+18c)}{p^2-1} + \frac{864p^2c^3}{p^2-1} \\ &\equiv \frac{864p^2c^3}{p^2-1} \pmod{y}. \end{aligned}$$

Since $\mathfrak{q} \neq p$, it follows that $\mathfrak{q} \mid c$. But then since $\mathfrak{q} \mid y$, we infer that $\mathfrak{q} \mid w$, a contradiction. Thus x and y must also be relatively prime.

Next we show that $g_1(Z) = Z^3 - uwZ - u^2$ and $g_2(Z) = Z^3 - xyZ - x^2$ are irreducible over $\mathbb{F}_q[T]$. Write $c = \overline{c}(p^2-1)$. Notice that $u \equiv 864\overline{c}^3(p^2-1)^2 \pmod{\mathfrak{p}_1}$. Then

$$g_1(Z) \equiv Z^3 - (864\overline{c}^3)^2(p^2-1)^4 = Z^3 - 2(p^2-1)[72\overline{c}^2(p^2-1)]^3 \pmod{\mathfrak{p}_1}.$$

Since $2(p^2-1)$ is not a cube modulo $\mathfrak{p}_1$, $g_1(Z)$ is irreducible modulo $\mathfrak{p}_1$, and so $g_1(Z)$ is irreducible over $\mathbb{F}_q[T]$. To see that $g_2(Z)$ is also irreducible, notice that $y = w + 18c \equiv 0 \pmod{\mathfrak{p}_2}$. We also have

$$u = \frac{8c}{p^2-1}\,(w(w+18c) + 108c^2) \equiv 864\overline{c}^3(p^2-1)^2 \pmod{\mathfrak{p}_2},$$

so $x = p^2 u \equiv 864 p^2 \overline{c}^3 (p^2-1)^2 \pmod{\mathfrak{p}_2}$. Then

$$\begin{aligned} g_2(Z) &\equiv Z^3 - xyZ - x^2 \equiv Z^3 - 864^2 p^4 \overline{c}^6 (p^2-1)^4 \\ &\equiv 2p(p^2-1)[72p\overline{c}^2(p^2-1)]^3 \pmod{\mathfrak{p}_2}. \end{aligned}$$

Since $2p(p^2-1)$ is not a cube modulo $\mathfrak{p}_2$, it follows that $g_2(Z)$ is irreducible modulo $\mathfrak{p}_2$, and therefore irreducible over $\mathbb{F}_q[T]$.

For condition (iii), we will show that $\frac{3}{2}\deg(uw) > \deg(u^2)$ and $\frac{3}{2}\deg(xy) > \deg(x^2)$. Since $\deg(w) > \deg(c)$, we see that

$$\begin{aligned} \frac{3}{2}\deg(uw) &= \frac{3}{2}(\deg(c) + 3\deg(w) - 2\deg(p)) \\ &> 2\deg(c) + 4\deg(w) - 4\deg(p) = \deg(u^2). \end{aligned}$$

Similarly,

$$\begin{aligned} \frac{3}{2}\deg(xy) &= \frac{3}{2}(2\deg(p) + \deg(u) + \deg(w)) = \frac{3}{2}(\deg(c) + 3\deg(w)) \\ &> 2\deg(c) + 4\deg(w) = 4\deg(p) + 2\deg(u) = \deg(x^2). \end{aligned}$$

Finally, we show that condition (i) is also satisfied, namely, that $4uw^3 - 27u^2$ and $4xy^3 - 27x^2$ are not squares in $\mathbb{F}_q[T]$. This follows from the other conditions. Let θ_1 and θ_2 be roots of $g_1(Z)$ and $g_2(Z)$, respectively, and let L_1 and L_2 be the normal closures of $\mathbb{F}_q(T)(\theta_1)$ and $\mathbb{F}_q(T)(\theta_2)$ respectively. It suffices to show that the Galois groups of L_1 and L_2 over $\mathbb{F}_q(T)$ are S_3 since cubic fields with square discriminants are normal. So for $i = 1, 2$ suppose, for contradiction, that the Galois group of L_i over $\mathbb{F}_q(T)$ is $\mathbb{Z}/3\mathbb{Z}$. Let $\mathfrak{q}$ be a prime in $\mathbb{F}_q[T]$ that is totally ramified in L_i. If $v_{\mathfrak{q}}(a)$ denotes the exact power of $\mathfrak{p}$ dividing a, then a function field analogue of Llorente and Nart's characterization of prime decomposition in cubic fields [13] implies that $\mathfrak{q} \mid uw$, $\mathfrak{q} \mid u^2$, and $1 \le v_{\mathfrak{q}}(b_i) \le v_{\mathfrak{q}}(a_i)$, where $g_i^*(Z) = Z^3 + a_i Z + b_i$ is obtained from $g_i(Z)$ by substituting Z/h for Z with appropriate $h \in \mathbb{F}_q[T]$ so that $v_{\mathfrak{p}}(a_i) \le 1$ or $v_{\mathfrak{p}}(b_i) \le 2$ for all primes $\mathfrak{p} \in \mathbb{F}_q[T]$. Now u and w are relatively prime, so $\mathfrak{q} \mid u$ and $\mathfrak{q} \nmid w$. This contradicts the condition that $v_{\mathfrak{q}}(b_i) \le v_{\mathfrak{q}}(a_i)$. Thus, no prime is totally ramified in L_1, contradicting the assumption that the splitting field of $g_1(Z)$ is a $\mathbb{Z}/3\mathbb{Z}$-extension of $\mathbb{F}_q(T)$. The argument for L_2 is similar. The pairs u, w and x, y must therefore each generate cubic, cyclic, unramified extensions of the quadratic fields $\mathbb{F}_q(T)(\sqrt{4uw^3 - 27u^2})$ and $\mathbb{F}_q(T)(\sqrt{4xy^3 - 27x^2})$, respectively, in which the infinite prime splits completely. ■

The following lemma is part of a function field analogue of Llorente and Nart's [13] determination of prime decomposition in cubic fields. We include the statement and proof of only the cases we require. A complete statement and proof can be found in [5].

LEMMA 3. *Let p be an irreducible polynomial in $\mathbb{F}_q[T]$, and $g(Z) = Z^3 - AZ + B \in \mathbb{F}_q(T)[Z]$. Let θ be a root of g.*

(i) *If $p \mid A$, $p \nmid B$, $\deg(p)$ even, and $(-B)^{(|p|-1)/3} \not\equiv 1 \pmod{p}$, then p is inert in $\mathbb{F}_q(T)(\theta)$.*
(ii) *If $p \nmid A$, $p \mid B$, and A is a square modulo p, then p splits completely in $\mathbb{F}_q(T)(\theta)$.*
(iii) *If $p \nmid A$, $p \mid B$, and A is not a square modulo p, then p splits into two distinct primes in $\mathbb{F}_q(T)(\theta)$, both unramified.*

Proof. (i) If $p \mid A$ and $p \nmid B$, then

$$g(Z) = Z^3 - AZ + B \equiv Z^3 + B \pmod{p}.$$

It suffices to show that $Z^3 + B$ is irreducible modulo p if $\deg(p)$ is even and $(-B)^{(|p|-1)/3} \not\equiv 1 \pmod{p}$. Since $\deg(p)$ is even and $(-B)^{(|p|-1)/3} \not\equiv 1$, it follows that $-B$ is not a cube modulo p, so the polynomial is irreducible as claimed.

(ii) If $p \nmid A$ and $p \mid B$, then

$$g(Z) = Z^3 - AZ + B \equiv Z^3 - AZ \equiv Z(Z^2 - A) \pmod{p}.$$

Since A is a square modulo p, then g factors into three distinct factors modulo p, so p splits completely in $\mathbb{F}_q(T)(\theta)$.

(iii) As in case (ii), we have

$$g(Z) = Z^3 - AZ + B \equiv Z^3 - AZ \equiv Z(Z^2 - A) \pmod{p}.$$

But since A is not a square modulo p, the two polynomials on the right are both irreducible. Thus p splits into two primes in $\mathbb{F}_q(T)(\theta)$, both unramified, one of relative degree 1 and one of relative degree 2. ∎

We are now ready to prove the main theorem.

Proof of Theorem 1. Given $c, w \in \mathbb{F}_q(T)$, set

$$u = \frac{8c}{p^2 - 1}(w^2 + 18cw + 108c^2), \qquad x = p^2 u, \qquad y = w + 18c.$$

Let θ_1 be a root of $g_1(Z) = Z^3 - uwZ - u^2$ and θ_2 a root of $g_2(Z) = Z^3 - xyZ - x^2$. Let L_1 and L_2 denote the normal closures of $\mathbb{F}_q(\theta_1)$ and $\mathbb{F}_q(\theta_2)$, respectively. By Lemma 2, the pairs u, w and x, y satisfy the hypotheses of Theorem 2, so that L_1 and L_2 are unramified, cyclic, cubic extensions of $\mathbb{F}_q(\theta_1)$ and $\mathbb{F}_q(\theta_2)$, respectively. Notice, however, that the cubic fields $\mathbb{F}_q(\theta_1)$ and $\mathbb{F}_q(\theta_2)$ have discriminants which differ by a square factor:

$$\begin{aligned}4xy^3 - 27x^2 &= 4(p^2u)(w+18c)^3 - 27(p^2u)^2 \\ &= p^2[4u(w^3 + 54c(w^2 + 18wc + 108c^2)) - 27p^2u^2] \\ &= p^2[4uw^3 + 27u^2(p^2-1) - 27p^2u^2] \\ &= p^2(4uw^3 - 27u^2).\end{aligned}$$

Thus L_1 and L_2 are both S_3-extensions of $\mathbb{F}_q(T)$ with the same quadratic subfield

$$\begin{aligned}&\mathbb{F}_q(T)(\sqrt{4uw^3 - 27u^2}) \\ &= \mathbb{F}_q(T)\left(\sqrt{\frac{8c}{p^2-1}(w^2+18cw+108c^2)(4w^3-27u)}\right) \\ &= \mathbb{F}_q(T)\left(\sqrt{\frac{8c}{p^2-1}(w^2+18cw+108c^2)\left[4w^3 - \frac{216c}{p^2-1}(w^2+18cw+108c^2)\right]}\right) \\ &= \mathbb{F}_q(T)\left(\sqrt{\frac{8c}{(p^2-1)^2}(w^2+18cw+108c^2)[4w^3(p^2-1) - 216c(w^2+18cw+108c^2)]}\right) \\ &= \mathbb{F}_q(T)(\sqrt{d}).\end{aligned}$$

Finally, we claim that L_1 and L_2 are not isomorphic. We will show that the prime $p \in \mathbb{F}_q[T]$ decomposes differently in the two fields. For L_2, notice that $v_p(x) = 2$ and $p \nmid y$. To apply Lemma 3, we first substitute Z/p for Z. The new "A" is then xy/p^2, and we have

$$\frac{xy}{p^2} = u(w+18c) \equiv \frac{864 \cdot 18c^4}{-1} = -2^6 3^5 c^4 = -3(2^3 3^2 c^2)^2 \pmod{p}.$$

Since p has even degree, -3 is a square modulo p, so by parts (ii) and (iii) of the lemma, we see that p splits completely in $K_2 = \mathbb{F}_q(T)(\theta_2)$ and therefore p splits completely in the normal closure L_2. Now for L_1, notice that $p \mid w$ and $p \nmid u$. Furthermore,

$$(u^2)^{(|p|-1)/3} \equiv \left[\left(\frac{64c^2}{-1}\right)(108c^2)^2\right]^{(|p|-1)/3} = (-2^{10}3^6c^6)^{(|p|-1)/3} \not\equiv 1 \pmod{p}.$$

By Lemma 3(i) then, p is inert in $K_1 = \mathbb{F}_q(T)(\theta_1)$, so clearly p does not split completely in L_1. Thus p splits differently in L_1 and L_2, so the two fields are not isomorphic. Thus $\mathbb{F}_q(T)(\sqrt{d})$ has two distinct cubic, cyclic, unramified extensions in which the prime at infinity splits completely, and therefore has 3-rank at least 2. ∎

We conclude this section by showing that Theorem 1 yields infinitely many real and infinitely many imaginary quadratic function fields with 3-rank at least 2. The following lemma can be found in [19].

Lemma 4. *Let d be any square-free polynomial in $\mathbb{F}_q[T]$. The prime at infinity in $\mathbb{F}_q(T)$ decomposes in the quadratic extension $\mathbb{F}_q(T)(\sqrt{d})$ as follows.*

(i) *If* $\deg(d)$ *is odd, then infinity is totally ramified.*
(ii) *If* $\deg(d)$ *is even and* $\operatorname{sgn}(d)$ *is a square in* $\mathbb{F}_q$, *then infinity splits completely.*
(iii) *If* $\deg(d)$ *is even and* $\operatorname{sgn}(d)$ *is not a square in* $\mathbb{F}_q$, *then infinity is inert.*

We say that $\mathbb{F}_q(T)(\sqrt{d})$ is real in case (ii) and imaginary otherwise. Note that since $\deg(w) > \deg(c)$, we have

$$\deg(d) = \deg(c) + 5\deg(w) + 2\deg(p).$$

If $\deg(c)$ and $\deg(w)$ have opposite parities, then $\deg(d)$ is odd, and so the prime at infinity is totally ramified in $\mathbb{F}_q(T)(\sqrt{d})$. If, however, $\deg(c)$ and $\deg(w)$ have the same parity, then $\deg(d)$ is even. We also have

$$\operatorname{sgn}(c) = 32\operatorname{sgn}(c)\operatorname{sgn}(w)^5\operatorname{sgn}(p^2),$$

so infinity splits completely in $\mathbb{F}_q(T)(\sqrt{d})$ if $2\operatorname{sgn}(c)\operatorname{sgn}(w)$ is a square in $\mathbb{F}_q$ and is inert otherwise. We can easily choose c and w whose leading terms have the desired properties; therefore Theorem 1 produces infinitely many quadratic function fields of any desired signature with 3-rank at least 2.

Acknowledgments. The author was supported, in part, by a grant from the AWM. She would also like to thank Michael Rosen for several helpful discussions.

References

[1] M. Bauer, M. Jacobson, Y. Lee, and R. Scheidler, *Construction of hyperelliptic function fields of high 3-rank*, Math. Comp. 77 (2008), 503–530.

[2] M. Craig, *A type of class group for imaginary quadratic fields*, Acta Arith. 22 (1973), 449–459.

[3] F. Diaz y Diaz, *On some families of imaginary quadratic fields*, Math. Comp. 32 (1978), 637–650.

[4] C. Erickson, N. Kaplan, N. Mendoza, A. M. Pacelli, and T. Shayler, *Parametrized families of quadratic number fields with 3-rank at least 2*, Acta Arith. 130 (2007), 141–147.

[5] C. Erickson, N. Kaplan, N. Mendoza, and T. Shayler, *Williams College SMALL REU Algebraic Number Theory report*, unpublished.

[6] C. Friesen, *Class number divisibility in real quadratic function fields*, Canad. Math. Bull. 35 (1992), 361–370.

[7] H. Hasse, *Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage*, Math. Z. 31 (1930), 565–582.

[8] Y. Kishi and K. Miyake, *Parametrization of the quadratic fields whose class numbers are divisible by three*, J. Number Theory 80 (2000), 209–217.

[9] Y. Lee, *The structure of the class groups of global function fields with any unit rank*, J. Ramanujan Math. Soc. 20 (2005), 125–145.

[10] —, *Class number divisibility of relative quadratic function fields*, Acta Arith. 121 (2006), 161–173.

[11] Y. Lee and A. Pacelli, *Subgroups of the class groups of global function fields: the inert case*, Proc. Amer. Math. Soc. 133 (2005), 2883–2889.
[12] —, —, *Higher rank subgroups in the class groups of imaginary function fields*, J. Pure Appl. Algebra 207 (2006), 51–62.
[13] P. Llorente and E. Nart, *Effective determination of the decomposition of rational primes in a cubic field*, Proc. Amer. Math. Soc. 87 (1983), 579–585.
[14] P. Llorente and J. Quer, *On the 3-Sylow subgroup of the class group of quadratic fields*, Math. Comp. 50 (1988), 321–333.
[15] T. Nagell, *Über die Klassenzahl imaginär-quadratischer Zahlkörper*, Abh. Math. Sem. Univ. Hamburg 1 (1922), 140–150.
[16] A. Pacelli, *Abelian subgroups of any order in class groups of global function fields*, J. Number Theory 106 (2004), 29–49.
[17] —, *The prime at infinity and the rank of the class group of a global function field*, ibid. 116 (2006), 311–323.
[18] J. Quer, *Corps quadratiques de 3-rang 6 et courbes elliptiques de rang 12*, C. R. Acad. Sci. Paris Sér. I Math. 305 (1987), 215–218.
[19] M. Rosen, *Number Theory in Function Fields*, Springer, New York, 2002.
[20] —, *The Hilbert class field in function fields*, Expo. Math. 5 (1987), 365–378.
[21] P. Weinberger, *Real quadratic fields with class numbers divisible by n*, J. Number Theory 5 (1973), 237–241.
[22] Y. Yamamoto, *On unramified Galois extensions of quadratic number fields*, Osaka J. Math. 7 (1970), 57–76.

Department of Mathematics
Williams College
Williamstown, MA 01267, U.S.A.
E-mail: Allison.Pacelli@williams.edu

Received on 5.11.2007
and in revised form on 30.3.2009 (5565)