

CONSTRUCTION OF HYPERELLIPTIC FUNCTION FIELDS OF HIGH THREE-RANK

M. BAUER, M. J. JACOBSON, JR., Y. LEE, AND R. SCHEIDLER

ABSTRACT. We present several explicit constructions of hyperelliptic function fields whose Jacobian or ideal class group has large 3-rank. Our focus is on finding examples for which the genus and the base field are as small as possible. Most of our methods are adapted from analogous techniques used for generating quadratic number fields whose ideal class groups have high 3-rank, but one method, applicable to finding large l -ranks for odd primes $l \geq 3$, is new and unique to function fields. Algorithms, examples, and numerical data are included.

1. INTRODUCTION AND MOTIVATION

The Cohen-Lenstra heuristics [6] imply that the ideal class group of an imaginary quadratic number field is expected to have low l -rank for any odd prime l , and there is strong numerical evidence to support this claim. As a result, beginning in the 1970's, a considerable body of literature has been devoted to the construction of families of “atypical” imaginary quadratic fields of unusually large 3-rank and the development of algorithms for finding such fields [30], [34], [33], [7], [8], [10], [31], [11], [27], [20], [22], [21], [4]; some of this work will be discussed in more detail in this paper. For completeness, we mention that the record is held by Llorente and Quer [27, 21] who found three imaginary quadratic fields of 3-rank 6.

Friedman and Washington [13] proposed a function field analogue of the Cohen-Lenstra heuristics, conjecturing that the l -rank of the Jacobian of a hyperelliptic curve over a finite field is small with high probability, despite the fact that it can be as large as twice the genus of the curve. This result was recently formalized and proved by Achter [1]. Lee and Pacelli [25, 19] provided explicit constructions of infinite families of degree m function field extensions $\mathbb{K}/\mathbb{F}_q(x)$ whose ideal class group has d -rank $m - 1$ when d , m and q are pairwise coprime; the simplest case yields an infinitude of hyperelliptic function fields of odd characteristic and positive d -rank. It is well-known that the Jacobian and the ideal class group of an imaginary hyperelliptic function field are very closely linked; they are essentially isomorphic (possibly up to a factor of $\mathbb{Z}/2\mathbb{Z}$), so their respective d -ranks are equal when d is odd. Therefore, we can use the ideal class group to describe our methods without loss of generality.

2000 *Mathematics Subject Classification*. Primary 11R11. Secondary 11R65, 11Y16, 11Y40, 14H05, 14H40.

Key words and phrases. Hyperelliptic function field, ideal class group, Jacobian, 3-rank.

The first, second, and fourth authors were supported by NSERC of Canada.

The third author was supported by an AWM-NSF Mentoring Grant.

In this article, we present methods to construct and explicitly compute hyperelliptic function fields of large 3-rank. As opposed to methods such as [25, 19] in which families of curves with certain rank properties are constructed, our focus is on *small* examples, namely hyperelliptic function fields where both the base field and the genus are as small as possible. We generalized methods of Craig [7], Shanks [30], Shanks and Weinberger [34], and Diaz y Diaz [10] for finding quadratic number fields with high 3-rank. The method of Diaz y Diaz, essentially a brute-force search for field discriminants satisfying conditions that guarantee 3-rank at least 3, turned out to be the most useful, yielding function fields with 3-rank as high as 7. This method fixes the base field \mathbb{F}_q (we used $q = 5, 7, 11, 13, 17$ for our examples) and produces examples of varying but reasonably small genus — our examples all had genus at most 10. We also present a new method unique to function fields, in which the underlying hyperelliptic curve is fixed and the 3-rank is increased by enlarging the base field. If the curve is defined over a sufficiently small base field, then the examples obtained by this method will still be of reasonable size. Unlike the methods generalized from quadratic number fields, this method is applicable to finding examples with large l -rank for any odd prime l not dividing q . Both of our methods are primarily useful for small values of q , as their run-time complexities are proportional to a power of q due to enumerating all polynomials over \mathbb{F}_q up to a certain degree for the Diaz y Diaz method and computing the L -polynomial of the hyperelliptic function field for the second method.

While the problem of finding quadratic number fields and function fields of large d -rank is interesting in its own right, there are further reasons for investigating this topic, particularly the case $d = 3$. For a fundamental discriminant $D \in \mathbb{Z}$, $D < 0$, the associated *dual* discriminant is $\overline{D} = -3D/\gcd(D, 3)^2$, i.e. $\overline{D} = -D/3$ if 3 divides D and $-3D$ otherwise. Scholz's Theorem [29] states that the 3-rank of an imaginary quadratic number field is either equal to the 3-rank of the associated dual real quadratic field (the *non-escalatory* case) or exceeds it by 1 (the *escalatory* case), and Scholz gave criteria to distinguish between the two scenarios. In fact, some of the work cited above investigates whether the fields under discussion are escalatory or non-escalatory; the three fields of Llorente and Quer [27, 21] mentioned earlier are in fact escalatory, giving rise to three real quadratic fields of the impressive 3-rank 5. Recently, the third author has extended Scholz's theorem to function fields [17, 18], proving that if q is an odd prime power and l an odd prime with $q \equiv -1 \pmod{l}$, then the l -rank of the real quadratic function field $\mathbb{F}_q(x, \sqrt{D(x)})$ (with $D(x) \in \mathbb{F}_q[x]$ monic, square-free, and of even degree) is either equal to the l -rank of the imaginary hyperelliptic function field $\mathbb{F}_q(x, \sqrt{uD(x)})$ (with u any non-square in \mathbb{F}_q) or is 1 less; if the latter (escalatory) case occurs, then l must divide the regulator of the real quadratic field.

It is also well-known that there is a remarkable connection between quadratic and cubic fields. More specifically, for any fundamental discriminant, there is a bijection between the quadratic field of that discriminant and any triple of conjugate cubic fields of the same discriminant. Furthermore, Hasse's Theorem [14] states that for a given quadratic number field of fixed discriminant whose ideal class group has 3-rank r , there are $(3^r - 1)/2$ non-isomorphic cubic fields of the same discriminant. The third author has proved a function field analogue of Hasse's result as well. In an unpublished manuscript [32] (see also Chapter 4 of [12]), Shanks proposed a technique which he called CUFFQI (short for "*Cubic Fields From*

Quadratic Infrastructure” and pronounced “cuff-key”) that, given an imaginary quadratic number field of 3-rank r , explicitly generates the associated $(3^r - 1)/2$ complex cubic fields of the same discriminant by making use of the infrastructure of the set of reduced principal ideals in the associated dual real quadratic field. Research on a function field version of CUFFQI is currently in progress. Although the constructions and examples presented here are interesting in their own right, it was the endeavour of rediscovering CUFFQI and adapting it to hyperelliptic function fields that motivated and eventually produced this paper, as high 3-rank hyperelliptic function fields are ideal candidates for testing CUFFQI.

2. PRELIMINARIES

Throughout Sections 2-4 of this paper, let \mathbb{F}_q be a finite field of order q where q is a power of an odd prime; in Section 5, we will allow q to be even or odd. For any non-zero polynomial F in the polynomial ring $\mathbb{F}_q[x]$, we denote by $\deg(F)$ the degree of F and by $\text{sgn}(F)$ the leading coefficient of F . We also write $|F| = q^{\deg(F)}$. If $E, F \in \mathbb{F}_q[x]$ with E non-constant and F non-zero, write $E \mid F$ if E divides F , and define $v_E(F) = e$ if $E^e \mid F$ and $E^{e+1} \nmid F$.

2.1. Overview of hyperelliptic function fields. A *hyperelliptic* function field over \mathbb{F}_q is a quadratic extension $\mathbb{K} = \mathbb{F}_q(x, y)$ of $\mathbb{F}_q(x)$ where $x \in \mathbb{K}$ is transcendental over \mathbb{F}_q . The function field \mathbb{K} is defined by a *hyperelliptic curve* over \mathbb{F}_q which (for odd q) has the form $y^2 = D(x)$ with $D(x) \in \mathbb{F}_q[x]$ a square-free polynomial of degree at least 3, so \mathbb{K} can be written as $\mathbb{K} = \mathbb{F}_q(x, \sqrt{D(x)})$. The *genus* of \mathbb{K} is $g = \lfloor (\deg(D) - 1)/2 \rfloor$. It is well-known (see for example Proposition 14.6, p. 248, of [28]) that the place at infinity of $\mathbb{F}_q(x)$ defined by the negative degree valuation is ramified in \mathbb{K} if D has odd degree, inert in \mathbb{K} if D has even degree and non-square leading coefficient, and split in \mathbb{K} if D has even degree and square leading coefficient. In the first two cases, $\mathbb{K}/\mathbb{F}_q(x)$ is an *imaginary* quadratic extension, whilst in the latter scenario, $\mathbb{K}/\mathbb{F}_q(x)$ is *real*.

The *maximal order* (or *coordinate ring*) of $\mathbb{K}/\mathbb{F}_q(x)$ is the integral closure of the polynomial ring $\mathbb{F}_q[x]$ in \mathbb{K} and is denoted by \mathcal{O} . For any element $\alpha = a + b\sqrt{D} \in \mathbb{K}$ we denote by $\bar{\alpha} = a - b\sqrt{D}$ its *conjugate* and by $N(\alpha) = \alpha\bar{\alpha}$ its *norm*. Similarly, for any ideal \mathfrak{a} in \mathcal{O} , we let $\bar{\mathfrak{a}} = \{\bar{\alpha} \mid \alpha \in \mathfrak{a}\}$ be its *conjugate ideal*. Note that $\mathfrak{a}\bar{\mathfrak{a}} = (N(\mathfrak{a}))$ is the principal ideal generated by a monic polynomial $N(\mathfrak{a})$ that is the *norm* of \mathfrak{a} . The ideal \mathfrak{a} is *reduced* if \mathfrak{a} is *primitive*, i.e. \mathfrak{a} has no polynomial factors, and $\deg(N(\mathfrak{a})) \leq g$. If \mathfrak{a} is primitive, then $N(\mathfrak{a})$ is the unique monic polynomial in \mathfrak{a} of minimal degree.

Let \mathcal{C} denote the ideal class group of $\mathbb{K}/\mathbb{F}_q(x)$; that is, the group of fractional \mathcal{O} -ideals modulo principal fractional \mathcal{O} -ideals. If $\mathbb{K}/\mathbb{F}_q(x)$ is imaginary, then every ideal class of \mathbb{K} has at most one reduced representative (see pp. 178-183 of [2]), whereas in a real quadratic extension, there can be many (in fact exponentially many) reduced representatives in any given ideal class of \mathbb{K} .

Suppose that $\mathbb{K}/\mathbb{F}_q(x)$ is imaginary. Then there is only one place at infinity, denoted by ∞ , in \mathbb{K} of degree $f = 1$ or $f = 2$, and the group of units of \mathcal{O} consists of only the trivial units \mathbb{F}_q^* , i.e. the non-zero elements of \mathbb{F}_q . Then according to Proposition 14.1, p. 243, of [28], there is a short exact sequence

$$(2.1) \quad (0) \rightarrow \text{Jac}(\mathbb{F}_q) \rightarrow \mathcal{C} \rightarrow \mathbb{Z}/f\mathbb{Z} \rightarrow (0)$$

where $Jac(\mathbb{F}_q)$ denotes the Jacobian of \mathbb{K}/\mathbb{F}_q . We thus see that \mathcal{C} modulo an isomorphic copy of $Jac(\mathbb{F}_q)$ is isomorphic to $\mathbb{Z}/f\mathbb{Z}$, so we have that \mathcal{C} is isomorphic to $Jac(\mathbb{F}_q)$ if ∞ is ramified and the factor group is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ if ∞ is inert; in particular, for any $d \in \mathbb{N}$ odd, \mathcal{C} and $Jac(\mathbb{F}_q)$ have the same d -rank. In short, we say that \mathbb{K} has d -rank r if $Jac(\mathbb{F}_q)$ (or \mathcal{C}) has d -rank r .

2.2. d -Torsion Ideal Classes. Let $D \in \mathbb{F}_q[x]$ be any square-free polynomial of degree at least 3. For fixed $d \in \mathbb{N}$, consider the equation¹

$$(2.2) \quad 4A^d = B^2 - C^2D$$

in the unknowns $A, B, C \in \mathbb{F}_q[x] \setminus \{0\}$. Our key observation is the correspondence between solutions of (2.2) (with d odd) and elements in the ideal class group \mathcal{C} of the hyperelliptic function field $\mathbb{K} = \mathbb{F}_q(x, \sqrt{D})$ whose order is a divisor of d . More exactly, any d -torsion class yields a non-zero solution of (2.2) (Lemma 2.1 below), and more importantly, the converse also holds under a certain divisibility condition (Theorem 2.2 below).

Lemma 2.1. *Suppose that $d \in \mathbb{N}$ is odd. Then any non-zero ideal in the maximal order \mathcal{O} of the hyperelliptic function field $\mathbb{K} = \mathbb{F}_q(x, \sqrt{D})$ whose d -th power is principal yields a non-zero solution (A, B, C) of (2.2). More exactly, if \mathfrak{a} is a non-zero ideal in \mathcal{O} of norm $U \in \mathbb{F}_q[x]$, and $\mathfrak{a}^d = (\lambda)$ where $\lambda = V + W\sqrt{D} \in \mathcal{O}$, then there exists $u \in \mathbb{F}_q^*$ such that $(A, B, C) = (uU, 2u^{(d-1)/2}V, 2u^{(d-1)/2}W)$ is a non-zero solution of (2.2).*

Proof. Since $U = N(\mathfrak{a})$, we have $(U^d) = (\lambda\bar{\lambda}) = (V^2 - W^2D)$, so there exists $u \in \mathcal{O}^*$ such that

$$(2.3) \quad uU^d = V^2 - W^2D.$$

Conjugating (2.3) reveals that $u = \bar{u}$, so $u \in \mathbb{F}_q^*$. Multiplying (2.3) by $4u^{d-1}$, we obtain $4(uU)^d = (2u^{(d-1)/2}V)^2 - (2u^{(d-1)/2}W)^2D$ as claimed, and $uU \neq 0$, so this is a non-zero solution. \square

Theorem 2.2. *Suppose that $d \geq 3$ is odd and let (A, B, C) be a solution of (2.2) with $ABC \neq 0$. If $G = \gcd(A, B)$ divides D , then this solution yields a non-zero ideal in the maximal order \mathcal{O} of the hyperelliptic function field $\mathbb{K} = \mathbb{F}_q(x, \sqrt{D})$ whose d -th power is principal. More exactly, if $\mathfrak{a} = (A, \lambda/H)$ is the ideal in \mathcal{O} generated by A and λ/H , where $\lambda = (B + C\sqrt{D})/2$ and $H = G^{(d-1)/2}$, then \mathfrak{a} is a primitive integral ideal of norm $\text{sgn}(A)^{-1}A$ with $\mathfrak{a}^d = (\lambda)$.*

Proof. Set $J = \gcd(B, C)$. We first show that $H \mid J$, or equivalently, $\lambda/H \in \mathcal{O}$, so that \mathfrak{a} is indeed an integral ideal in \mathcal{O} . This is clear for $G = 1$, so assume that $G \neq 1$ and set $e = v_G(J) \geq 0$. Suppose $e < (d-1)/2$. Then $G^{2e+2} \mid G^d \mid A^d$ and $G^{2e+1} \mid J^2G \mid C^2D$, so $G^{2e+1} \mid B^2 = 4A^d + C^2D$. Since $v_G(B^2)$ is even, we must have $G^{2e+2} \mid B^2$, so $G^{2e+2} \mid C^2D = B^2 - 4A^d$. Now D square-free implies $v_G(D) = 1$, so $G^{2e+1} \mid C^2$. Again since $v_G(C^2)$ is even, we have $G^{2e+2} \mid C^2$. But then $G^{e+1} \mid B$ and $G^{e+1} \mid C$, so $G^{e+1} \mid J$, contradicting the definition of e . It follows that $e \geq (d-1)/2$, so $H \mid G^e \mid J$.

¹In the function field setting, one can easily eliminate the factor 4 on the left-hand side of (2.2). However, we chose to keep it to make the connection to the number field methods more readily visible, particularly for the Diaz y Diaz technique [10] discussed in Section 3. From a practical and computational viewpoint, the factor 4 makes no difference in any of our algorithms.

We claim that G is coprime to any power of A/G . To that end, since G is squarefree, it suffices to show that G is coprime to A/G . Assume to the contrary that there is an irreducible polynomial P dividing $\gcd(G, A/G)$. Then $P^2 \mid A$, so $v_P(A) > 1$. Since $G = \gcd(A, B)$ is square-free, we must have $v_P(B) = 1$. On the other hand, $P^3 \mid P^d \mid G^d \mid 4A^d + C^2D = B^2$, a contradiction.

Next, we prove that $N(\mathfrak{a}) = \text{sgn}(A)^{-1}A$. We have $(N(\mathfrak{a})) = \mathfrak{a}\bar{\mathfrak{a}} = (A^2, A\lambda/H, A\bar{\lambda}/H, A^d/H^2) = (A)\mathfrak{b}$ with $\mathfrak{b} = (A, \lambda/H, \bar{\lambda}/H, (A/G)^{d-1})$, so it suffices to show that $\mathfrak{b} = \mathcal{O}$. Note that $H(\lambda/H + \bar{\lambda}/H) = B \in \mathfrak{b}$, so $G = \gcd(A, B) \in \mathfrak{b}$. It follows that $1 = \gcd(G, (A/G)^{d-1}) \in \mathfrak{b}$, implying $\mathfrak{b} = \mathcal{O}$.

To establish that \mathfrak{a} is primitive, assume that $(S) \mid \mathfrak{a}$ for some non-zero $S \in \mathbb{F}_q[x]$. Then $S \mid (\lambda/H)$ and $S \mid (\bar{\lambda}/H)$, so $S \mid (B/H)$. Furthermore, $S^2 \mid \mathfrak{a}\bar{\mathfrak{a}} = (A)$, so $S \mid G$, and therefore $S^{(d-1)/2} \mid H$. Then $S^2 \mid S^{(d+1)/2} \mid SH \mid B$ and $S^2 \mid A$ yield $S^2 \mid G$, so $S \in \mathbb{F}_q^*$.

Finally, to see that λ is a generator of \mathfrak{a}^d , we show that $(\lambda) \mid \mathfrak{a}^d$; since both ideals have identical norm, namely $(\text{sgn}(A)^{-1}A)^d$, they must be equal. The ideal \mathfrak{a}^d is generated by elements of the form $\alpha_i = A^{d-i}(\lambda/H)^i$ with $0 \leq i \leq d$, so it suffices to show that each α_i is an \mathcal{O} -multiple of λ . For $i = 0$, this holds since $A^d = \lambda\bar{\lambda}$, so we need to show that $H^i \mid A^{d-i}\lambda^{i-1}$ in \mathcal{O} for $1 \leq i \leq d$. Since $G^{(d+1)/2} \mid B$, $G^{(d-1)/2} \mid C$, and $G \mid D$, we see that $G^d \mid \lambda^2$. Then $G^{d-i} \mid A^{d-i} \mid A^{2(d-i)}$ and $G^{d(i-1)} \mid \lambda^{2(i-1)}$ yield $G^{(d-1)i} = G^{(d-i)+d(i-1)} \mid A^{2(d-i)}\lambda^{2(i-1)}$. Taking square roots produces the desired result, i.e. $H^i \mid A^{d-i}\lambda^{i-1}$. \square

The ideal $\mathfrak{a} = (A, \lambda/H)$ of Theorem 2.2 is called the ideal *corresponding* to the solution (A, B, C) of (2.2) (or to the pair (A, B)).

As a point of interest, we note that if q is even, then a hyperelliptic function field has the form $\mathbb{K} = \mathbb{F}_q(x, y)$ where $y^2 + Ey = D$ with $E, D \in \mathbb{F}_q[x]$ (there are certain conditions on the degrees and leading coefficients of D and E that we need not state in detail). Here, the analogue of equation (2.2) (with the factor of 4 removed) is

$$(2.4) \quad A^d = B^2 + C^2D + BCE .$$

Lemma 2.1 is still true with (2.4) in place of (2.2). An analogue of Theorem 2.2 holds for example under the assumptions $G = \gcd(A, B) \mid \gcd(D, E)$ and E coprime to A/G , but it is unclear if or how these conditions can be relaxed, or how to find solutions of (2.4). This is a subject for future research.

2.3. A strategy for obtaining high prime rank. We note that it is sufficient to consider only solutions of (2.2) with d prime. To see this, suppose $d = ps$ with p prime and $s \in \mathbb{N}$, and that we have a triple (A, B, C) with $4A^p = B^2 - C^2D$. Then $4A^d = 4(A^p)^s = B_s^2 - C_s^2D$ where B_s and C_s are defined via $(B \pm C\sqrt{D})^s = 2^{s-1}(B_s \pm C_s\sqrt{D})$. The polynomials B_s and C_s can easily be evaluated recursively using the arithmetic of Lucas functions.

Let $d = l$ be an odd prime (the case $d = 2$ was discussed in [40]). Suppose $D \in \mathbb{F}_q[x]$ is a square-free polynomial of odd degree at least 3 or even degree at least 4 and non-square leading coefficient, so $\mathbb{K} = \mathbb{F}_q(x, \sqrt{D})$ is an imaginary hyperelliptic function field.² Then it is well-known that every ideal class of \mathbb{K} has at most one unique reduced representative, and exactly one such representative

²In light of Scholz' Theorem, the condition on \mathbb{K} being imaginary is essentially no restriction, at least in the case where $q \equiv -1 \pmod{l}$.

if $\deg(D)$ is odd.³ The reduced ideal in the principal class is \mathcal{O} ; it is the only reduced ideal of constant norm (i.e. norm 1). If (A, B, C) is a solution of (2.2) satisfying Theorem 2.2 with $0 < \deg(A) \leq g = \lfloor (\deg(D) - 1)/2 \rfloor$, then it is clear from Theorem 2.2 that the ideal \mathfrak{a} in \mathbb{K} corresponding to this solution is the unique reduced representative of an ideal class of order l .

This leads to the following strategy for finding imaginary hyperelliptic function fields of high l -rank. Fix an odd prime power q and $A_1 = A \in \mathbb{F}_q[x]$. Find all non-zero $B_1 = B$ such that the square-free part D_B of $B^2 - 4A^l$ has odd degree ≥ 3 or even degree ≥ 4 and non-square leading coefficient, $\gcd(A, B)$ divides D_B , and $0 < \deg(A) \leq g_B = \lfloor (\deg(D_B) - 1)/2 \rfloor$. If no such B exists, try a different A . Note that the conditions on D_B force $|B|^2 \leq |A|^l$, so the search space for B is finite. Each pair (A, B) yields an ideal class of order l in the imaginary hyperelliptic function field $\mathbb{K}_B = \mathbb{F}_q(x, \sqrt{D_B})$, so each \mathbb{K}_B has l -rank at least 1.

For each B found above, search for further solutions of (2.2) (with $d = l$ and $D = D_B$), i.e. search for pairs (A_i, B_i) ($i = 2, 3, \dots$) such that $B_i \neq 0$, the square-free part of $B_i^2 - 4A_i^l$ equals D_B , $\gcd(A_i, B_i) \mid D_B$, $0 < \deg(A_i) \leq g_B$, and no two among the A_i ($i = 1, 2, \dots$) differ by a constant factor. Then the corresponding ideals $\mathfrak{a}_1, \mathfrak{a}_2, \dots$ are all distinct (since their norms are distinct) and reduced, so they generate different ideal classes of \mathbb{K}_B of order l . Now if the method for producing the pairs (A_i, B_i) from (A, B) can guarantee at least t among the ideal classes $[\mathfrak{a}_1], [\mathfrak{a}_2], \dots$ and their conjugates to be independent (for suitable $t \in \mathbb{N}$), then each field K_B has l -rank at least t .

In the next section, we present a method that utilizes this strategy for $l = 3$; initially, $t = 2$, but a subsequent refinement of the search technique yields $t = 3$.

3. DIAZ Y DIAZ'S CONSTRUCTION

In 1978, Diaz y Diaz [10] devised a search technique using the strategy described above for generating quadratic number fields of 3-rank at least 2, and if certain conditions are met, the 3-rank is at least 3. Since his approach has a high numerical yield even for parameters of modest size and can be applied to hyperelliptic function fields without too many changes with the same lower bounds on the 3-rank, we describe our function field adaption of this technique in some detail.

3.1. The idea for 3-rank at least 2. The method is based on the following idea. Suppose we have three solutions (A_i, B_i, C) ($i = 1, 2, 3$) with $A_i, B_i, C \in \mathbb{F}_q[x]$ and $A_i B_i C \neq 0$ of

$$(3.1) \quad 4A^3 = B^2 - C^2D$$

for fixed D , with pairwise distinct A_i ; note that the C values of these three triples are identical. Then

$$(3.2) \quad 4(A_i - A_1)(A_i^2 + A_i A_1 + A_1^2) = (B_i - B_1)(B_i + B_1)$$

for $i = 2, 3$. Suppose also that the linear factor on the left-hand side of (3.2) divides the first linear factor on the right-hand side, and that furthermore, the ratios are the same for $i = 2, 3$, i.e. $(B_2 - B_1)/(A_2 - A_1) = (B_3 - B_1)/(A_3 - A_1)$. Call this

³If $\deg(D)$ is even and $\text{sgn}(D)$ is a non-square in \mathbb{F}_q , then there can be ideal classes \mathbf{C} such that every integral ideal in \mathbf{C} has a norm whose degree exceeds g . Each such class contains exactly $q + 1$ pairwise equivalent primitive ideals whose norm has degree $g + 1$; see p. 183 of [2].

ratio $2V \in \mathbb{F}_q[x]$. If we set $T_i = A_i - A_1$, then $B_i - B_1 = 2T_iV$. Substituting this into (3.2) yields

$$(3.3) \quad 3A_1^2 + 3A_1T_i + T_i^2 = V(B_1 + T_iV)$$

for $i = 2, 3$. If we subtract (3.3) for $i = 3$ from (3.3) for $i = 2$ and divide by $T_3 - T_2$, we obtain $T_3 = V^2 - T_2 - 3A_1$, or equivalently (in a more symmetric form) $A_1 + A_2 + A_3 = V^2$. So we see that the pairs (A_1, B_1) and (A_2, B_2) uniquely determine the third pair (A_3, B_3) . Note that if we set $A = A_1$, $B = B_1$, $T = T_2$, and $U = B + TV$, then (3.3) for $i = 2$ can be rewritten as

$$(3.4) \quad 3A^2 + 3AT + T^2 = UV, \quad B = U - TV,$$

so we have the following lemma:

Lemma 3.1. *Let (A, B, C) be a solution of (3.1) with ABC non-zero. If A and B satisfy (3.4) for some polynomials $T, U, V \in \mathbb{F}_q[x]$, then (3.1) has three solutions (A_1, B_1, C) , (A_2, B_2, C) , (A_3, B_3, C) where $A_1 = A$, $B_1 = B$, $A_2 = A + T$, $B_2 = B + 2TV$, $A_3 = A + \tilde{T}$, $B_3 = B + 2\tilde{T}V$ with $\tilde{T} = V^2 - 3A - T$.*

Under the right conditions, the three solutions of Lemma 3.1 generate an imaginary hyperelliptic function field of 3-rank at least 2:

Lemma 3.2. *Assume that $\mathbb{K} = \mathbb{F}_q(x, \sqrt{D})$ is imaginary of genus g , and let A_i, B_i ($i = 1, 2, 3$) be as in Lemma 3.1 such that no two among the A_i ($i = 1, 2, 3$) differ by a constant factor. Suppose that $B_i \neq 0$, $\gcd(A_i, B_i)$ divides D , and $0 < \deg(A_i) \leq g$ for $i = 1, 2, 3$. Then \mathbb{K} has 3-rank at least 2.*

Proof. From our discussion in Section 2.3, we see that the three ideals \mathfrak{a}_i corresponding to the solutions (A_i, B_i, C) ($i = 1, 2, 3$) of (3.1) generate three distinct ideal classes of \mathbb{K} of order 3. The field \mathbb{K} cannot have 3-rank 1 since $\mathbb{Z}/3\mathbb{Z}$ contains only two distinct elements of order 3. So \mathbb{K} has 3-rank at least 2. \square

Lemma 5 of [10] shows that the product $\mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3$ is principal, so we cannot guarantee a 3-rank exceeding 2.

3.2. The search space. The above idea can be converted into a search strategy as follows. As described above, fix an odd prime power q and a non-constant polynomial $A \in \mathbb{F}_q[x]$. In light of (3.4), we search for non-zero polynomials $V \in \mathbb{F}_q[x]$ such that $3A^2 + 3AT + T^2 \equiv 0 \pmod{V}$ has a solution $T \in \mathbb{F}_q[x]$. Note that if $q \equiv 1 \pmod{3}$ and $u \in \mathbb{F}_q^*$ with $u^2 = -3$, then the equation $3A^2 + 3AT + T^2 = 0$ has solutions $T_{\pm} = A(\pm u - 3)/2 \in \mathbb{F}_q[x]$, so we can choose any suitable V and set $T \equiv T_+$ or $T_- \pmod{V}$.

Each pair (T, V) defines polynomials U and B as given in (3.4). Then Lemma 3.1 yields three solutions (A_i, B_i, C) ($i = 1, 2, 3$) of (3.1) for some square-free polynomial $D \in \mathbb{F}_q[x]$. We only consider those V, T, U, B which satisfy the following conditions:

Conditions (C)

- $|T| < |V|$;
- D has odd degree ≥ 3 or even degree ≥ 4 and non-square leading coefficient;
- no two among the A_i ($i = 1, 2, 3$) differ by a constant factor;
- $B_i \neq 0$ and $\gcd(A_i, B_i)$ divides D for $i = 1, 2, 3$;
- $0 < \deg(A_i) \leq g = \lfloor (\deg(D) - 1)/2 \rfloor$ for $i = 1, 2, 3$.

By Lemma 3.2, each pair (V, T) satisfying these conditions yields a hyperelliptic function field of 3-rank at least 2.

Given a value of A , the first step is to search for values of V for which the congruence $3A^3 + 3AT + T^2 \equiv 0 \pmod{V}$ arising from the first identity in (3.4) has a solution T . We can bound V in terms of A :

Lemma 3.3. *Under conditions (C), we have $\deg(V) \leq (3 \deg(A) - 1)/4$. Furthermore, if $3 \nmid q$, then $\deg(V) \geq \deg(A)/2$, and if $3 \mid q$, then $\deg(V) \geq 2$.*

Proof. Since $V^2 = A_1 + A_2 + A_3$, we have $\deg(V) \leq g/2$. Using the triangle inequality, the conditions on D yield $|A|^3 = |B^2 - C^2D| = \max\{|B|^2, |C^2D|\}$, so $|D| \leq |C^2D| \leq |A|^3$. Since $\deg(D) \geq 2g + 1$, we have $2 \deg(V) \leq g \leq (3 \deg(A) - 1)/2$, yielding the upper bound on $\deg(V)$.

Assume that $3 \nmid q$, and suppose by way of contradiction that $|V| < |A|^{1/2}$. Then $|T| < |V| < |A|^{1/2}$, so $|3A^2 + 3AT + T^2| = |A|^2$. Now $|B| \leq |A|^{3/2}$, so by (3.4) and the triangle inequality,

$$\begin{aligned} |A|^2 &= |3A^2 + 3AT + T^2| = |(B + TV)V| \\ &\leq \max\{|BV|, |TV^2|\} < \max\{|A|^2, |A|^{3/2}\} = |A|^2, \end{aligned}$$

a contradiction. Finally, suppose that $3 \mid q$. By (3.4), we have $T^2 = UV$. Since $A_1 \neq A_2$, we have $T \neq 0$, and hence $U \neq 0$, so $0 < |T| < |V| \leq |UV| = |T|^2$. It follows that $|T| > 1$ and hence $\deg(V) \geq \deg(T) + 1 \geq 2$. \square

The search for V can be further narrowed if $q \equiv -1 \pmod{3}$, so the method is particularly suited (though not limited) to this case. The following lemma and corollary give criteria that suitable values of V must satisfy in this case.

Lemma 3.4. *Suppose $q \equiv -1 \pmod{3}$. Under conditions (C), V is the norm in $\mathbb{F}_q(u)(x)/\mathbb{F}_q(x)$ of a polynomial in $\mathbb{F}_q(u)[x]$ where $u^2 = -3$.*

Proof. Irreducible polynomials in $\mathbb{F}_q[x]$ split two-fold in $\mathbb{F}_q(u)[x]$ if they have even degree and are irreducible in $\mathbb{F}_q(u)[x]$ if they have odd degree. So the statement of the lemma is clear if all irreducible divisors of V in $\mathbb{F}_q[x]$ have even degree, or have odd degree and appear in V as an even power.

Suppose there exists an irreducible divisor $P \in \mathbb{F}_q[x]$ of V of odd degree such that $v_P(V)$ is odd. For any $F \in \mathbb{F}_q(u)[x]$, denote by \bar{F} the image of F under the map $u \rightarrow -u$. Then $UV = 3A^2 + 3AT + T^2 = F\bar{F}$ where $F = (3A + 2T + uA)/2 \in \mathbb{F}_q(u)[x]$. Since P has odd degree, it is irreducible in $\mathbb{F}_q(u)[x]$, so it must divide F or \bar{F} in $\mathbb{F}_q(u)[x]$. But $P \mid F$ if and only if $\bar{P} = P \mid \bar{F}$, and in fact $v_P(F) = v_P(\bar{F})$ in $\mathbb{F}_q(u)[x]$. It follows that $v_P(UV)$ is even and at least 2. Therefore $v_P(U)$ is odd, so P divides U and hence $B = U - TV$. Furthermore, P divides $u^{-1}(F - \bar{F}) = A$, so $P \mid G$. Since $P^2 \mid F\bar{F} = 3A^2 + 3AT + T^2$, P must divide T . Also, $G^3 \mid A^3 + C^2D = B^2$, so $v_P(B) \geq 2$. Then $P^2 \mid B - TV = U$. Since $v_P(U)$ is odd, P^3 must divide U , so $P^4 \mid UV$. But then $P^2 \mid F$ and $P^2 \mid \bar{F}$, implying $P^2 \mid A$ and hence $P^2 \mid \gcd(A, B) = G$, contradicting the fact that G is square-free. \square

Corollary 3.5. *Suppose $q \equiv -1 \pmod{3}$. Under conditions (C), V is of the form $V = O^2E$ where*

1. O is the product of odd degree irreducible polynomials in $\mathbb{F}_q[x]$;
2. E is the product of even degree irreducible polynomials in $\mathbb{F}_q[x]$;
3. O divides A .

Proof. Parts 1 and 2 are clear from the proof of Lemma 3.4. Let $P \in \mathbb{F}_q[x]$ be irreducible with $v_P(O) = m \in \mathbb{N}$. Since $P^{2m} \mid O^2 \mid V \mid UV = F\bar{F}$ where F and \bar{F} are as in the proof of Lemma 3.4, we must have $P^m \mid F, \bar{F}$ in $\mathbb{F}_q(u)[x]$, so $P^m \mid u^{-1}(F - \bar{F}) = A$. \square

3.3. The algorithm for 3-rank at least 2. For each A , our algorithm generates a considerable number of hyperelliptic function fields of 3-rank at least 2. More exactly, for each pair (V, T) that results in conditions (C) being satisfied, it is possible to find not just one polynomial B , but a whole parameterized family of polynomials $B_F = B + F(T - \tilde{T}) + F^2V$ ($F \in \mathbb{F}_q[x]$) so that each pair (A, B_F) yields a hyperelliptic function field $\mathbb{K} = \mathbb{F}_q(x, \sqrt{D_F})$ of 3-rank at least 2.

Algorithm 3.6.

Input: An odd prime power q and a non-constant polynomial $A \in \mathbb{F}_q[x]$.

Output: A set of square-free polynomials $D_F \in \mathbb{F}_q[x]$ ($F \in \mathbb{F}_q[x]$) such that each hyperelliptic function field $\mathbb{K}_F = \mathbb{F}_q(x, \sqrt{D_F})$ has 3-rank at least 2.

Algorithm:

1. Let \mathcal{N} be the set of all non-constant $V \in \mathbb{F}_q[x]$ satisfying the degree bound(s) given in Lemma 3.3 and, if $q \equiv -1 \pmod{3}$, of the form given in Corollary 3.5.
2. For each $V \in \mathcal{N}$ do
 - 2.1 Find all $T \in \mathbb{F}_q[x]$, $|T| < |V|$, with $3A^2 + 3AT + T^2 \equiv 0 \pmod{V}$.
 - 2.2 Set $U = (3A^2 + 3AT + T^2)/V$ and $\tilde{T} = V^2 - 3A - T$.
 - 2.3 Compute the set $\mathcal{R}(V, T)$ of all $F \in \mathbb{F}_q[x]$ such that
 - $B_F \neq 0$, $B_F^2 \neq 4A^3$ where $B_F = U - TV + F(T - \tilde{T}) + F^2V$;
 - $|B_F| \leq |A|^{3/2}$;
 - $|T_F| \leq |\tilde{T}_F|$ where $T_F = T + FV$ and $\tilde{T}_F = \tilde{T} - FV$;
 - the square-free part D_F of $B_F^2 - 4A^3$ has either odd degree ≥ 3 or even degree ≥ 4 and non-square leading coefficient;
 - $A + T_F$ and $A + \tilde{T}_F$ are non-constant;
 - A , $A + T_F$, and $A + \tilde{T}_F$ do not differ by a constant factor;
 - $\lfloor (\deg(D_F) - 1)/2 \rfloor \geq \deg(A), \deg(\tilde{T}_F)$;
 - $\gcd(A, B_F)$, $\gcd(A + T_F, B_F + 2T_FV)$, and $\gcd(A + \tilde{T}_F, B_F + 2\tilde{T}_FV)$ all divide D_F .
 - 2.4 Output $\{D_F \mid F \in \mathcal{R}(T, V)\}$.

Theorem 3.7. *Algorithm 3.6 is correct.*

Proof. Let $F \in \mathcal{R}(V, T)$. As $F = (T_F - T)/V$, $|T| < |V| < |A|^{3/4}$ by Lemma 3.3, and $|T_F| \leq |\tilde{T}_F| < |D_F|^{1/2} \leq |A|^{3/2}$, we have $|F| < |T_F - T| < \max\{|A|^{3/2}, |A|^{3/4}\} = |A|^{3/2}$. It follows that the sets \mathcal{N} and $\mathcal{R}(V, T)$ are finite, so Algorithm 3.6 terminates.

Write $B_F^2 - 4A^3 = C_F^2 D_F \neq 0$, so $C_F \in \mathbb{F}_q[x]$ is the square part and D_F the square-free part of $B_F^2 - 4A^3$. Then $\mathbb{K}_F = \mathbb{F}_q(x, \sqrt{D_F})$ is an imaginary hyperelliptic function field of genus $g_F = \lfloor (\deg(D_F) - 1)/2 \rfloor$. It is easy to verify that $3A^2 + 3AT_F + T_F^2 = U_FV$ with

$$U_F = U + 3AF + 2TF + F^2V = U + F(V^2 + T - \tilde{T} + FV) .$$

Furthermore, $B_F = U_F - T_FV$ and $\tilde{T}_F = V^2 - 3A - T_F$. Set $A_1 = A$, $B_1 = B_F$, $A_2 = A + T_F$, $B_2 = B_F + 2T_FV$, $A_3 = A + \tilde{T}_F$, $B_3 = B_F + 2\tilde{T}_FV$. Then by

Lemma 3.1, $B_i^2 - 4A_i^3 = C_F^2 D_F$ for $i = 1, 2, 3$, and since $0 < \deg(A_i) \leq g_F$ for $i = 1, 2, 3$, \mathbb{K}_F has 3-rank at least 2 by Lemma 3.2. \square

We note that the set $\mathcal{R}(V, T)$ is non-empty if A has sufficiently large degree. Furthermore, we may limit our search to polynomials F with $|T_F| \leq |\tilde{T}_F|$ because otherwise, we may exchange T with \tilde{T} and replace F by $-F$ and obtain the same solution (A_1, B_1, C_F) to (2.2). However, we know of no better way to compute $\mathcal{R}(V, T)$ than to test all polynomials $F \in \mathbb{F}_q[x]$ with $|T_F| \leq |\tilde{T}_F|$. Thus, the runtime of Algorithm 3.6 is at least proportional to some power of q , so the method is only useful for small values of q .

Example 3.8. Let $A = x^4 + x = x(x+1)(x^2 + 4x + 1) \in \mathbb{F}_5[x]$. The first step of Algorithm 3.6 is to determine all $V \in \mathbb{F}_5[x]$ satisfying the degree bounds of Lemma 3.3 and, because $5 \equiv -1 \pmod{3}$, having the form given in Corollary 3.5. As $\deg(A) = 4$, we must have $\deg(V) = 2$, and by Corollary 3.5, the only permissible values of V are x^2 and $(x+1)^2 = x^2 + 2x + 1$. For each value of V , we determine all $T \in \mathbb{F}_5[x]$ with $|T| < |V|$ that satisfy $3A^2 + 3AT + T^2 \equiv 0 \pmod{V}$. As $\deg(V) = 2$, this means we need only consider T with $\deg(T) \leq 1$. We then determine the set $\mathcal{R}(V, T)$ corresponding to each (V, T) pair, each member of which yields a field with 3-rank at least 2.

For example, when $V = x^2$ and $T = 3x$, we obtain $U = (3A^2 + 3AT + T^2)/V = 3x^6 + 1$ and $\tilde{T} = V^2 - 3A - T = 3x^4 + 4x$. For $F = 2x^2$, we get $B_F = U - TV + F(T - \tilde{T}) + F^2V = x^6 + 1$ and $D_F = B_F^2 - 4A^3 = 2x^{12} + 3x^9 + x^3 + 1$. The three solutions of (2.2) obtained via Lemma 3.1 are $(A, B_F) = (x^4 + x, x^6 + 1)$, $(A+T, B_F+2TV) = (3x^4+4x, x^3+1)$, and $(A+\tilde{T}, B_F+2\tilde{T}V) = (2x^4, 3x^6+3x^3+1)$; as D_F is square-free, $C = 1$. It is easily verified that the conditions of Lemma 3.2 are satisfied, so the hyperelliptic function field $\mathbb{F}_5(x, \sqrt{D_F})$ has 3-rank at least 2. In fact, for $A = x^4 + x$, $V = x^2$, and $T = 3x$, we have $|\mathcal{R}(V, T)| = 42$, and each of the corresponding D_F values yields a hyperelliptic function field of 3-rank at least 2.

3.4. The algorithm for 3-rank at least 3. If the set $\mathcal{R}(V, T)$ is sufficiently large — in practice, this is usually the case — then there is a good chance that two distinct polynomials $G, H \in \mathcal{R}(V, T)$ produce the same polynomials B_G, B_H up to sign (and hence the same hyperelliptic function field $\mathbb{K}_G = \mathbb{K}_H$). In addition, we can expect that in some cases the solution triples (A_i, B_i, C) ($i = 1, 2, 3$) as defined in Lemma 3.1 with $T = T_G$ and $T = T_H$ produce three independent ideal classes of order 3, thereby yielding a lower bound of 3 on the 3-rank of K .

The algorithm below makes use of this fact and generates a (possibly empty) set of imaginary hyperelliptic function fields of 3-rank at least 3. We use the following notation: if \hat{V} is a polynomial generated by step 1 of Algorithm 3.6 and \hat{T} is the corresponding polynomial computed in step 2.1, then in step 2.3, $\hat{B}_F, \hat{T}_F, \hat{\tilde{T}}_F$, and \hat{D}_F have the obvious meaning.

Algorithm 3.9.

Input: An odd prime power q and a non-constant polynomial $A \in \mathbb{F}_q[x]$.

Output: Zero or more square-free polynomials $D_F(x) \in \mathbb{F}_q[x]$ ($F \in \mathbb{F}_q[x]$) such that each hyperelliptic function field $\mathbb{K}_F = \mathbb{F}_q(x, \sqrt{D_F(x)})$ has 3-rank at least 3.

Algorithm:

1. Call Algorithm 3.6 on input q and A . Set $\mathcal{S} = \{(V, T) \mid \mathcal{R}(V, T) \neq \emptyset\}$.

2. If $\#\mathcal{S} \geq 2$, then
 for all $(V, T) \in \mathcal{S}$ do
 for all $(\hat{V}, \hat{T}) \in \mathcal{S} \setminus \{(V, T)\}$ do
 for all $G \in \mathcal{R}(V, T)$ do
 for all $H \in \mathcal{R}(\hat{V}, \hat{T})$ do
 if $B_G = \pm \hat{B}_H$, none of the polynomials $A, A + T_G, A + \tilde{T}_G,$
 $A + \hat{T}_H, A + \hat{\tilde{T}}_H$ is constant and no two of them differ
 by a constant factor, then
 output D_G .

Theorem 3.10. *Algorithm 3.9 is correct, i.e. if it generates any output, it only outputs polynomials D_F such that \mathbb{K}_F has 3-rank at least 3.*

Proof. Let $(V, T), (\hat{V}, \hat{T})$ be two distinct pairs in \mathcal{S} such that $B_G = \pm \hat{B}_H$, none of the polynomials $A, A + T_G, A + \tilde{T}_G, A + \hat{T}_H, A + \hat{\tilde{T}}_H$ is constant, and no two of them differ by a constant factor. Define polynomials A_i, B_i ($1 \leq i \leq 6$) as follows:

| i | 1 | 2 | 3 | 4 | 5 | 6 |
|-------|-------|---------------|-----------------------|-------------|---------------------------|-----------------------------------|
| A_i | A | $A + T_G$ | $A + \tilde{T}_G$ | A | $A + \hat{T}_H$ | $A + \hat{\tilde{T}}_H$ |
| B_i | B_G | $B_G + 2T_GV$ | $B_G + 2\tilde{T}_GV$ | \hat{B}_H | $\hat{B}_H + 2\hat{T}_HV$ | $\hat{B}_H + 2\hat{\tilde{T}}_HV$ |

Then $B_i^2 - 4A_i^3 = C_G D_G^2$ for $i = 1, 2, 3$, and $B_i^2 - 4A_i^3 = \hat{C}_H^2 \hat{D}_H$ for $i = 4, 5, 6$. Now $A_1 = A_4$ and $B_1^2 = B_4^2$ imply $C_G D_G^2 = \hat{C}_H^2 \hat{D}_H$. Since D_G and \hat{D}_H are square-free, they differ only by a constant square factor, so $\mathbb{K}_G = \mathbb{F}_q(x, \sqrt{D_G}) = \mathbb{F}_q(x, \sqrt{\hat{D}_H})$. Normalize so that $C_G = \pm \hat{C}_H$ and $D_G = \hat{D}_H$ (this does not change the function field \mathbb{K}_G).

Let \mathfrak{a}_i be the ideal corresponding to the triple (A_i, B_i, C) ($1 \leq i \leq 6$). Then each \mathfrak{a}_i as well as its conjugate generates an ideal class of order 3 in \mathbb{K}_G . We note that $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \mathfrak{a}_5, \mathfrak{a}_6$ are pairwise distinct (again, because their norms are pairwise distinct) and are each distinct from their respective conjugate ideal (because they each generate an ideal class of order 3). Hence we have ten distinct ideal classes of order 3 in \mathbb{K}_G . The class group of \mathbb{K}_G cannot have 3-rank 2 since $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ has only eight distinct elements of order 3. Hence \mathbb{K}_G must have 3-rank at least 3. \square

Once again, the 3-rank may in fact be equal to 3, since $\mathfrak{a}_1 \mathfrak{a}_2 \mathfrak{a}_3$ and $\mathfrak{a}_4 \mathfrak{a}_5 \mathfrak{a}_6$ are both principal. Thus, we can only guarantee the independence of three ideal classes; for example, those generated by $\mathfrak{a}_1, \mathfrak{a}_2$, and one of $\mathfrak{a}_5, \mathfrak{a}_6$.

Example 3.11. Let $A = x^4 + x \in \mathbb{F}_5[x]$. As shown in Example 3.8, there are two valid V , and each of them has five permissible T . The sets $\mathcal{R}(V, T)$ are non-empty for each (V, T) pair, so we have $|\mathcal{S}| = 10$. Algorithm 3.9 searches for two distinct pairs (V, T) and (\hat{V}, \hat{T}) in \mathcal{S} such that $B_G = \pm \hat{B}_H$, where $G \in \mathcal{R}(V, T)$ and $H \in \mathcal{R}(\hat{V}, \hat{T})$. From Example 3.8, we have that $(x^2, 3x) = (V, T) \in \mathcal{S}$ with $G = 2x^2 \in \mathcal{R}(V, T)$ and $B_G = x^6 + 1$. Algorithm 3.6 finds that the pair $(x^2 + 2x + 1, 4x + 4) = (\hat{V}, \hat{T})$ is also in \mathcal{S} , with $H = 2x^2 + x + 4 \in \mathcal{R}(\hat{V}, \hat{T})$ and $\hat{B}_H = x^6 + 1 = B_G$. From Example 3.8 we have $A + T_G = 3x^4 + 4x$ and $A + \tilde{T}_G = 2x^4$, and the corresponding values for H are $A + \hat{T}_H = 3x^4 + 3x^2 + 4x + 3$ and $A + \hat{\tilde{T}}_H = 2x^4 + 4x^3 + 3x^2 + 4x + 3$. As none of $A, A + T_G, A + \tilde{T}_G, A + \hat{T}_H$, and $A + \hat{\tilde{T}}_H$ is constant and no two among them differ by a constant factor, by Theorem 3.10, the hyperelliptic function field

$\mathbb{F}_5(x, \sqrt{D_F})$ with $D_F = 2x^{12} + 3x^9 + x^3 + 1$ has 3-rank at least 3. In fact, the ideal class group of this field is isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/100\mathbb{Z}$.

4. OTHER CONSTRUCTIONS

For completeness, we mention some of the other constructions for finding quadratic number fields of high 3-rank that were cited in Section 1. We have generalized these constructions to the hyperelliptic function field setting and conducted numerical experiments in order to explore their suitability for generating high 3-rank function fields.

4.1. The Shanks/Weinberger fields. In [34], it was shown that the imaginary quadratic fields $\mathbb{Q}(\sqrt{-3p})$, where p is a prime of the form $p = A^6 + 4B^6$, have 3-rank at least one and are escalatory if and only if B is a multiple of 3. The first result (positive 3-rank) extends readily to the analogous function fields $\mathbb{K} = \mathbb{F}_q(x, \sqrt{-3P(x)})$ where $q \equiv -1 \pmod{3}$, $P(x) = A(x)^6 + 4B(x)^6$ is irreducible with $A(x), B(x) \in \mathbb{F}_q[x] \setminus \mathbb{F}_q$, and if $|A| = |B|$, then $\text{sgn}(A)^6 \neq -4\text{sgn}(B)^6$. It is not known whether there is a similar simple condition to determine whether these function fields are escalatory.

4.2. The Shanks series. In [30], Shanks defined four “series” of discriminants:

$$\begin{aligned} \text{Series 1: } \Delta(w) &= (3w^2 - 12w + 18)^2 - 2w^3, \\ \text{Series 2: } \Delta_2(x) &= (6x^2 - 12x + 9)^2 - 4x^3 = \Delta(2x)/4, \\ \text{Series 3: } \Delta_3(y) &= 9(3y^2 - 4y + 2)^2 - 6y^3 = \Delta(3y)/9, \\ \text{Series 6: } \Delta_6(z) &= 9(6z^2 - 4z + 1)^2 - 12z^3 = \Delta(6z)/9. \end{aligned}$$

He proved that with the exception of certain small cases, the fields $\mathbb{Q}(\sqrt{-3\Delta(w)})$ and $\mathbb{Q}(\sqrt{-3\Delta_2(x)})$ generated by square-free radicands of series 1 and 2, respectively, have positive 3-rank and are non-escalatory, while the series 3 and 6 fields $\mathbb{Q}(\sqrt{-\Delta_3(y)/3})$ and $\mathbb{Q}(\sqrt{-\Delta_6(y)/3})$ (again considering square-free radicands only) have 3-rank at least 2 and are escalatory, thereby producing infinite families of real quadratic fields of 3-rank at least 1. Numerical examples revealed that some of the series 3 and 6 fields in [30] had 3-rank 3, and [33] produced instances in these series of 3-rank 4. Subsequent follow-up computations [20], [27], [21] using the Shanks series 3 and 6 as well as the Diaz y Diaz technique [10] and Mestre’s elliptic curve method [22] produced many more imaginary quadratic fields of 3-rank 3 and 4 as well as 20 examples of 3-rank 5. The latter include two series 3 fields and two series 6 fields; being escalatory, these three Shanks fields give rise to four real quadratic fields of 3-rank 4.

In the function field setting, these series all produce the same fields. Once again, the lower bounds on the 3-rank of the Shanks series fields extend easily to the corresponding function fields — we need to again assume that $q \equiv -1 \pmod{3}$ to obtain imaginary hyperelliptic fields, and the parameters w, x, y, z need to be polynomials with coefficients in \mathbb{F}_q . Our numerical data indicates that some of the fields produced are escalatory, while some are not. Again, it is not known whether there is a simple condition to separate the two cases.

4.3. Craig's construction. The imaginary quadratic number fields generated by Craig's method [7] have 3-rank at least 3, but tend to be large. In his construction, Craig made use of two results originally due to Yamamoto [38] on constructing independent ideal classes of some fixed order in a quadratic number field. Craig considered Mordell's parameterized solutions

$$X = S^4, \quad Y = S(18T^3 - S^3), \quad Z = 18T^4, \quad W = 3T(S^3 - 6T^3)$$

of the Diophantine equation $X^3 + Y^3 = 2(Z^3 + W^3)$ [24]. From these quadruples (X, Y, Z, W) , he constructed five pairs (A_i, B_i) ($1 \leq i \leq 5$) such that $4A_i^3 - B_i^2 = 4A_j^2 - B_j^2$ for all i, j . These five pairs give rise to ideal classes of order 3 in the quadratic number field $\mathbb{Q}(\sqrt{D})$ where D is the square-free part of $B_i^2 - 4A_i^3$ for all i . Using Yamamoto's theorem, three of these classes can be shown to be independent, thereby producing a quadratic number field of 3-rank at least 3.

Yamamoto's results as well as Craig's reasoning can be readily extended to hyperelliptic function fields over a finite field \mathbb{F}_q with certain restrictions on q ; for details, see [3]. Unfortunately, in this setting, the technique produces just two independent ideal classes of order 3, thereby guaranteeing a lower bound of only 2 on the 3-rank of the field. This is due to the fact that 7 is a prime in \mathbb{Q} , whereas it is of course a constant in $\mathbb{F}_q(t)$. As a result, in the function field scenario, only two (but no three) of Craig's five pairs (A_i, B_i) can be proved to produce independent ideal classes using Yamamoto's results. Furthermore, not surprisingly, the method produces huge function fields; see Section 6.1.

It is worth mentioning that Craig also provided a remarkable method for creating quadratic number fields of 3-rank at least 4 [8], but the algorithm is impractical — the smallest suitable D has over 100 decimal digits — so we did not investigate an extension of this method to function fields.

5. INCREASING THE FIELD OF CONSTANTS

Until now, we have only considered the case $d = 3$, i.e. the question of constructing a hyperelliptic function field of high 3-rank, and we used number field methods to accomplish this. In contrast to this approach, we will now explain how to increase the 3-rank — or more generally, the l -rank for any prime l coprime to q — of a given hyperelliptic function field by extending the base field \mathbb{F}_q . In other words, we fix a hyperelliptic curve and vary the field over which we consider the curve. This technique has no analogue to number fields. While both strategies may be employed independently of each other, the combination of the two will generate examples of hyperelliptic fields with maximal 3-rank very efficiently. Furthermore, if the hyperelliptic curve is defined over a small field \mathbb{F}_q , then the resulting examples with maximal 3-rank of $2g$ may still be defined over a reasonably small extension field.

We point out that the results in this section apply to both real and imaginary hyperelliptic function fields of both even and odd characteristic. Specifically, we investigate the l -rank of the Jacobian, rather than the ideal class group, of the extension $\mathbb{K}/\mathbb{F}_q(x)$. We saw that if $\mathbb{K}/\mathbb{F}_q(x)$ is imaginary, both these groups have identical l -rank. However, when $\mathbb{K}/\mathbb{F}_q(x)$ is real, then the exact sequence (2.1) no longer applies, so in this case, the Jacobian will generally have much larger l -rank than the ideal class group.

Let $\mathbb{K} = \mathbb{F}_q(x, y)$ be a hyperelliptic function field of genus g over a finite field \mathbb{F}_q ; if q is odd, then we again write the corresponding hyperelliptic curve as $y^2 = D(x)$. The idea is to increase the base field from \mathbb{F}_q to \mathbb{F}_{q^n} for some $n \in \mathbb{N}$. We note that this may change the signature of the extension, i.e. the splitting behaviour of the place at infinity in $\mathbb{F}_q(x)$ in the resulting function field. Set $\mathbb{K}_n = \mathbb{K}\mathbb{F}_{q^n} = \mathbb{F}_{q^n}(x, y)$. In the case of odd q , the signature of \mathbb{K}_n relates to that of \mathbb{K} as follows. If $\deg(D)$ is odd, then both extensions $\mathbb{K}/\mathbb{F}_q(x)$ and $\mathbb{K}_n/\mathbb{F}_{q^n}(x)$ are totally ramified at infinity and hence imaginary. If $\mathbb{K}/\mathbb{F}_{q^n}(x)$ is real, then so is $\mathbb{K}_n/\mathbb{F}_{q^n}(x)$, but the converse need not be true. More specifically, if $\deg(D)$ is even and $\text{sgn}(D)$ is a non-square in \mathbb{F}_q^* , then $\mathbb{K}/\mathbb{F}_q(x)$ is imaginary (with the place at infinity of $\mathbb{F}_q(x)$ inert in \mathbb{K}), and $\mathbb{K}_n/\mathbb{F}_{q^n}(x)$ is still imaginary if n is odd, but $\mathbb{K}_n/\mathbb{F}_{q^n}(x)$ is real (with the place at infinity of $\mathbb{F}_{q^n}(x)$ split in \mathbb{K}_n) if n is even.

Rather than limiting ourselves to the 3-rank, we discuss the more general setting of the l -rank of a field \mathbb{K}_n , where l is a prime not dividing q ; some of our reasoning even applies to the d -rank where d is any integer coprime to q . Specifically, we will address the following questions:

1. How can we compute the minimal positive integer n_l such that $\mathbb{K}_{n_l}/\mathbb{F}_{q^{n_l}}$ has maximal l -rank $2g$? Can we at least find an upper bound on n_l ?
2. How can we find a positive integer n such that the l -rank of $\mathbb{K}_n/\mathbb{F}_{q^n}$ is guaranteed to exceed the l -rank of \mathbb{K}/\mathbb{F}_q ? What is (a lower bound on) the increase in l -rank?

For question 1, we use the fact that n_l is the order of a $2g \times 2g$ matrix M_l arising from a certain Galois representation. This order is easily computed if M_l is converted to a suitable normal form; here, we will choose the primary rational canonical form which is determined by the minimal polynomial of M_l . We do not know this minimal polynomial, but we are able to compute the characteristic polynomial F_l of M_l , using a deep result originally due to Weil [37] that links F_l to the L -polynomial $L(t)$ of \mathbb{K}/\mathbb{F}_q . The L -polynomial can be computed relatively easily if q and g are of reasonable size. Furthermore, if $F_l(t)$ has an irreducible divisor P different from $t-1$, then we can provide an answer to question 2 above; namely, we know that the l -rank increases by at least $\deg(P)$ if n is taken to be the order of a certain block submatrix of M_l corresponding to P .

5.1. Theoretical background. We denote by $\overline{\mathbb{F}_q}$ the algebraic closure of \mathbb{F}_q . For any field \mathbb{E} with $\mathbb{F}_q \subseteq \mathbb{E} \subseteq \overline{\mathbb{F}_q}$, let $\text{Gal}(\mathbb{E}/\mathbb{F}_q)$ denote the Galois group of \mathbb{E}/\mathbb{F}_q and $\text{Jac}(\mathbb{E})$ the group of \mathbb{E} -rational points on the Jacobian of the hyperelliptic curve defining \mathbb{K} . For brevity, write $\mathcal{G} = \text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ and $\mathcal{J} = \text{Jac}(\overline{\mathbb{F}_q})$. Note that $\text{Jac}(\mathbb{F}_q) \subseteq \text{Jac}(\mathbb{E}) \subseteq \mathcal{J}$ up to isomorphism (see pp. 177-179 of [28]). For any $d \in \mathbb{N}$, denote by $\text{Jac}(\mathbb{E})[d]$ the d -torsion group of $\text{Jac}(\mathbb{E})$, i.e. the subgroup of elements in $\text{Jac}(\mathbb{E})$ whose order divides d . For brevity, we write $\mathcal{J}[d] = \text{Jac}(\overline{\mathbb{F}_q})[d]$.

We let $\pi_q \in \mathcal{G}$ denote the absolute q -th power Frobenius automorphism defined via $\pi_q(\alpha) = \alpha^q$ for all $\alpha \in \overline{\mathbb{F}_q}$. Note that the action of π_q extends to \mathcal{J} and to $\mathcal{J}[d]$. If \mathbb{E}/\mathbb{F}_q is a finite extension, i.e. $\mathbb{E} = \mathbb{F}_{q^n}$ for some $n \in \mathbb{N}$, then let $\pi_{q,n}$ denote the restriction of π_q to \mathbb{F}_{q^n} . Then the Galois group $\text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is a cyclic group of order n generated by $\pi_{q,n}$. The action of $\pi_{q,n}$ once again extends to $\text{Jac}(\mathbb{F}_{q^n})$ and to $\text{Jac}(\mathbb{F}_{q^n})[d]$.

Galois representations. Details about the following discussion can be found on pp. 180ff. of [28]. Let d be any positive integer coprime to q . By p. 180 of [28] (Corollary

to Theorem 11.12), $\mathcal{J}[d]$ is isomorphic to $2g$ copies of $\mathbb{Z}/d\mathbb{Z}$, so the maximal d -rank that is possible⁴ for any extension $\mathbb{K}_n/\mathbb{F}_{q^n}$ is $2g$. However, since $\mathcal{J}[d]$ is a finite subgroup of \mathcal{J} that is invariant under the action of \mathcal{G} on \mathcal{J} , the field of rationality of $\mathcal{J}[d]$, i.e. the smallest extension \mathbb{E}/\mathbb{F}_q with $\mathcal{J}[d] \subseteq \text{Jac}(\mathbb{E})$, is a finite extension of \mathbb{F}_q whose degree over \mathbb{F}_q is our desired value n_d from question 1 above; that is, $\text{Jac}(\mathbb{F}_{q^{n_d}})[d] \cong (\mathbb{Z}/d\mathbb{Z})^{2g}$.

If $\text{Aut}(\mathcal{J}[d])$ denotes the group of automorphisms of $\mathcal{J}[d]$, then the exact sequence

$$(5.1) \quad (0) \rightarrow \text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_{q^{n_d}}) \rightarrow \mathcal{G} \rightarrow \text{Aut}(\mathcal{J}[d])$$

gives rise to an injection $\text{Gal}(\mathbb{F}_{q^{n_d}}/\mathbb{F}_q) \cong \mathcal{G}/\text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_{q^{n_d}}) \rightarrow \text{Aut}(\mathcal{J}[d])$. Since $\mathcal{J}[d] \cong (\mathbb{Z}/d\mathbb{Z})^{2g}$, we have $\text{Aut}(\mathcal{J}[d]) \subseteq \text{Gl}_{2g}(\mathbb{Z}/d\mathbb{Z})$, the group of non-singular matrices over $\mathbb{Z}/d\mathbb{Z}$. Thus, we obtain an injection

$$(5.2) \quad \rho_d : \text{Gal}(\mathbb{F}_{q^{n_d}}/\mathbb{F}_q) \rightarrow \text{Gl}_{2g}(\mathbb{Z}/d\mathbb{Z}) .$$

Since ρ_d is injective and π_{q,n_d} is a generator of $\text{Gal}(\mathbb{F}_{q^{n_d}}/\mathbb{F}_q)$, n_d is equal to the order of the matrix $M_d = \rho_d(\pi_{q,n_d})$. Hence, in order to find n_d , it suffices to find the image M_d of π_{q,n_d} under the Galois representation ρ_d and compute its order in $\text{Gl}_{2g}(\mathbb{Z}/d\mathbb{Z})$. Note that this order is invariant under similarity, so if $A = S^{-1}M_dS$ for some $S \in \text{GL}_{2g}(\mathbb{Z}/d\mathbb{Z})$, then obviously, $\text{ord}(A) = \text{ord}(M_d)$. Our goal is therefore to find a normal form A of M_d that is explicitly computable and for which $\text{ord}(A)$ is easy to find. We choose for A the primary rational canonical form of M_d , which can be determined from the minimal polynomial of π_{q,n_d} .

Primary rational canonical form. The following material can be found for example in Section 4, Chapter VII, of [16]. Let V be a vector space over some field k and ϕ a linear transformation on V . We say that ϕ *acts cyclically* on a subspace W of V if W is spanned by the set $\{\phi^i(v) \mid i \geq 0\}$ for some $v \in V$; in this case, W is said to be *ϕ -cyclic*. Recall that the *minimal polynomial* of ϕ is the unique monic polynomial $G_\phi(t) \in k[t]$ of minimal degree with $G_\phi(\phi) = 0$; it divides all other polynomials F with $F(\phi) = 0$, including the characteristic polynomial F_ϕ of ϕ .

For any monic polynomial $f(t) = t^r + a_{r-1}t^{r-1} + \cdots + a_0 \in k[t]$, the $r \times r$ matrix

$$A_f = \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 & 0 \\ \cdot & & & & & & \cdot \\ \cdot & & & & & & \cdot \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 \\ -a_0 & -a_1 & -a_2 & -a_3 & \cdots & -a_{r-2} & -a_{r-1} \end{pmatrix}$$

is called the *companion matrix* of $f(t)$. Theorem 4.3, p. 358, of [16] states that ϕ acts cyclically on a subspace W of V if and only if W has an ordered basis relative to which the matrix associated to the restriction $\phi|_W$ of ϕ to W is the companion matrix of the minimal polynomial of $\phi|_W$. In general, ϕ will not act cyclically on V , but we have the following decomposition theorem (see Theorem 4.2 on p. 356, Theorem 4.6 on p. 360, and Theorem 5.2 on p. 367, of [16]):

⁴We note that when l divides q , i.e. l is equal to the characteristic of \mathbb{F}_q , then the maximal l -rank of \mathcal{J} is only g , and all l -ranks between 1 and g are possible. The theory behind this scenario is very different from the case where l does not divide q which we consider here; see [39] and [26], for example.

Let $d = l^n$ be a prime power coprime to q . The exact sequence (5.1) specifies a homomorphism from \mathcal{G} to $Gl_{2g}(\mathbb{Z}/l^n\mathbb{Z})$. The action of \mathcal{G} on $\mathcal{J}[l^n]$ extends to the Tate module which is the inverse limit

$$T_l(\mathcal{J}) = \varprojlim_n \mathcal{J}[l^n] ,$$

and consequently, we obtain a homomorphism from \mathcal{G} to $Gl_{2g}(\mathbb{Z}_l)$, where \mathbb{Z}_l denotes the l -adic integers. Note that applying reduction modulo l to this homomorphism yields the map ρ_l of (5.2) (with $d = l$).

Let $F_{\pi_q}(t)$ be the characteristic polynomial of the action of the absolute Frobenius π_q on $T_l(\mathcal{J})$. Then $F_{\pi_q}(t) = t^{2g}L(t^{-1})$ (see for example [23], p. 144). Again applying reduction modulo l , we see that $F_{\pi_q}(t) \equiv F_{\pi_{q,n_l}}(t) \pmod{l}$, and we obtain

$$(5.3) \quad F_{\pi_{q,n_l}}(t) \equiv t^{2g}L(t^{-1}) \pmod{l} .$$

Since $F_{\pi_{q,n_l}}(t)$ has coefficients in \mathbb{F}_l , the L -polynomial of \mathbb{K}/\mathbb{F}_q uniquely determines $F_{\pi_{q,n_l}}(t)$.

5.2. Algorithms for increasing the l -rank. Let l be a prime not dividing q (in our previous context, $l = 3$). Then $Jac(\mathbb{F}_{q^{n_l}})[l] \cong (\mathbb{Z}/l\mathbb{Z})^{2g}$ is a $2g$ -dimensional vector space over the finite field \mathbb{F}_l , and the action of the q -th power Frobenius π_{q,n_l} on $Jac(\mathbb{F}_{q^{n_l}})[l]$ (which we also denote by π_{q,n_l}) is a linear map on this space. By Section 5.1, the parameter n_l of question 1 above is equal to the order of the matrix $A_{\pi_{q,n_l}}$ in primary rational canonical form corresponding to the image M_l of π_{q,n_l} under the injection (5.2). The following theorem answers Question 1 which asked for an effective way to compute (an upper bound on) n_l .

Theorem 5.2. *Let $L(t)$ be the L -polynomial of \mathbb{K}/\mathbb{F}_q , and set $F(t) \equiv t^{2g}L(t^{-1}) \pmod{l}$, $F(t) \in \mathbb{F}_l[t]$. Let $F = P_1^{m_1}P_2^{m_2}\dots P_s^{m_s}$ be the factorization of F into distinct monic irreducibles in $\mathbb{F}_l[t]$ and define a set \mathcal{S} as follows:*

$$(5.4) \quad \mathcal{S} = \{ (P_i^{m_{ij}}) \mid 1 \leq i \leq s, 1 \leq j \leq k_i, m_{i1} \geq \dots \geq m_{ik_i} \geq 1, \\ \text{and } \sum_{j=1}^{k_i} m_{ij} = m_i \text{ for } 1 \leq i \leq s \} .$$

For any tuple $\mathbf{P} = (P_i^{m_{ij}}) \in \mathcal{S}$, define the matrix

$$(5.5) \quad A_{\mathbf{P}} = \begin{pmatrix} A_{11} & & & & \\ & A_{12} & & & 0 \\ & & \ddots & & \\ & & & \ddots & \\ & 0 & & & A_{sk_s} \end{pmatrix} ,$$

where A_{ij} is the companion matrix of $P_i^{m_{ij}}$. Then $b = \max\{\text{ord}(A_{\mathbf{P}}) \mid \mathbf{P} \in \mathcal{S}\}$ is an upper bound on n_l , and is equal to n_l if $F(t)$ is square-free.

Proof. By (5.3) we have $F(t) = F_{\pi_{q,n_l}}(t)$, so by Theorem 5.1, the set \mathcal{S} consists of all possible choices for the elementary divisors of π_{q,n_l} . Hence, the collection of matrices $A_{\mathbf{P}}, \mathbf{P} \in \mathcal{S}$, represents all possible choices for the matrix $A_{\pi_{q,n_l}}$ corresponding to π_{q,n_l} as described in Theorem 5.1. Since $n_l = \text{ord}(A_{\pi_{q,n_l}})$, b is an upper bound on

n_l . If $F(t)$ is square-free, then $m_i = 1$ for $1 \leq i \leq s$, so \mathcal{S} contains only the one tuple $\mathbf{P} = (P_1, P_2, \dots, P_s)$. Hence $A_{\mathbf{P}} = A_{\pi_{q, n_l}}$, and hence $b = n_l$. \square

If the set \mathcal{S} of (5.4) is not too large, i.e. there are not too many choices for the elementary divisors of π_{q, n_l} , then it is feasible to compute the bound b on n_l of Theorem 5.2 via an exhaustive search on \mathcal{S} . Computationally, this will not be costly compared to the effort of determining the L -polynomial of \mathbb{K}/\mathbb{F}_q which is far more difficult and dominates the run-time of this approach.

The following is an algorithmic description of Theorem 5.2:

Algorithm 5.3.

Input: A prime power q , a hyperelliptic function field \mathbb{K}/\mathbb{F}_q of genus g , and a prime l not dividing q .

Output: The minimal integer n_l such that the extension $\mathbb{K}_{n_l}/\mathbb{F}_{q^{n_l}}$ has l -rank $2g$ or, if this is impossible, an upper bound b on n_l .

Algorithm:

1. Compute the L -polynomial $L(t)$ of \mathbb{K}/\mathbb{F}_q .
2. Set $F(t) \equiv t^{2g}L(t^{-1}) \pmod{l}$, $F(t) \in \mathbb{F}_l[t]$.
3. Find the factorization $F = P_1^{m_1}P_2^{m_2}\dots P_s^{m_s}$ of $F(t)$ into distinct monic irreducible polynomials in $\mathbb{F}_l[t]$.
4. Compute the set \mathcal{S} of (5.4).
5. Set $b = \max\{\text{ord}(A_{\mathbf{P}}) \mid \mathbf{P} \in \mathcal{S}\}$ with $A_{\mathbf{P}}$ given in (5.5).
6. If $m_i = 1$ for $1 \leq i \leq s$, output $n_l = b$, else indicate that it is impossible to find n_l and output the upper bound b on n_l .

For clarity, we have given the simplest description of this technique. One can speed up step 5 considerably by considering the effect that repeated factors of a polynomial have on the order of its companion matrix. In particular, if P is an irreducible polynomial in $\mathbb{F}_l[t]$ and $n = \text{ord}(A_P)$, then for any $k \in \mathbb{N}$, A_{P^k} has order $nl^{\lceil \log_l k \rceil}$. However, we again point out that step 5 is not the bottleneck in the computation, so the previous algorithm is sufficient for any practical application.

Example 5.4. Consider $q = 373$, the hyperelliptic function field $\mathbb{K} = \mathbb{F}_{373}(x, \sqrt{D})$ of genus 4 with

$$D(x) = x^9 + 245x^8 + 175x^7 + 340x^6 + 122x^5 + 70x^4 + 196x^3 + 210x^2 + 316x + 337 ,$$

and $l = 3$. Using Magma, it is possible to determine that the zeta function of \mathbb{K} is $\zeta(t) = L(t)/(373t^2 - 374t + 1)$ with

$$L(t) = 373^4 t^8 + 33 \cdot 373^3 t^7 + 347 \cdot 373^2 t^6 - 3785 \cdot 373 t^5 - 188703 t^4 - 3785 t^3 + 347 t^2 + 33 t + 1 .$$

In step 2 of Algorithm 5.3, we obtain

$$F(t) = t^8 + 2t^6 + t^5 + t^3 + 2t^2 + 1 .$$

This polynomial is irreducible over \mathbb{F}_3 , so the set \mathcal{S} of (5.4) is $\mathcal{S} = \{F\}$, and we simply calculate the order of the companion matrix A_F which is 41. We conclude that $\mathbb{K}/\mathbb{F}_{373}$ has 3-rank 0, and the same is true for every extension $\mathbb{K}_n/\mathbb{F}_{373^n}$ with $n < 41$. Furthermore, $\text{Jac}(\mathbb{F}_{373^{41}})$ has full 3-rank $2 \cdot 4 = 8$.

Example 5.4 obviously represents the best possible outcome for Algorithm 5.3. We provide another example where the outcome is not as conclusive, which will also

be useful shortly in describing how to derive partial information about the l -rank from factors $t - 1$ of the characteristic polynomial.

Example 5.5. Consider $q = 179$, the hyperelliptic function field $\mathbb{K} = \mathbb{F}_{179}(x, \sqrt{D})$ of genus 4 with

$$D(x) = x^9 + 151x^8 + 168x^7 + 10x^6 + 32x^5 + 141x^4 + 110x^3 + 35x^2 + 160x + 2 ,$$

and $l = 3$. Again, with the aid of Magma, it is possible to determine that $\zeta(t) = L(t)/(179t^2 - 180t + 1)$ is the zeta function of \mathbb{K} with

$$L(t) = 179^4 t^8 - 17 \cdot 179^3 t^7 + 315 \cdot 179^2 t^6 - 3041 \cdot 179 t^5 + 56275 t^4 - 3041 t^3 + 315 t^2 - 17 t + 1 .$$

Step 2 of Algorithm 5.3 yields

$$F(t) = t^8 + t^7 + t^5 + t^4 + 2t^3 + 2t + 1 .$$

Over \mathbb{F}_3 , $F(t)$ factors as $F = P_1 P_2 P_3^2 P_4$ where

$$P_1 = t + 1, \quad P_2 = t + 2, \quad P_3 = t^2 + 1, \quad P_4 = t^2 + t + 2 ,$$

so the set \mathcal{S} of (5.4) is

$$\mathcal{S} = \{ (P_1, P_2, P_3, P_3, P_4), (P_1, P_2, P_3^2, P_4) \} .$$

The companion matrices of $P_1, P_2, P_3, P_3^2, P_4$ have orders 2, 1, 4, 12, and 8, respectively, so the two matrices $A_{\mathbf{P}}, \mathbf{P} \in \mathcal{S}$, have respective orders 8 and 24, producing $b = 24$ in step 5 of Algorithm 5.3. We conclude that $Jac(\mathbb{F}_{179^{24}})$ has 3-rank 8.

Let V_{21} be the subspace of $Jac(\mathbb{F}_{179})$ corresponding to $P_2 = t - 1$ as described in Theorem 5.1. Then π_{n_3} restricted to V_{21} has eigenvalue 1 and is hence the identity. Therefore, $V_{21} = \mathbb{F}_{179}$, so $Jac(\mathbb{F}_{179})$ has 3-rank at least 1. In fact, it has 3-rank exactly 1, as no higher power of $t - 1$ divides $F(t)$.

We now demonstrate how to derive additional information about the l -rank of extensions \mathbb{K}_n of a hyperelliptic function field \mathbb{K} using factors of the form $t - 1$ of $F(t)$. Suppose \mathbb{K}/\mathbb{F}_q already has positive l -rank at least $r \in \mathbb{N}$; for example, $l = 3$ and \mathbb{K}/\mathbb{F}_q was constructed using one of the methods discussed in Sections 3 and 4. Then $Jac(\mathbb{F}_q) \cong (\mathbb{Z}/l\mathbb{Z})^r \times \mathcal{H}$ for some suitable finite Abelian group \mathcal{H} , and $t - 1$ must divide the characteristic polynomial $F(t)$ of π_{q, n_i} at least r times. Using the notation of Theorem 5.1, write $P_i = t - 1$ and $v_{t-1}(F) = m_i$ for a suitable index i . Then the diagonal $m_i \times m_i$ block submatrix A_i corresponding to the elementary divisors $(t - 1)^{m_{ij}}, 1 \leq j \leq k_i$, is

$$A_i = \begin{pmatrix} A_{i1} & & & & \\ & A_{i2} & & & 0 \\ & & \ddots & & \\ & & & 0 & \\ & & & & A_{ik_i} \end{pmatrix} ,$$

where A_{ij} is the companion matrix of $(t - 1)^{m_{ij}}, 1 \leq j \leq k_i$. Note that each A_{ij} has 1 as its only eigenvalue, with an eigenspace of dimension 1. Since \mathbb{K}/\mathbb{F}_q has l -rank at least r , the eigenspace of A_i corresponding to its only eigenvalue 1 has dimension at least r . It follows that there must be at least r matrices A_{ij} , so $k_i \geq r$. Thus, r is a lower bound on the number of terms in the sum $\sum_{j=1}^{k_i} m_{ij} = m_i$ appearing in

(5.4). This additional restriction can be taken into account when determining the set \mathcal{S} in step 4 of Algorithm 5.3. In particular, if $r = m_i$, then $k_i = r$ and $m_{ij} = 1$ for $1 \leq j \leq k_i$, so $A_i = I_{m_i}$, the $m_i \times m_i$ identity matrix, in which case $Jac(\mathbb{F}_q)$ has l -rank exactly m_i .

We now provide an answer to question 2, i.e. by how much the base field must be extended to guarantee an increase in l -rank.

Theorem 5.6. *Let $L(t)$ be the L -polynomial of \mathbb{K}/\mathbb{F}_q , and set $F(t) \equiv t^{2g}L(t^{-1}) \pmod{l}$, $F(t) \in \mathbb{F}_l[t]$. Suppose $F(t)$ has an irreducible factor $P(t) \in \mathbb{F}_l[t]$, different from $t-1$. Let n be the order of the companion matrix A_P of P in $Gl_{\deg(P)}(\mathbb{F}_l)$. Then the l -rank of \mathbb{K}_n exceeds the l -rank of any proper subfield of \mathbb{K}_n by at least $\deg(P)$.*

Proof. Without loss of generality, assume that P is monic. Then some power P^k of P is an elementary divisor of π_{q,n_l} . Since P is irreducible, it has $\deg(P)$ distinct roots α_i , $1 \leq i \leq \deg(P)$. Let n be the order of α_1 in $\mathbb{F}_q(\alpha_1)^*$. Since all the α_i are Galois conjugates, each α_i also has order n in $\mathbb{F}_q(\alpha_i)^*$.

Now since P^k has the same roots as P , the matrix A_{P^k} has the same eigenvalues as A_P , and since $\alpha_i \neq 1$ for $1 \leq i \leq \deg(P)$, π_{q,n_l} does not act trivially on the eigenspaces of A_{P^k} . Furthermore, each α_i corresponds to a distinct eigenspace V_i of A_{P^k} of dimension 1. Since $\alpha_i^n = 1$ for $1 \leq i \leq \deg(P)$, the only eigenvalue of the matrix $A_{P^k}^n$ is 1, and the V_i are independent subspaces that are invariant under $A_{P^k}^n$. Hence, $A_{P^k}^n$ has only one eigenvalue of 1 with an eigenspace $W = \bigoplus_{i=1}^{\deg(P)} V_i$ of dimension $\deg(P)$.

Since $n = \text{ord}(A_{P^k})$, n is the minimal positive exponent such that π_{q,n_l}^n acts trivially on any non-trivial subspace of W . Therefore, $W \subseteq Jac(\mathbb{F}_{q^n}) \setminus Jac(\mathbb{E})$ for any subfield \mathbb{E} of \mathbb{F}_{q^n} . Since W has dimension $\deg(P)$, it follows that the l -rank of $Jac(\mathbb{F}_{q^n})$ exceeds the l -rank of $Jac(\mathbb{E})$ by at least $\deg(P)$. \square

It is important to note here that if we have different non-trivial irreducible factors of the same degree, we can draw the same conclusion about each factor independently. Since these factors correspond to disjoint subspaces, we may combine the contributions of all the factors to the process of increasing the l -rank. We will provide an illustrative example for this reasoning, but once again, we first formulate the previous theorem as an algorithm:

Algorithm 5.7.

Input: A prime power q , a hyperelliptic function field \mathbb{K}/\mathbb{F}_q of genus g , and a prime l not dividing q .

Output: Integers n, m so that the l -rank of \mathbb{K}_n exceeds the l -rank of any proper subfield of \mathbb{K}_n by at least m , or possibly no output.

Algorithm:

1. Compute the L -polynomial $L(t)$ of \mathbb{K}/\mathbb{F}_q .
2. Set $F(t) \equiv t^{2g}L(t^{-1}) \pmod{l}$, $F(t) \in \mathbb{F}_l[t]$.
3. Find the factorization $F = P_1^{m_1}P_2^{m_2} \dots P_s^{m_s}$ of $F(t)$ into distinct monic irreducible polynomials in $\mathbb{F}_l[t]$.
4. Find an index $i \in \{1, 2, \dots, s\}$ such that $P_i \neq t-1$. If no such index exists, abort. Else set $m = \deg(P_i)$.
5. Compute the order n of the companion matrix of P_i in $Gl_m(\mathbb{F}_l)$.
6. Output n, m .

Example 5.8. We revisit Example 5.5. Recall that the characteristic polynomial factored over \mathbb{F}_3 as $F = P_1 P_2 P_3^2 P_4$ where

$$P_1 = t + 1, \quad P_2 = t + 2, \quad P_3 = t^2 + 1, \quad P_4 = t^2 + t + 2 .$$

$F(t)$ has three irreducible factors P_1, P_2, P_4 with exponent 1. The corresponding orders of the companion matrices A_{P_1}, A_{P_2} and A_{P_4} are 2, 1 and 8, respectively. We already saw how the factor $P_2 = t - 1$ established that $Jac(\mathbb{F}_{179})$ has 3-rank 1. Since $\text{ord}(A_{P_1}) = 2$, by Theorem 5.6, the 3-rank of $Jac(\mathbb{F}_{179^2})$ exceeds the 3-rank of $Jac(\mathbb{F}_{179})$ by at least $\deg(P_1) = 1$, so $Jac(\mathbb{F}_{179^2})$ has 3-rank at least 2. In fact, none of $A_{P_4}^2, A_{P_3}^2$, and $A_{P_2}^2$ have 1 as an eigenvalue, so $Jac(\mathbb{F}_{179^2})$ has 3-rank exactly 2. Since $\text{ord}(A_{P_4}) = 8$, Theorem 5.6 shows that the 3-rank of $Jac(\mathbb{F}_{179^8})$ exceeds the rank of any proper subfield by at least 2. Since \mathbb{F}_{179^8} contains \mathbb{F}_{179^2} as a subfield, and since $Jac(\mathbb{F}_{179^2})$ has 3-rank 2, we conclude that $Jac(\mathbb{F}_{179^8})$ has 3-rank at least 4.

It is possible to deduce even more. Note that the matrix $A_{\pi_{179, n_3}}$ consists of the companion matrices A_{P_1}, A_{P_2} , either A_{P_3} twice or $A_{P_3}^2$, and A_{P_4} . In the case where A_{P_3} appears twice, $A_{\pi_{179, n_3}}^8 = I_8$, the 8×8 identity matrix, in which case $Jac(\mathbb{F}_{179^8})$ has full 3-rank 8. In the other case, where $A_{P_3}^2$ is the third companion matrix in $A_{\pi_{179, n_3}}$, we note that $A_{P_3}^4$ has 1 as an eigenvalue of multiplicity 4, with a 2-dimensional eigenspace. So the 3-rank of $Jac(\mathbb{F}_{179^4})$ exceeds that of $Jac(\mathbb{F})$ for any subfield \mathbb{F} of \mathbb{F}_{179^4} by at least 2. Hence, $Jac(\mathbb{F}_{179^4})$ has 3-rank at least 4, and with Theorem 5.6, we see that $Jac(\mathbb{F}_{179^8})$ has 3-rank at least 6.

6. NUMERICAL RESULTS

We have implemented our generalizations of the Craig, Shanks/Weinberger Series, Shanks Series, and Diaz y Diaz methods for searching for high 3-rank hyperelliptic function fields. Our algorithms were implemented in C++ using the NTL number theory library [35] for polynomial and finite field arithmetic. We used the GNU C++ compiler version 3.2, and the computations described below were performed on a Pentium IV 2.4 GHz computer running Linux.

The group structures of our imaginary hyperelliptic function fields were computed using a slight modification of Algorithm 4.1 of [5]. Instead of the fixed set of generators required by Algorithm 4.1, we used a sequence of low-degree prime ideals and iteratively compute the subgroup generated by the first ideal, then the first two, the first three, etc. This algorithm is based on the baby-step giant-step technique, and runs in time $O(2^r \sqrt{|Jac(\mathbb{F}_q)|})$, where r is the number of prime ideals required to generate the entire Jacobian. Using the methods of [36], one computes a lower bound H on $|Jac(\mathbb{F}_q)|$ such that $H < |Jac(\mathbb{F}_q)| < 2H$. As soon as the order of the subgroup generated by the low-degree prime ideals is greater than H , then the entire Jacobian is computed and the algorithm terminates. Note that, as the bound on $|Jac(\mathbb{F}_q)|$ is unconditionally correct, the group structures we compute are also unconditionally correct and the 3-ranks quoted below are exact, not just lower bounds.

The same algorithm was used to compute the group structure of our real hyperelliptic function fields. Principality and equivalence testing were handled by computing the set of all reduced principal ideals and using table look-up. As all the examples we encountered had non-trivial ideal class groups, and in general high 3-ranks, the regulators were sufficiently small that this approach worked well.

Again, the class groups, and hence the 3-ranks, computed are unconditionally correct.

We summarize the results of our computations below.

6.1. Craig method. As mentioned in Section 4.3, this method produces huge function fields. In fact, we ran the technique using all 24 admissible primes $q < 10,000$ — the smallest of these is $q = 307$ — and obtained a total of 98,614,830 hyperelliptic function fields, each of which had genus 23. So our smallest example had a Jacobian of size roughly $307^{23} \approx 10^{58}$, which is much too large to compute the 3-rank using known methods.

6.2. Shanks/Weinberger method. We tested the Shanks/Weinberger method using $q = 5, 11, 17,$ and 23 to construct imaginary hyperelliptic function fields $\mathbb{F}_q(x, \sqrt{-3P(x)})$ with $P(x) = A(x)^6 + 4B(x)^6$, $P(x)$ square-free, and $\text{sgn}(A)^6 \neq -4\text{sgn}(B)^6$ when $|A| = |B|$. For $q = 5$, we used all $A(x)$ with $1 \leq \deg(A(x)) \leq 3$ and all $B(x)$ with $1 \leq \deg(B(x)) \leq 2$, and for $q = 11$ we used $1 \leq \deg(A(x)), \deg(B(x)) \leq 2$. For $q = 17$ and 23 , we used the same bounds on $A(x)$ and $B(x)$, but only the first 100 polynomials of each degree.

Using the algorithm outlined above, we computed the class group for each function field of unique discriminant generated. As described in Section 4.1, these function fields are guaranteed to have 3-rank at least 2 under the condition that $P(x)$ is irreducible. Our computations suggest that this irreducibility condition is unnecessary, as all our examples had 3-rank at least 2. For each value of q we found numerous examples with 3-rank as large as 5. For $q = 5$ and 17 we found examples with 3-rank 4 and genus as low as 8 for $q = 5$ and 5 for $q = 17$. For $q = 11$ and 23 we found examples with 3-rank 5 and genus as low as 5. For more details, see [3].

6.3. Shanks series method. We tested the Shanks series method using $q = 5, 11,$ and 17 to construct imaginary hyperelliptic function fields $\mathbb{F}_q(x, \sqrt{-3\Delta(w)})$ with $\Delta(w) = (3w^2 - 12w + 18)^2 - 2w^3$ square-free. For $q = 5$, we used all $w \in \mathbb{F}_q[x]$ with $1 \leq \deg(w) \leq 6$, for $q = 11$ we used $1 \leq \deg(w) \leq 4$, and for $q = 17$ we used $1 \leq \deg(w) \leq 3$. As pointed out in Section 4.2, all four Shanks series produce the same function fields, so we only considered Series 1. For each value of q we found numerous examples with 3-rank as large as 4. For $q = 5$ the smallest examples with 3-rank 4 had genus 11, and for $q = 11$ and 17 they had genus 5. For more detail see [3].

6.4. Diaz y Diaz method. We tested the Diaz y Diaz method for generating hyperelliptic function fields with 3-rank at least 2 (Algorithm 3.6) and 3 (Algorithm 3.9) using $q = 5, 7, 11, 13,$ and 17 . In Table 1, we summarize the algorithm parameters used for each value of q and give the number of fields with 3-rank at least 2 found by Algorithm 3.6. In our implementation, we considered polynomials A with $\deg A \leq \max(\deg A)$. We used all monic polynomials A of degree d when $d \leq \text{all}(A)$, and when $d > \text{all}(A)$, we used the first $\text{num}(A)$ monic polynomials of degree d for which all irreducible factors of degree larger than 2 occurred with multiplicity at most 1, as previous experiments indicated that polynomials A of this form were more likely to yield fields with 3-rank at least 3 after running Algorithm 3.9. For $q = 7$ and $q = 17$, the value $\text{num}(A)$ varied depending on $\deg(A)$. For example, as listed in Table 1, we used 1000 different A polynomials of degree

4 and 40 of degree 6 for $q = 17$. Note that $\deg(A) = 5$ does not yield any examples when $q \equiv -1 \pmod{3}$ by Lemma 3.3 and Corollary 3.5. Finally, the column denoted by $3\text{-rank} \geq 2$ contains the number of fields with 3-rank at least 2 output by Algorithm 3.6 for each value of q .

TABLE 1. Number of fields with 3-rank at least 2 from the Diaz y Diaz method.

| q | $\max(\deg A)$ | $\text{all}(A)$ | $\text{num}(A)$ | $3\text{-rank} \geq 2$ |
|-----|----------------|-----------------|------------------------|------------------------|
| 5 | 7 | 6 | 1000 | 15469080 |
| 7 | 7 | 4 | 50 (5), 20 (6), 10 (7) | 42083084 |
| 11 | 6 | 4 | 50 | 31152109 |
| 13 | 5 | 3 | 20 | 30664584 |
| 17 | 6 | 3 | 1000 (4), 40 (6) | 57636366 |

As Table 1 shows, Algorithm 3.6 produced an enormous number of fields with 3-rank at least 2; usually in the tens of millions. As a result, we only computed the class group structures for the fields output by Algorithm 3.9 that have 3-rank at least 3. Our data is summarized in Table 2. For each value of q , we give the total number of hyperelliptic function fields found over \mathbb{F}_q having the specified 3-rank (Total), the minimum genus of all such fields found ($\min g$), and the discriminant of the first such field output by our algorithm with minimum genus (First $D(x)$).

Each of $q = 5, 11,$ and 17 are congruent to $-1 \pmod{3}$, so the results of Lemma 3.4 and Corollary 3.5 restrict the search space in Algorithm 3.6. As a result, the algorithm runs much faster in these cases, but produces fewer fields of high 3-rank. Nevertheless, the Diaz y Diaz algorithms produced high 3-rank fields with the lowest genus of all the methods we implemented.

6.5. Increasing the field of constants. We applied the methods of Section 5 to the imaginary hyperelliptic function fields with odd degree D and smallest genus that we found for each 3-rank, in an effort to find fields with reasonably small class groups with even larger 3-rank. The results are presented in Table 3. The first four columns give the 3-rank of the hyperelliptic function field of discriminant D with genus g over \mathbb{F}_q . By 3-rank over \mathbb{F}_{q^2} we denote the 3-rank of the resulting field when the base field is lifted to \mathbb{F}_{q^2} , and N_3 denotes the extension degree required to ensure that the function field over $\mathbb{F}_{q^{N_3}}$ has 3-rank equal to $2g$ (so N_3 is an upper bound on n_3 in the notation of Section 5).

The addition of the 3-rank over \mathbb{F}_{q^2} made it possible to determine the sum of the dimensions of the eigenspaces for the collections of squares of the companion matrices. In some of the examples, this additional piece of information allowed for the complete determination of the original companion matrices. When it was possible to determine the degree of the minimal extension field required to obtain full 3-rank, i.e. $N_3 = n_3$, these entries were marked with asterisks.

As is to be expected, the size of N_3 is strongly correlated to the gap between the 3-rank over \mathbb{F}_q and the maximal 3-rank that is obtainable, namely $2g$; when this gap was large, N_3 was also large. The only times this gap was smaller than expected corresponded to cases where the 3-rank increased dramatically by passing to \mathbb{F}_{q^2} , and hence the missing part of the 3-rank that remained was small. As the

TABLE 2. 3-rank statistics from the Diaz y Diaz method.

| q | 3-rank | Total | $\min g$ | First $D(x)$ |
|-----|--------|--------|----------|---|
| 5 | 3 | 7664 | 5 | $2x^{12} + 3x^9 + x^3 + 1$ |
| | 4 | 298 | 8 | $3x^{17} + x^{16} + 3x^{14} + 3x^{13} + 2x^{12} + 3x^{10} + 4x^6$ $+x^5 + 2x^4 + 3x^2 + x + 3$ |
| 7 | 3 | 905362 | 4 | $3x^9 + 2x^6 + x^4 + 6x^2 + 2x + 4$ |
| | 4 | 320132 | 4 | $3x^9 + 3x^6 + x^3 + 5$ |
| | 5 | 35736 | 5 | $5x^{12} + 3x^{11} + 4x^{10} + x^9 + 2x^7 + 4x^6 + 6x^5$ $+2x^2 + 2x + 4$ |
| | 6 | 1048 | 7 | $3x^{15} + x^{14} + 3x^{12} + 4x^{11} + x^{10} + 2x^9 + 5x^8 + 4x^7$ $+2x^6 + 6x^5 + x^4 + 4x^3 + 5x^2 + x + 4$ |
| | 7 | 6 | 10 | $3x^{21} + x^{18} + 4x^{15} + x^{12} + 5x^9 + 2x^6 + 5x^3 + 4$ |
| 11 | 3 | 20175 | 4 | $7x^9 + 9x^8 + 8x^5 + 10x^4 + 10x^2 + 10x + 10$ |
| | 4 | 797 | 5 | $10x^{12} + 3x^{10} + 3x^8 + 2x^6 + 3x^4 + x^2 + 6$ |
| | 5 | 71 | 5 | $7x^{12} + 2$ |
| 13 | 3 | 363395 | 4 | $9x^9 + x^5 + 3x^4 + 4x^3 + 5x^2 + 10$ |
| | 4 | 141884 | 4 | $9x^9 + 11x^6 + 4x^3 + 5$ |
| | 5 | 16732 | 4 | $9x^9 + 4x^6 + 3x^3 + 5$ |
| | 6 | 685 | 5 | $5x^{12} + x^9 + 11x^6 + 9x^3 + 10$ |
| | 7 | 1 | 7 | $9x^{15} + 3x^{14} + 9x^{13} + 5x^{12} + 4x^{11} + 2x^{10} + 9x^9$ $+3x^8 + 9x^7 + x^6 + 4x^5 + 5x^4 + 12x^3 + 2x^2$ $+12x + 5$ |
| 17 | 3 | 2490 | 4 | $13x^9 + 15x^8 + 2x^7 + 15x^6 + 4x^5 + x^4 + 5x^3$ $+8x^2 + 7x + 8$ |
| | 4 | 51 | 5 | $13x^{11} + 12x^{10} + 6x^9 + 8x^8 + 10x^7 + 14x^6 + 9x^5$ $+11x^4 + 12x^3 + 11x^2 + 16x + 12$ |

table indicates, this approach provides extremely tight and small bounds for N_3 when the 3-rank of the associated Jacobian is large with respect to the genus.

7. CONCLUSION

Our efforts to generalize existing methods for generating quadratic number fields with high 3-rank to the hyperelliptic function field setting have proved to be quite successful. In particular, the Shanks/Weinberger, Shanks series, and Diaz y Diaz methods all routinely produce relatively low-genus function fields over \mathbb{F}_q with 3-rank as large as 5 when $q \equiv -1 \pmod{3}$, and 3-rank as large as 7 when $q \equiv 1 \pmod{3}$. The techniques of Section 5 allow us to compute the extension degree of \mathbb{F}_q such that the 3-rank of a given function field defined over \mathbb{F}_q is maximal — no equivalent technique is known in number fields.

TABLE 3. 3-ranks obtained from lifting the base field.
 Entries marked with an asterisk satisfy $N_3 = n_3$.

| q | D | g | 3-rank | 3-rank over \mathbb{F}_{q^2} | N_3 |
|-----|---|-----|--------|-----------------------------------|-------|
| 5 | $3x^{12} + 3x^{10} + 2x^6 + 3x^2 + 3$ | 5 | 2 | 3 | 24* |
| | $2x^{12} + 3x^9 + x^3 + 1$ | 5 | 3 | 5 | 18 |
| | $3x^{17} + x^{16} + 3x^{14} + 3x^{13} + 2x^{12} + 3x^{10}$ $+4x^6 + x^5 + 2x^4 + 3x^2 + x + 3$ | 8 | 4 | 8 | 168* |
| 7 | $3x^9 + 2x^6 + x^4 + 6x^2 + 2x + 4$ | 4 | 3 | 4 | 18 |
| | $3x^9 + 3x^6 + x^3 + 5$ | 4 | 4 | 5 | 6* |
| | $3x^{13} + 4x^{12} + 6x^{10} + x^9 + 2x^8 + 6x^7 + x^6$ $+4x^5 + x^4 + x^3 + x^2 + 3x$ | 6 | 5 | 5 | 84* |
| | $3x^{15} + x^{14} + 3x^{12} + 4x^{11} + x^{10} + 2x^9 + 5x^8$ $+4x^7 + 2x^6 + 6x^5 + x^4 + 4x^3 + 5x^2 + x + 4$ | 7 | 6 | 6 | 84* |
| | $3x^{21} + x^{18} + 4x^{15} + x^{12} + 5x^9 + 2x^6$ $+5x^3 + 4$ | 10 | 7 | 7 | 15* |
| 11 | $7x^6 + 5x^5 + 7x^4 + 2x^3 + 7x^2 + 5x + 10$ | 2 | 2 | 3 | 6* |
| | $7x^9 + 9x^8 + 8x^5 + 10x^4 + 10x^2 + 10x + 10$ | 4 | 3 | 6 | 8* |
| | $10x^{12} + 3x^{10} + 3x^8 + 2x^6 + 3x^4 + x^2 + 6$ | 5 | 4 | 7 | 6* |
| | $7x^{12} + 2$ | 5 | 5 | 9 | 6* |
| 13 | $9x^9 + x^5 + 3x^4 + 4x^3 + 5x^2 + 10$ | 4 | 3 | 4 | 18 |
| | $9x^9 + 11x^6 + 4x^3 + 5$ | 4 | 4 | 6 | 6* |
| | $9x^9 + 4x^6 + 3x^3 + 5$ | 4 | 5 | 7 | 6* |
| | $5x^{12} + x^9 + 11x^6 + 9x^3 + 10$ | 5 | 6 | 7 | 6* |
| | $9x^{15} + 3x^{14} + 9x^{13} + 5x^{12} + 4x^{11} + 2x^{10}$ $+9x^9 + 3x^8 + 9x^7 + x^6 + 4x^5 + 5x^4 + 12x^3$ $+2x^2 + 12x + 5$ | 7 | 7 | 7 | 84* |
| 17 | $11x^6 + 8x^5 + 10x^4 + x^3 + 11x^2 + 9x + 5$ | 2 | 2 | 3 | 6* |
| | $13x^9 + 15x^8 + 2x^7 + 15x^6 + 4x^5 + x^4 + 5x^3$ $+8x^2 + 7x + 8$ | 4 | 3 | 6 | 6* |
| | $13x^{11} + 12x^{10} + 6x^9 + 8x^8 + 10x^7 + 14x^6$ $+9x^5 + 11x^4 + 12x^3 + 11x^2 + 16x + 12$ | 5 | 4 | ≥ 5 | 18 |

One method that has proved successful in the number field case that we did not attempt to generalize is that of Belabas [4]. His method is especially well-suited for determining quadratic fields of minimal discriminant with a given 3-rank. For example, he determined that $\mathbb{Q}(\sqrt{-5393946914743})$ is the smallest such field with 3-rank 5. Generalizing this method to hyperelliptic function fields is not at all straightforward, involving the derivation of hyperelliptic function field analogues

of the Davenport-Heilbronn Theorem [9] and related theory of binary cubic forms. This is work in progress.

Another method that could be employed in the case of hyperelliptic function fields is to find hyperelliptic curves defined over \mathbb{Q} whose torsion subgroups have large 3-rank and reduce them modulo a prime p . For example, parameterized families of genus two and three curves over \mathbb{Q} whose torsion subgroups have 3-rank as high as 3 are presented in [15], so the same curves considered over \mathbb{F}_p would also have 3-rank up to 3. Although such examples would not have as high 3-rank as those produced by the Diaz y Diaz method, they would have smaller genus than any of the examples with 3-rank equal to three produced by our method, and would be especially good candidates for the constant field extension method.

Except for Section 5, we have restricted to hyperelliptic function fields of odd characteristic; the method in Section 5 applies to fields of characteristic 2 as well. As mentioned in Section 2.2, the main results on d -torsion on which the Diaz y Diaz method relies can in principle be adapted to even characteristic, but this task is non-trivial and the subject of further research. We also did not explore constructions of hyperelliptic function fields of high l -rank over characteristic l , since this would require a completely different approach that is well beyond the scope of this paper.

Other than the methods for increasing the l -rank based on enlarging the base field presented in Section 5, our algorithms deal exclusively with the problem of finding hyperelliptic function fields with high 3-rank. However, the theoretical background from which the Diaz y Diaz method is derived is presented in terms of searching for examples with high l rank for any odd prime l (see Section 2.3). It should be possible to develop explicit algorithms using these results to search for examples with high l -rank for $l > 3$. It would be useful to improve the efficiency of Algorithm 3.6, for example by reducing the set of polynomials F considered in computing $\mathcal{R}(V, T)$, in order to achieve this goal and to improve the efficiency in the case $l = 3$ as well.

Finally, we have not commented on the question of when any of the fields we constructed were escalatory or non-escalatory. Finding simple criteria under which certain parameterized families such as the Shanks and Shanks-Weinberger are escalatory or non-escalatory, or even necessary and sufficient conditions under which any hyperelliptic function field is escalatory or non-escalatory, is the subject of future work.

REFERENCES

1. J. Achter, The distribution of class groups of function fields. *J. Pure Appl. Algebra* **204** (2006), 316-333.
2. E. Artin, Quadratische Körper im Gebiete der höheren Kongruenzen. *Math. Zeitschrift* **19** (1924), 153-206.
3. M. L. Bauer, M. J. Jacobson, Jr., Y. Lee and R. Scheidler, Construction of Hyperelliptic Function Fields of High Three-Rank. *University of Calgary Yellow Series* **849**. Available at www.math.ucalgary.ca/files/publications/3443849.pdf.
4. K. Belabas, On quadratic fields with large 3-rank. *Math. Comp.* **73** (2004), 2061-2074.
5. J. Buchmann, M.J. Jacobson, Jr., and E. Teske, On some computational problems in finite abelian groups. *Math. Comp.* **66** (1997), 1663-1687.
6. H. Cohen and H. W. Lenstra, Jr., Heuristics on class groups of number fields. In *Number Theory* (Noordwijkerhout, 1983), *Lect. Notes Math.* **1068**, 33-62, Springer, Berlin, 1984.
7. M. Craig, A type of class group for imaginary quadratic fields. *Acta Arith.* **XXII** (1973), 449-459.
8. M. Craig, A Construction for irregular discriminants. *Osaka J. Math.* **14** (1977), 365-402.

9. H. Davenport and H. Heilbronn, On the density of discriminants of cubic fields (ii), *Proc. Roy. Soc. London A* **322** (1971), 405-420.
10. F. Diaz y Diaz, On some families of imaginary quadratic fields. *Math. Comp.* **32** (1978), 637-650.
11. F. Diaz y Diaz, D. Shanks and H. C. Williams, Quadratic fields with 3-rank equal to 4. *Math. Comp.* **33** (1979), 836-840.
12. G. W.-W. Fung, *Computational Problems in Complex Cubic Fields*. Doctoral Dissertation, University of Manitoba, 1990.
13. E. Friedman and L. C. Washington, On the distribution of divisor class groups of curves over a finite field. In *Théorie des Nombres* (Québec, PQ, 1987), 227-239, de Gruyter, Berlin, 1989.
14. H. Hasse, *Arithmetische Theorie der kubischen Einheiten*. *Math. Zeitschrift* **31** (1930), 565-582.
15. E. W. Howe, F. Leprévost, and B. Poonen, Large torsion subgroups of split Jacobians of curves of genus two or three, *Forum Math.* **12** (2000), 315-364.
16. T. W. Hungerford, *Algebra*. Springer-Verlag, New York 1974.
17. Y. Lee, Cohen-Lenstra heuristics and the Spiegelungssatz: function fields. *J. Number Theory* **106** (2004), 187-199.
18. Y. Lee, The Scholz theorem in function fields. *J. Number Theory* **122** (2007), 408-414.
19. Y. Lee and A. M. Pacelli, Class groups of imaginary function fields: the inert case. *Proc. Amer. Math. Soc.* **133** (2005), 2883-2889.
20. P. Llorente, Cubic fields and class fields of real quadratic fields (in Spanish). *Publ. Sec. Mat. Univ. Autònoma Barcelona* **26** (1982), 93-109.
21. P. Llorente and J. Quer, On the 3-Sylow subgroup of the class group of quadratic fields. *Math. Comp.* **50** (1988), 321-333.
22. J.-F. Mestre, Courbes elliptiques et groupes de classes d'ideaux de certain corps quadratiques. *J. Reine Angew. Math.* **343** (1983), 23-25.
23. J. S. Milne, Abelian Varieties. In *Arithmetic Geometry* (G. Cornell and J. Silverman, eds.), Springer-Verlag, New York, 1986.
24. L. J. Mordell, *Diophantine Equations*. *Pure Appl. Math. Ser.* **30**, Academic Press 1969.
25. A. M. Pacelli, Abelian subgroups of any order in class groups of global function fields. *J. Number Theory* **106** (2004), 26-49.
26. D. Glass and R. Pries, Hyperelliptic curves with prescribed p -torsion. *Manuscripta Math.* **117** (2005), 299-317.
27. 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.
28. M. Rosen, *Number Theory in Function Fields*. Springer 2002.
29. A. Scholz, Über die Beziehung der Klassenzahlen quadratischer Körper zueinander. *J. Reine Angew. Math.* **166** (1932), 201-203.
30. D. Shanks, New types of quadratic fields having three invariants divisible by 3. *J. Number Theory* **4** (1972), 537-556.
31. D. Shanks, Class groups of the quadratic fields found by F. Diaz y Diaz. *Math. Comp.* **30** (1976), 173-178.
32. D. Shanks, *Determining all cubic fields having a given fundamental discriminant*. Unpublished manuscript.
33. D. Shanks and R. Serafin, Quadratic fields with four invariants divisible by 3. *Math. Comp.* **27** (1973), 183-187.
34. D. Shanks and P. Weinberger, A quadratic field of prime discriminant requiring three generators for its class group, and related theory. *Acta Arith.* **XXI** (1972), 71-87.
35. V. Shoup, NTL: A library for doing number theory. Software, 2001. Available from <http://www.shoup.net/ntl>.
36. A. Stein and E. Teske, Explicit bounds and heuristics on class numbers in hyperelliptic function fields. *Math. Comp.* **71** (2002), 837-861.
37. A. Weil, *Variétés Abéliennes de Courbes Algébriques*. Hermann, Paris 1948.
38. Y. Yamamoto, On unramified Galois extensions of quadratic number fields. *Osaka J. Math.* **7** (1970), pp. 57-76.
39. N. Yui, On the Jacobian varieties of hyperelliptic curves over fields of characteristic $p > 2$. *J. Algebra* **52** (1978), 378-410.

40. X.-K. Zhang, Algebraic function fields of type $(2, 2, \dots, 2)$. *Sci. Sinica Ser. A* **31** (1988), 521-530.

DEPARTMENT OF MATHEMATICS AND STATISTICS, UNIVERSITY OF CALGARY, 2500 UNIVERSITY DRIVE NW, CALGARY, ALBERTA, CANADA T2N 1N4

E-mail address: mbauer@math.ucalgary.ca

DEPARTMENT OF COMPUTER SCIENCE, UNIVERSITY OF CALGARY, 2500 UNIVERSITY DRIVE NW, CALGARY, ALBERTA, CANADA T2N 1N4

E-mail address: jacobs@cpsc.ucalgary.ca

DEPARTMENT OF MATHEMATICS, SIMON FRASER UNIVERSITY, 8888 UNIVERSITY DRIVE, BURNABY, BRITISH COLUMBIA, CANADA, V5A 1S6

E-mail address: yoonjinl@sfu.ca

DEPARTMENT OF MATHEMATICS AND STATISTICS, UNIVERSITY OF CALGARY, 2500 UNIVERSITY DRIVE NW, CALGARY, ALBERTA, CANADA T2N 1N4

E-mail address: rscheidl@math.ucalgary.ca