Hyperelliptic Function Fields of High Three Rank

Renate Scheidler

Joint work with:
- Mark Bauer & Mike Jacobson, CISaC, University of Calgary
- Yoonjin Lee, Simon Fraser University

Research supported by NSERC of Canada
Motivation

Problem: Construct hyperelliptic function fields whose Jacobian/ideal class group has large 3-rank.

Relevance:

- Interesting problem in its own right
- Connection between 3-ranks of the curves $y^2 = D(x)$ and $y^2 = -3D(x)$
- Connection to cubic fields
  - Number of cubic fields of fixed discriminant
  - K. Belabas’ tables of cubic fields
  - D. Shanks’ CUFFQI Algorithm
Hyperelliptic Function Fields

- $\mathbb{F}_q$ finite field, $q$ odd
- $D(x) \in \mathbb{F}_q[x]$ squarefree with
  - $\deg(D) = 2g + 1$ odd or
  - $\deg(D) = 2g + 2$ even and $\text{sgn}(D) \notin \square_q$

$$K = \mathbb{F}_q(x, y) \text{ with } y^2 = D(x)$$

is a hyperelliptic function field of genus $g = \left\lfloor \frac{\deg(D) - 1}{2} \right\rfloor$.

- $\text{Jac}(K/\mathbb{F}_q)$ denotes the Jacobian of $K/\mathbb{F}_q$
- $\mathbb{F}_q[x, y]$ is the maximal order of $K/\mathbb{F}_q(x)$
- $\text{Cl}(K/\mathbb{F}_q(x))$ is the ideal class group of $K/\mathbb{F}_q(x)$
There is an exact sequence

\[(0) \rightarrow \text{Jac}(K/F_q) \rightarrow \text{Cl}(K/F_q(x)) \rightarrow \mathbb{Z}/f\mathbb{Z} \rightarrow (0)\]

with

\[f = \begin{cases} 
1 & \text{if } \deg(D) \text{ odd} \\
2 & \text{if } \deg(D) \text{ even and } \text{sgn}(D) \notin \mathbb{Q}_q
\end{cases}\]

So for any \(d\) odd:

\[d\text{-rank}(\text{Jac}(K/F_q)) = d\text{-rank}(\text{Cl}(K/F_q(x)))\]
Shanks-Weinberger Fields (1972): $3$-rank $\geq 1$

$$D = -3(A^4 + 4B^6) \text{ prime}$$

For function fields, use $q \equiv -1 \pmod{3}$ and $D$ need not be irreducible. We found many examples with small $q$ and small genus and $3$-rank up to $5$.

Shanks Series (1972): $3$-rank $\geq 2$

$$D_3(s) = 2s^3 - 3(3s^2 - 4s + 2)^2$$
$$D_6(t) = 4t^3 - 3(6t^2 - 4t + 1)^2 = \frac{1}{4}D_3(2t)$$

squarefree, $s \equiv -1 \pmod{6}$, $t \equiv 1 \pmod{3}$.

For function fields with $q \equiv -1 \pmod{3}$, they produce the same fields. We found many examples with small $q$ and small genus and $3$-rank up to $4$. 


Consider the equation

\[ A^3 = B^2 - C^2D \]  

in (nonzero) unknowns \( A, B, C \in \mathbb{F}_q[x] \).

\[ \text{Solutions of (*)} \iff \text{principal } \mathbb{F}_q[x, y]-\text{ideal cubes} \]

- If \( a^3 = (V + W\sqrt{D}) \) is principal, then \((uN(a), uV, uW)\) is a solution of (*) \((u \in \mathbb{F}_q^*)\)

- Let \((A, B, C)\) be a solution of (*) with \( G = \gcd(A, B) \) dividing \( D \). If

\[ a = \left( A, \frac{B + C\sqrt{D}}{G} \right), \]

then \( a^3 = (B + C\sqrt{D}) \) is primitive and principal
Craig’s Constructions (1973 & 1974)

- 1973 construction finds solutions to (*) arising from parameterized solutions
  \[ X = S^4, \ Y = S(18T^3 - S^3), \ Z = 18T^4, \ W = 3T(S^3 - 6T^3) \]
  to the Diophantine equation
  \[ X^3 + Y^3 = 2(X^3 + W^3) \]
- 1973 construction has 3-rank \( \geq 3 \)
- Reduces to 3-rank 2 in function fields (7 is not a prime but a unit!)
- Smallest Jacobian: \( q = 307, \ g = 23 \) (size 307^{23} \approx 10^{58})
- 1974 construction guarantees 3-rank 4, but produces even huger \( D (\geq 10^{101}) \)
Diaz y Diaz Construction (1978)

- searches for solutions of (*) of a specific form

- guarantees 3-rank at least 2

- if search is lucky, it guarantees 3-rank at least 3

- In 1987, Quer & Jordi found 3 Diaz y Diaz fields of 3-rank 6

- We found around 800,000 hyperelliptic function fields of 3-rank between 3 and 6
  157 of these had 3-rank 6 \((q = 7, g = 7\) and \(q = 13, g = 5\))
Consider solutions \((A, B, C)\) of (*) of the form

\[
\begin{align*}
B &= U - TV \\
UV &= 3A^2 + 3AT + T^2
\end{align*}
\]

\((T, U, V \in \mathbb{F}_q[x])\)

Then we have 3 solutions \((A_i, B_i, C), \ i = 1, 2, 3\)

\[
\begin{align*}
A_1 &= A, & B_1 &= B \\
A_2 &= A + T, & B_2 &= B + 2TV \\
A_3 &= A + \tilde{T}, & B_3 &= B + 2\tilde{T}V \quad (\tilde{T} = V^2 - 3A - T)
\end{align*}
\]

Unfortunately, the product of the 3 associated ideals is principal. However, if

- \(A_i \neq uA_j\) with \(u \in \mathbb{F}_q^*\) for all \(i, j\)
- \(\deg(A_i) \leq g = \left\lfloor \frac{\deg(D) - 1}{2} \right\rfloor\)
- \(\gcd(A_i, B_i)\) divides \(D\) \((i = 1, 2, 3)\)

then \(K = \mathbb{F}_q(x, \sqrt{D(x)})\) has 3-rank at least 2
Properties of the Diaz y Diaz Solutions

- if \( q \equiv -1 \pmod{3} \), then \( V = O^2E \) where
  - \( O \) is the product of odd degree irreducibles in \( \mathbb{F}_q[x] \)
  - \( E \) is the product of even degree irreducibles in \( \mathbb{F}_q[x] \)
  - \( O \) divides \( A \)

- \( \deg(V) \leq \frac{1}{4}(3\deg(A) - 1) \)

- if \( q \equiv -1 \pmod{3} \), then \( \deg(V) \geq \frac{\deg(A)}{2} \)

Also note that if

\[
B_F = U - TV + F(T - \tilde{T}) + F^2V \quad \text{with} \quad F \in \mathbb{F}_q[x],
\]

then \( B_F = U_F - TV \) where

\[
U_F = U + 3AF + 2TF + F^2V.
\]
Diaz y Diaz’ Algorithm (3-rank 2)

- Pick any $A \in \mathbb{F}_q[x]$
- Search for suitable $V \in \mathbb{F}_q[x]$
- For each suitable $V$ do
  - Find $T$ with $3A^2 + 3AT + T^2 \equiv 0 \pmod{V}$
  - Set $U = \frac{3A^2 + 3AT + T^2}{V}$
  - For each such $T$, find all $F$ with
    - $B_F \neq A^3$ and $\deg(B_F^2) \leq \deg(A^3)$ where
      $B_F = U - TV + F(2T + 3A - V^2) + F^2V$
    - the squarefree part $D_F$ of $A^3 - B_F^2$ has odd degree or even degree and non-square leading coefficient
    - The 3 Diaz y Diaz solutions derived from $A$ and $B_F$ satisfy the Diaz y Diaz conditions
- Output all such $D_F$

Each field $\mathbb{K}_F = \mathbb{F}_q\left(x, \sqrt{D_F(x)}\right)$ has 3-rank at least 2
Example

\(q = 5 \equiv -1 \pmod{3}, \ A = x^4 + x = (x)(x+1)(x^2+4x+1) \in \mathbb{F}_5[x]\)

\[\text{deg}(A) = 4 \implies \text{deg}(V) \leq 2 \implies \text{deg}(T) \leq 1\]

Permissible \(V\) values: \(x^2\) and \((x + 1)^2 = x^2 + 2x + 1\)

For \(V = x^2\), a solution to \(3A^2 + 3AT + T^2 \equiv 0 \pmod{V}\) is \(T = 3x\)

Then

\[U = (3A^2 + 3AT + T^2)/V = 3x^6 + 1\]
\[\tilde{T} = V^2 - 3A - T = 3x^4 + 4x\]
\[|\mathcal{R}(V, T)| = 42\]

For each of the 42 polynomials \(F \in \mathcal{R}(V, T)\), the corresponding \(D_F\) yields a hyperelliptic function field of 3-rank at least 2
Example (cont’d)

One permissible \( F \in \mathcal{R}(V,T) \) is \( F = 2x^2 \), yielding

\[
\begin{align*}
B_F &= U - TV + F(T - \tilde{T}) + F^2V = x^6 + 1 \\
D_F &= B_F^2 - 4A^3 = 2x^{12} + 3x^9 + x^3 + 1
\end{align*}
\]

The three Diaz y Diaz solutions

\[
\begin{align*}
(A_1, B_1) &= (A, B_F) = (x^4 + x, x^6 + 1) \\
(A_2, B_2) &= (A + T, B_F + 2TV) = (3x^4 + 4x, x^3 + 1) \\
(A_3, B_3) &= (A + \tilde{T}, B_F + 2\tilde{T}V) = (2x^4, 3x^6 + 3x^3 + 1)
\end{align*}
\]

all satisfy the Diaz y Diaz conditions

\( D_F \) squarefree \( \Rightarrow \) \( C = 1 \)

\( \mathbb{K} = \mathbb{F}_5(x, \sqrt{D_F}) \) has 3-rank at least 2
Diaz y Diaz’ Algorithm (3-rank 3)

If at least 2 pairs \((V, T)\) are found in the previous algorithm:

for all \((V, T')\) do
  for all \((\hat{V}, \hat{T}) \neq (V, T)\) do
    for all \(F\) belonging to \((V, T)\) do
      for all \(\hat{F}\) belonging to \((\hat{V}, \hat{T})\) do
        if \(B_F = \pm \hat{B}_{\hat{F}}\) and none of \(A_1, A_2, A_3, \hat{A}_2, \hat{A}_3\) differ by a constant factor
          output \(D_F\)

Each field \(K_F = \mathbb{F}_q \left( x, \sqrt{D_F(x)} \right)\) has 3-rank at least 3
$q = 5, \quad A = x^4 + x.$

Each of the two valid $V$ values $x^2$ and $(x + 1)^2$ has 5 permissible $T$, and $\mathcal{R}(V, T) \neq \emptyset$ for each $(V, T)$ pair. So we check 10 $(V, T)$ pairs. We find for example:

$$(V, T) = (x^2, 3x), \quad F = 2x^2 \in \mathcal{R}(V, T)$$
$$(\hat{V}, \hat{T}) = (x^2 + 2x + 1, 4x + 4), \quad \hat{F} = 2x^2 + x + 4 \in \mathcal{R}(\hat{V}, \hat{T})$$

and $B_F = B_{\hat{F}} = x^6 + 1$. Then

$$A_1 = x^4 + x$$
$$A_2 = 3x^4 + 4x, \quad \hat{A}_2 = 3x^4 + 3x^2 + 4x + 3$$
$$A_3 = 2x^4 \quad \hat{A}_3 = 2x^4 + 4x^3 + 3x^2 + 4x + 3$$

None of these differ by a constant factor, so $K = \mathbb{F}_5(x, \sqrt{D_F})$ with $D_F = 2x^{12} + 3x^9 + x^3 + 1$ has 3-rank at least 3.

In fact, $Cl(K/\mathbb{F}_q(x)) \cong \mathbb{Z}/900\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$
Increasing the Field of Constants

For \( n \in \mathbb{N} \), set \( K_n = \mathbb{KF}_{q^n} = \mathbb{F}_{q^n}(x, \sqrt{D(x)}) \)

Questions (and some answers):

**Question:** What is the maximal 3-rank of any \( K_n \)?

**Answer:** \( 2g \).

For any \( d \in \mathbb{N} \) with \( \gcd(q, n) = 1 \), the \( d \)-torsion of \( Jac(KF_q/F_q) \) satisfies

\[
Jac(KF_q/F_q)[d] \cong (\mathbb{Z}/d\mathbb{Z})^{2g}
\]

But there exists a minimal finite extension \( \mathbb{F}_{q^{n(d)}} \) with

\[
Jac(K_{n(d)}/\mathbb{F}_{q^{n(d)}})[d] \cong (\mathbb{Z}/d\mathbb{Z})^{2g}
\]
Question: What is (an upper bound on) $n = n(d)$?

Answer: Galois representation

$$\rho_d : \text{Gal}(\mathbb{F}_{q^{n(d)}}/\mathbb{F}_q) \hookrightarrow \text{Gl}_2(\mathbb{Z}/d\mathbb{Z})$$

Frobenius $\pi_{q,d} \mapsto M_d$

So $n(d) = \text{ord}(M_d)$

Note that $n(d)$ is invariant under conjugation in $\text{Gl}_2(\mathbb{Z}/d\mathbb{Z})$

To find $n(d)$, use the primary rational canonical form of $M_d$

Henceforth assume $d = l$ prime
Companion Matrices

If

\[ f(t) = t^r + a_{r-1}t^{r-1} + \cdots + a_0 \]

is a monic polynomial, then the *companion matrix* of \( f(t) \) is

\[
M_f = \begin{pmatrix}
0 & 1 & 0 & 0 & \cdots & 0 \\
0 & 0 & 1 & 0 & \cdots & 0 \\
0 & 0 & 0 & 1 & \cdots & 0 \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & 0 & \cdots & 1 \\
-a_0 & -a_1 & -a_2 & -a_3 & \cdots & -a_{r-1}
\end{pmatrix}
\]
Primary Rational Canonical Form

Let

\[ P_1^{m_1}P_2^{m_2} \cdots P_s^{m_s} \]

be the prime factorization of the minimal polynomial of \( M_l \) over the field \( \mathbb{F}_l \).

The primary rational canonical form of \( M_l \) is

\[
\begin{pmatrix}
M_{11} & M_{12} & \cdots & 0 \\
0 & M_{12} & \cdots & 0 \\
0 & 0 & \cdots & M_{sk_s}
\end{pmatrix}
\]

where \( M_{ij} \) is the companion matrix of \( P_i^{m_{ij}} \) and \( m_{ij} \leq m_i \) for \( 1 \leq i \leq s \) and \( 1 \leq j \leq k_i \).
To find the primary rational canonical form of $M_l$, we need to find the minimal polynomial of $M_l$.

The *Frobenius polynomial* is the characteristic polynomial $F(t) \in \mathbb{F}_l(t)$ of $M_l$. We have

$$F(t) \equiv t^{2g}L(t^{-1}) \pmod{l}$$

where $L(t)$ is the $L$-polynomial of $\mathbb{K}/\mathbb{F}_q$:

$$\zeta(s) = \sum_{\mathfrak{d} \in \text{Div}(\mathbb{K}/\mathbb{F}_q)} t^{\deg(\mathfrak{d})} = \frac{L(t)}{(1-t)(1-qt)} \quad (t = q^{-s})$$

This uniquely determines $F(t)$.

$F(t)$ is a multiple of the the minimal polynomial of $M_l$, and is equal to it if $F(t)$ is squarefree.
Algorithm for Finding (a Bound on) \( n(l) \)

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 \( F = Q_1^{e_1}Q_2^{e_2} \cdots Q_u^{e_u} \).
4. For each combination of \( e_{ij} \) with \( e_{ij} \leq e_i \) and \( \sum_{ij} e_{ij} \deg(Q_i) = 2g \), compute the companion matrices \( M_{ij} \) of \( Q_i^{e_{ij}} \) and set

\[
M = \begin{pmatrix}
M_{11} & M_{12} & \cdots & 0 \\
0 & \cdots & \cdots & 0 \\
& & \cdots & M_{sk_s}
\end{pmatrix}
\]

5. Set \( b = \max \{ \text{ord}(M) \mid M \text{ computed in step 4} \} \).
6. If \( e_i = 1 \) for \( 1 \leq i \leq u \), output \( n(l) = b \), else indicate that it is impossible to find \( n(l) \) and output the upper bound \( b \) on \( n(l) \).
Example

Let \( q = 373 \) and consider the genus 4 field defined by

\[
y^2 = x^9 + 245x^8 + 175x^7 + 340x^6 + 122x^5 + 70x^4 \\
    + 196x^3 + 210x^2 + 316x + 337
\]

Using Magma: \( \zeta(t) = L(t)/(373t^2 - 374t + 1) \) with

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

The Frobenius polynomial over \( \mathbb{F}_3 \) is irreducible:

\[
F(t) = t^8 + 2t^6 + t^5 + t^3 + 2t^2 + 1.
\]

\[
\text{ord}(M_3) = 41 \Rightarrow \begin{cases} 
3\text{-rank 0 over all } \mathbb{F}_{373^n} \text{ with } n < 41 \\
3\text{-rank } 2 \cdot 4 = 8 \text{ over } \mathbb{F}_{373^{41}}
\end{cases}
\]

Best possible scenario for this method
How Much is Enough?

More Questions:

- Find $n$ so that the 3-rank of $K_n$ is guaranteed to exceed the 3-rank of $K$.
- By how much does the 3-rank of $K_n$ exceed the 3-rank of $K$?

Partial Answer:

Suppose there exists $P(t) \in \mathbb{F}_l[t]$ with

- $P(t)$ is nonlinear and irreducible
- $P(t)$ divides $F(t)$, but $P^2(t)$ does not divide $F(t)$

Let $M_P$ be the companion matrix of $P(t)$ and $n = \text{ord}(M_P)$. Then

\[
l\text{-rank}(K_n) \geq l\text{-rank}(K) + \deg(P)\]
Combining the Methods

Suppose $\mathbb{K}/\mathbb{F}_q$ has $l$-rank at least $r > 0$, e.g. $l = 3$ and $\mathbb{K}$ was obtained by the Shanks, Shanks-Weinberger, Craig, or Diaz y Diaz method. Then

$$\text{Jac}(\mathbb{K}/\mathbb{F}_q) \cong (\mathbb{Z}/l\mathbb{Z})^r \times \mathcal{H}$$

so

$$F(t) = (t - 1)^r G(t)$$

Remove a factor of $(t - 1)^r$ from $F(t)$ before doing the search on candidates for the primary rational canonical form, i.e. search on $G(t)$.

In fact:

$$(t - 1)^r \mid F(t) \Rightarrow 3\text{-rank}(\mathbb{K}) = r$$

$$(t - 1)^{r+1} \mid F(t) \Rightarrow 3\text{-rank}(\mathbb{K}) = r + 1$$
Let $q = 179$ and consider the genus 4 field defined by
\[ y^2 = x^9 + 151 x^8 + 168 x^7 + 10 x^6 + 32 x^5 + 141 x^4 + 110 x^3 + 35 x^2 + 160 x + 2 \]

Using Magma: $\zeta(t) = L(t)/(179 t^2 - 180 t + 1)$ with
\[
L(t) = 179^4 t^8 - 17 \cdot 179^3 t^7 + 315 \cdot 179^2 t^6 - 3041 \cdot 179 t^5 - 56275 t^4 - 3041 t^3 + 315 t^2 - 17 t + 1
\]
The Frobenius polynomial over $\mathbb{F}_3$ is
\[
F(t) = t^8 + t^7 + t^5 + t^4 + 2 t^3 + 2 t + 1 = (t + 1)(t + 2)(t^2 + 1)^2(t^2 + t + 2)
\]
The order of the corresponding companion matrices are 2, 1, 4 or 12, and 8, respectively. So our algorithm produces an upper bound of 24.

Hence, over $\left\{ \mathbb{F}_{179}, \mathbb{F}_{179^{24}} \right\}$, we have 3-rank $\left\{ \geq 1, 8 \right\}$
**Example (cont’d)**

Order of companion matrix \[
\begin{pmatrix}
M_{t+1} \\
M_{t+2} \\
M_{t^2+t+2}
\end{pmatrix}
\] is \[
\begin{pmatrix}
2 \\
1 \\
8
\end{pmatrix}
\]

The \( t + 1 \) term implies 3-rank \( \geq 2 \) over \( \mathbb{F}_{179^2} \)

The squares of all the remaining possible companion matrices do not have 1 as an eigenvalue, so (3-rank over \( \mathbb{F}_{179^2} \)) \( = 2 \).

The \( t^2 + t + 2 \) term implies (3-rank over \( \mathbb{F}_{179^8} \)) \( \geq 3 \). However, (3-rank over \( \mathbb{F}_{179^2} \)) \( = 2 \) \& \( \mathbb{F}_{179^2} \leq \mathbb{F}_{179^8} \) \( \Rightarrow \) (3-rank over \( \mathbb{F}_{179^8} \)) \( \geq 4 \)

In fact, \( M_{t^2+t+2}^4 \) has eigenvalue 1, and the corresponding eigenspace has dimension 2. So

- (3-rank over \( \mathbb{F}_{179^4} \)) \( \geq \) (3-rank over any subfield) \( + 2 \)
- (3-rank over \( \mathbb{F}_{179^8} \)) \( \geq 6 \)
Conclusions

• We have a number of methods for constructing hyperelliptic function fields of high 3-rank
• Some of these derive from number fields, while the method of increasing the field of constants is unique to function fields
• The methods can be combined to work very well

Further Work

• Constructions for $l > 3$ prime
• Constructions for any $n$
• . . .