Class numbers of algebraic function fields, or Jacobians of curves over finite fields

Anastassia Etropolski

January 9, 2016
Class Numbers of Number Fields

- $K$ a number field
Class Numbers of Number Fields

- $K$ a number field
- $\mathcal{O}_K$ the ring of integers of $K$
Class Numbers of Number Fields

- $K$ a number field
- $\mathcal{O}_K$ the ring of integers of $K$
- $\text{Cl}(K) = \text{Cl}(\mathcal{O}_K)$ the class group of $K$
Class Numbers of Number Fields

- $K$ a number field
- $\mathcal{O}_K$ the ring of integers of $K$
- $\text{Cl}(K) = \text{Cl}(\mathcal{O}_K)$ the class group of $K$
- $h_K = \# \text{Cl}(K)$ the class number of $K$
Class Numbers of Number Fields

- $K$ a number field
- $\mathcal{O}_K$ the ring of integers of $K$
- $\text{Cl}(K) = \text{Cl}(\mathcal{O}_K)$ the class group of $K$
- $h_K = \# \text{Cl}(K)$ the class number of $K$

**Theorem (Gauss’s Conjecture)**

Given a positive integer $h$, there are only finitely many **imaginary quadratic fields** with class number $h$. 

Class Numbers of Number Fields

- $K$ a number field
- $\mathcal{O}_K$ the ring of integers of $K$
- $\text{Cl}(K) = \text{Cl}(\mathcal{O}_K)$ the class group of $K$
- $h_K = \# \text{Cl}(K)$ the class number of $K$

**Theorem (Gauss’s Conjecture)**

Given a positive integer $h$, there are only finitely many **imaginary quadratic fields** with class number $h$.

Proven by Hecke (1916) and Heilbronn (1934).
Class Numbers of Number Fields

- \( K \) a number field
- \( \mathcal{O}_K \) the ring of integers of \( K \)
- \( \text{Cl}(K) = \text{Cl}(\mathcal{O}_K) \) the class group of \( K \)
- \( h_K = \# \text{Cl}(K) \) the class number of \( K \)

**Theorem (Gauss’s Conjecture)**

Given a positive integer \( h \), there are only finitely many **imaginary quadratic fields** with class number \( h \).

Proven by Hecke (1916) and Heilbronn (1934).

It is still an open problem to show that there are **infinitely many** real quadratic fields with class number 1, as we expect.
Problem (Gauss Class Number Problem)

Enumerate all imaginary quadratic fields with class number $h$. 

Remark: These results rely on extremely deep mathematics, including state of the art results about modularity and low-lying zeros of $L$-functions.
Problem (Gauss Class Number Problem)

Enumerate all imaginary quadratic fields with class number $h$.

$h = 1$ \quad \text{Heegner (1952) + Stark (1967), Baker (1966)}$
Problem (Gauss Class Number Problem)

Enumerate all imaginary quadratic fields with class number $h$.

\begin{align*}
  h = 1 & \quad \text{Heegner (1952) + Stark (1967), Baker (1966)} \\
  h = 2 & \quad \text{Baker (1971) + Stark (1971)}
\end{align*}
Problem (Gauss Class Number Problem)

Enumerate all imaginary quadratic fields with class number $h$.

- $h = 1$ Heegner (1952) + Stark (1967), Baker (1966)
- $h = 3$ Oesterlé (1984)
Problem (Gauss Class Number Problem)

Enumerate all imaginary quadratic fields with class number $h$.

$h = 1$  Heegner (1952) + Stark (1967), Baker (1966)
$h = 3$  Oesterlé (1984)
$h = 4$  Arno (1992)

Remark: These results rely on extremely deep mathematics, including state of the art results about modularity and low-lying zeros of $L$-functions.
### Problem (Gauss Class Number Problem)

Enumerate all imaginary quadratic fields with class number $h$.

<table>
<thead>
<tr>
<th>$h$</th>
<th>Authors</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Heegner (1952) + Stark (1967), Baker (1966)</td>
</tr>
<tr>
<td>3</td>
<td>Oesterlé (1984)</td>
</tr>
<tr>
<td>4</td>
<td>Arno (1992)</td>
</tr>
<tr>
<td>5, 6, 7</td>
<td>Wagner (1996)</td>
</tr>
</tbody>
</table>
Imaginary Quadratic Fields

Problem (Gauss Class Number Problem)

Enumerate all imaginary quadratic fields with class number $h$.

- $h = 1$: Heegner (1952) + Stark (1967), Baker (1966)
- $h = 4$: Arno (1992)
- $h = 5, 6, 7$: Wagner (1996)
- $h \leq 100$: Watkins (2004) + 7 months of computation

Remark: These results rely on extremely deep mathematics, including state of the art results about modularity and low-lying zeros of $L$-functions.
Problem (Gauss Class Number Problem)

Enumerate all imaginary quadratic fields with class number $h$.

<table>
<thead>
<tr>
<th>$h$</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Heegner (1952) + Stark (1967), Baker (1966)</td>
</tr>
<tr>
<td>3</td>
<td>Oesterlé (1984)</td>
</tr>
<tr>
<td>4</td>
<td>Arno (1992)</td>
</tr>
<tr>
<td>5, 6, 7</td>
<td>Wagner (1996)</td>
</tr>
<tr>
<td>$h \leq 100$</td>
<td>Watkins (2004) + 7 months of computation</td>
</tr>
</tbody>
</table>

Remark: These results rely on extremely deep mathematics, including state of the art results about modularity and low-lying zeros of $L$-functions.
Problem (Gauss Class Number Problem)

Enumerate all imaginary quadratic fields with class number $h$.

$h = 1$  Heegner (1952) + Stark (1967), Baker (1966)
$h = 3$  Oesterlé (1984)
$h = 4$  Arno (1992)
$h = 5, 6, 7$  Wagner (1996)
$h \leq 100$  Watkins (2004) + 7 months of computation

**Remark:** These results rely on extremely deep mathematics, including state of the art results about modularity and low-lying zeros of $L$-functions.
The Analogy

In the analogy between number fields and function fields, the role of $K$ is played by the function field $\mathbb{F}_q(C)$ of a smooth curve $C$ over a finite field $\mathbb{F}_q$. 
In the analogy between number fields and function fields, the role of $K$ is played by the function field $\mathbb{F}_q(C)$ of a smooth curve $C$ over a finite field $\mathbb{F}_q$.

prime ideals $\leftrightarrow$ closed points of $C$ over $\mathbb{F}_q$
In the analogy between number fields and function fields, the role of $K$ is played by the function field $\mathbb{F}_q(C)$ of a smooth curve $C$ over a finite field $\mathbb{F}_q$.

- prime ideals $\leftrightarrow$ closed points of $C$ over $\mathbb{F}_q$
- fractional ideals $\leftrightarrow$ linear combinations of points, i.e. divisors

Question

"How many" algebraic function fields are there with a fixed class number $h$?
The Analogy

In the analogy between number fields and function fields, the role of $K$ is played by the function field $F_q(C)$ of a smooth curve $C$ over a finite field $F_q$.

- prime ideals $\leftrightarrow$ closed points of $C$ over $F_q$
- fractional ideals $\leftrightarrow$ linear combinations of points, i.e. divisors
- principal ideals $\leftrightarrow$ principal divisors
In the analogy between number fields and function fields, the role of $K$ is played by the function field $\mathbf{F}_q(C)$ of a smooth curve $C$ over a finite field $\mathbf{F}_q$.

- prime ideals $\leftrightarrow$ closed points of $C$ over $\mathbf{F}_q$
- fractional ideals $\leftrightarrow$ linear combinations of points, i.e. divisors
- principal ideals $\leftrightarrow$ principal divisors
- $\text{Cl}(K) \leftrightarrow \text{Div/Prin},$ i.e. $\text{Jac}(C)$
In the analogy between number fields and function fields, the role of $K$ is played by the function field $\mathbb{F}_q(C)$ of a smooth curve $C$ over a finite field $\mathbb{F}_q$.

| prime ideals | ↔ | closed points of $C$ over $\mathbb{F}_q$ |
| fractional ideals | ↔ | linear combinations of points, i.e. divisors |
| principal ideals | ↔ | principal divisors |
| $\text{Cl}(K)$ | ↔ | $\text{Div/Prin}$, i.e. $\text{Jac}(C)$ |
| $h_K$ | ↔ | $\# \text{Jac}(C)$ |
The Analogy

In the analogy between number fields and function fields, the role of $K$ is played by the function field $\mathbb{F}_q(C)$ of a smooth curve $C$ over a finite field $\mathbb{F}_q$.

| prime ideals   | $\leftrightarrow$ | closed points of $C$ over $\mathbb{F}_q$ |
| fractional ideals | $\leftrightarrow$ | linear combinations of points, i.e. divisors |
| principal ideals | $\leftrightarrow$ | principal divisors |
| $\text{Cl}(K)$   | $\leftrightarrow$ | $\text{Div/Prin}$, i.e. $\text{Jac}(C)$ |
| $h_K$            | $\leftrightarrow$ | $\# \text{Jac}(C)$ |

**Question**

“How many” algebraic function fields are there with a fixed class number $h$?
A pleasant surprise

Let $C$ be a smooth curve over $\mathbb{F}_q$ of genus $g$. 
A pleasant surprise

Let $C$ be a smooth curve over $\mathbb{F}_q$ of genus $g$.

- Throughout we assume that $g > 0$. 

By the Weil Conjectures:

\[
(1 - q^{1/2})^2 \leq h \leq (1 + q^{1/2})^2,
\]

so if $g \geq 1$, we have $(1 - q^{1/2})^2 \leq h$, and we get an upper bound on $q$ depending only on $h$.

For example: If $h = 1$, then $q \leq 4$.

Riemann-Roch gives an explicit upper bound on $g$ in terms of $h$ and $q$.

For example: If $h = 1$, then $q = 4$ and $g \leq 1$, or $q = 3$ and $g \leq 2$, or $q = 2$ and $g \leq 4$.

So there are only finitely many algebraic function fields with a given class number!
A pleasant surprise

Let $C$ be a smooth curve over $\mathbb{F}_q$ of genus $g$.

- Throughout we assume that $g > 0$.
- By the Weil Conjectures:

$$(1 - q^{1/2})^{2g} \leq h \leq (1 + q^{1/2})^{2g},$$

so if $g \geq 1$, we have $(1 - q^{1/2})^2 \leq h$, and we get an upper bound on $q$ depending only on $h$. 

A pleasant surprise

Let $C$ be a smooth curve over $\mathbb{F}_q$ of genus $g$.

- Throughout we assume that $g > 0$.
- By the Weil Conjectures:

$$ (1 - q^{1/2})^{2g} \leq h \leq (1 + q^{1/2})^{2g}, $$

so if $g \geq 1$, we have $(1 - q^{1/2})^2 \leq h$, and we get an upper bound on $q$ depending only on $h$.

For example: If $h = 1$, then $q \leq 4$. 

A pleasant surprise

Let $C$ be a smooth curve over $\mathbb{F}_q$ of genus $g$.

- Throughout we assume that $g > 0$.
- By the Weil Conjectures:

\[
(1 - q^{1/2})^{2g} \leq h \leq (1 + q^{1/2})^{2g},
\]

so if $g \geq 1$, we have $(1 - q^{1/2})^2 \leq h$, and we get an upper bound on $q$ depending only on $h$.

For example: If $h = 1$, then $q \leq 4$.

- Riemann-Roch gives an explicit upper bound on $g$ in terms of $h$ and $q$. 
A pleasant surprise

Let $C$ be a smooth curve over $\mathbb{F}_q$ of genus $g$.

- Throughout we assume that $g > 0$.
- By the Weil Conjectures:

$$(1 - q^{1/2})^{2g} \leq h \leq (1 + q^{1/2})^{2g},$$

so if $g \geq 1$, we have $(1 - q^{1/2})^2 \leq h$, and we get an upper bound on $q$ depending only on $h$.

For example: If $h = 1$, then $q \leq 4$.

- Riemann-Roch gives an explicit upper bound on $g$ in terms of $h$ and $q$.

For example: If $h = 1$, then $q = 4$ and $g \leq 1$, or $q = 3$ and $g \leq 2$, or $q = 2$ and $g \leq 4$. 
A pleasant surprise

Let $C$ be a smooth curve over $\mathbf{F}_q$ of genus $g$.

- Throughout we assume that $g > 0$.
- By the Weil Conjectures:

$$
(1 - q^{1/2})^{2g} \leq h \leq (1 + q^{1/2})^{2g},
$$

so if $g \geq 1$, we have $(1 - q^{1/2})^2 \leq h$, and we get an upper bound on $q$ depending only on $h$.

For example: If $h = 1$, then $q \leq 4$.

- Riemann-Roch gives an explicit upper bound on $g$ in terms of $h$ and $q$.

For example: If $h = 1$, then $q = 4$ and $g \leq 1$, or $q = 3$ and $g \leq 2$, or $q = 2$ and $g \leq 4$.

So there are only finitely many algebraic function fields with a given class number!
The Class Number One Problem

**Theorem (Leitzel-Madan-Queen (1975))**

Up to isomorphism, there are seven algebraic function fields with class number 1. They are the fields $F/F_q$, where $F = F_q(x, y)/f(x, y)$ as given below.

<table>
<thead>
<tr>
<th>$q$</th>
<th>$g$</th>
<th>$f(x, y)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1</td>
<td>$y^2 + y + x^3 + x + 1$</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>$y^2 + y + x^5 + x^3 + 1$</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>$y^2 + y + (x^3 + x^2 + 1)(x^3 + x + 1)^{-1}$</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>$y^4 + xy^3 + (x^2 + x)y^2 + (x^3 + 1)y + x^4 + x + 1$</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>$y^4 + (x^2 + x + 1)y + (x^4 + x + 1)$</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>$y^2 + 2x^3 + x + 1$</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>$y^2 + y - x^3 + \eta$, where $F_4^\times = \langle \eta \rangle$</td>
</tr>
</tbody>
</table>
The Class Number One Problem

**Theorem (L-M-Q (1975), Mercuri-Stirpe, Shen-Shi (2014))**

Up to isomorphism, there are eight algebraic function fields with class number 1. They are the fields $F/F_q$, where $F = F_q(x, y)/f(x, y)$ as given below.

<table>
<thead>
<tr>
<th>$q$</th>
<th>$g$</th>
<th>$f(x, y)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1</td>
<td>$y^2 + y + x^3 + x + 1$</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>$y^2 + y + x^5 + x^3 + 1$</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>$y^2 + y + (x^3 + x^2 + 1)(x^3 + x + 1)^{-1}$</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>$y^4 + xy^3 + (x^2 + x)y^2 + (x^3 + 1)y + x^4 + x + 1$</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>$y^4 + (x^2 + x + 1)y + (x^4 + x + 1)$</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>$y^2 + 2x^3 + x + 1$</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>$y^2 + y - x^3 + \eta$, where $F_4^\times = \langle \eta \rangle$</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>$y^5 + y^3 + y^2(x^3 + x^2 + 1) + y(x^7 + x^5 + x^4 + x^3 + x)/(x^4 + x + 1)$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$+(x^{13} + x^{12} + x^8 + x^6 + x^2 + x + 1)/(x^4 + x + 1)^2$</td>
</tr>
</tbody>
</table>
Class Number 2 and 3

- 1975: Leitzel-Madan-Queen classify imaginary quadratic function fields whose integral closure has $h = 2$. 
Class Number 2 and 3

- 1975: Leitzel-Madan-Queen classify imaginary quadratic function fields whose integral closure has $h = 2$.
- 1991: Le Brigand gives a complete classification of quadratic function fields with $h = 2$. 
Class Number 2 and 3

- 1975: Leitzel-Madan-Queen classify imaginary quadratic function fields whose integral closure has $h = 2$.
- 1991: Le Brigand gives a complete classification of quadratic function fields with $h = 2$.
- 1995: Le Brigand completes the full $h = 2$ classification.
Class Number 2 and 3

- 1975: Leitzel-Madan-Queen classify imaginary quadratic function fields whose integral closure has $h = 2$.
- 1991: Le Brigand gives a complete classification of quadratic function fields with $h = 2$.
- 1995: Le Brigand completes the full $h = 2$ classification.
- 2011: Picone classifies the quadratic function fields with $h = 3$ and shows that if $q > 2$, there are no non-quadratic ones.
Resolving the Class Number 3 Case

Theorem (E.)

Up to isomorphism, there are 13 non-quadratic algebraic function fields over $\mathbb{F}_2$ with class number 3. More precisely, four of them have genus 3 and nine have genus 4.
Theorem (E.)

Up to isomorphism, there are 13 non-quadratic algebraic function fields over $\mathbb{F}_2$ with class number 3. More precisely, four of them have genus 3 and nine have genus 4.

Together with Picone’s result, this gives a complete classification.
Resolution of the Class Number 3 Case

Theorem (E.)

Up to isomorphism, there are 13 non-quadratic algebraic function fields over $\mathbb{F}_2$ with class number 3. More precisely, four of them have genus 3 and nine have genus 4.

Together with Picone’s result, this gives a complete classification.

Theorem (E. (2016), Picone (2011))

Up to isomorphism, there are exactly 27 algebraic function fields with class number 3.
L-polynomials and the Weil Conjectures

Let $C$ be a smooth curve over $\mathbb{F}_q$. 
L-polynomials and the Weil Conjectures

Let $C$ be a smooth curve over $\mathbb{F}_q$.

- Let $A_n := \#\{\text{effective degree } n \text{ divisors on } C\}$. 
L-polynomials and the Weil Conjectures

Let $C$ be a smooth curve over $\mathbb{F}_q$.
- Let $A_n := \#\{\text{effective degree } n \text{ divisors on } C\}$.
- The Zeta-function of $C$ is $Z(t) := \sum_{n \geq 0} A_n t^n$. 
L-polynomials and the Weil Conjectures

Let $C$ be a smooth curve over $\mathbb{F}_q$.

- Let $A_n := \#\{\text{effective degree } n \text{ divisors on } C\}$.
- The Zeta-function of $C$ is $Z(t) := \sum_{n \geq 0} A_n t^n$.
- $L(t) = (1 - t)(1 - qt)Z(t)$ is a degree $2g$ polynomial over $\mathbb{Z}$. 
L-polynomials and the Weil Conjectures

Let $C$ be a smooth curve over $\mathbf{F}_q$.

- Let $A_n := \#\{\text{effective degree } n \text{ divisors on } C\}$.
- The Zeta-function of $C$ is $Z(t) := \sum_{n\geq 0} A_n t^n$.
- $L(t) = (1 - t)(1 - qt)Z(t)$ is a degree $2g$ polynomial over $\mathbf{Z}$.
- It turns out that $L(1) = h$.
L-polynomials and the Weil Conjectures

Let $C$ be a smooth curve over $\mathbb{F}_q$.

- Let $A_n := \#\{\text{effective degree } n \text{ divisors on } C\}$.
- The Zeta-function of $C$ is $Z(t) := \sum_{n \geq 0} A_n t^n$.
- $L(t) = (1 - t)(1 - qt)Z(t)$ is a degree $2g$ polynomial over $\mathbb{Z}$.
- It turns out that $L(1) = h$.
- Write $L(t) = a_0 + a_1 t + \cdots + a_{2g} t^{2g} = \prod_{i=1}^{2g} (1 - \alpha_i t)$. Then
  
  1. $a_0 = 1$
Let $C$ be a smooth curve over $\mathbb{F}_q$.

- Let $A_n := \#\{\text{effective degree } n \text{ divisors on } C\}$.
- The Zeta-function of $C$ is $Z(t) := \sum_{n \geq 0} A_n t^n$.
- $L(t) = (1 - t)(1 - qt)Z(t)$ is a degree $2g$ polynomial over $\mathbb{Z}$.
- It turns out that $L(1) = h$.
- Write $L(t) = a_0 + a_1 t + \cdots + a_{2g} t^{2g} = \prod_{i=1}^{2g} (1 - \alpha_i t)$. Then
  1. $a_0 = 1$
  2. $a_{2g-i} = q^{g-i} a_i$ for $0 \leq i \leq g$
L-polynomials and the Weil Conjectures

Let $C$ be a smooth curve over $\mathbb{F}_q$.

- Let $A_n := \#\{\text{effective degree } n \text{ divisors on } C\}$.
- The Zeta-function of $C$ is $Z(t) := \sum_{n \geq 0} A_n t^n$.
- $L(t) = (1 - t)(1 - qt)Z(t)$ is a degree $2g$ polynomial over $\mathbb{Z}$.
- It turns out that $L(1) = h$.
- Write $L(t) = a_0 + a_1 t + \cdots + a_{2g} t^{2g} = \prod_{i=1}^{2g} (1 - \alpha_i t)$. Then
  
  1. $a_0 = 1$
  2. $a_{2g-i} = q^{g-i} a_i$ for $0 \leq i \leq g$
  3. $|\alpha_i| = \sqrt{q}$, and up to relabeling, $\alpha_i \alpha_{g+i} = q$
L-polynomials and the Weil Conjectures

Let $C$ be a smooth curve over $\mathbb{F}_q$.

- Let $A_n := \#\{\text{effective degree } n \text{ divisors on } C\}$.
- The Zeta-function of $C$ is $Z(t) := \sum_{n \geq 0} A_n t^n$.
- $L(t) = (1 - t)(1 - qt)Z(t)$ is a degree $2g$ polynomial over $\mathbb{Z}$.
- It turns out that $L(1) = h$.
- Write $L(t) = a_0 + a_1 t + \cdots + a_{2g} t^{2g} = \prod_{i=1}^{2g} (1 - \alpha_i t)$. Then
  1. $a_0 = 1$
  2. $a_{2g-i} = q^{g-i} a_i$ for $0 \leq i \leq g$
  3. $|\alpha_i| = \sqrt{q}$, and up to relabeling, $\alpha_i \alpha_{g+i} = q$

- Hasse-Weil Bound: $|\#C(\mathbb{F}_{q^r}) - (q^r + 1)| \leq 2gq^{r/2}$
Introducing a new set of parameters

- Define $n_r := \#\{\text{closed points of degree } n \text{ on } C\}$. 
Introducing a new set of parameters

- Define $n_r := \# \{\text{closed points of degree } n \text{ on } C\}$.
- We can rewrite $L(t)$ in terms of $n_r$, $1 \leq r \leq g$. 
Introducing a new set of parameters

- Define $n_r := \# \{\text{closed points of degree } n \text{ on } C\}$.
- We can rewrite $L(t)$ in terms of $n_r$, $1 \leq r \leq g$.
- Given $h, q, g$, there exists a finite list of admissible $(n_1, \ldots, n_g)$.
Introducing a new set of parameters

- Define $n_r := \#\{\text{closed points of degree } n \text{ on } C\}$.
- We can rewrite $L(t)$ in terms of $n_r$, $1 \leq r \leq g$.
- Given $h, q, g$, there exists a finite list of admissible $(n_1, \ldots, n_g)$.
- N.B. Such a sequence might not arise from an honest $L$-polynomial, so some can be eliminated using the Weil Conjectures.
Introducing a new set of parameters

- Define $n_r := \#\{\text{closed points of degree } n \text{ on } C\}$.
- We can rewrite $L(t)$ in terms of $n_r$, $1 \leq r \leq g$.
- Given $h, q, g$, there exists a finite list of admissible $(n_1, \ldots, n_g)$.
- N.B. Such a sequence might not arise from an honest $L$-polynomial, so some can be eliminated using the Weil Conjectures.
- Putting this all together, we get a finite set of conditions our function field must satisfy in order to have class number $h$. 
Quadratic vs. non-quadratic

- Quadratic function fields $\rightsquigarrow$ hyperelliptic curves.
Quadratic vs. non-quadratic

- Quadratic function fields $\leadsto$ hyperelliptic curves.
- Hyperelliptic curves have very well understood ramification.
Quadratic vs. non-quadratic

- Quadratic function fields $\mapsto$ hyperelliptic curves.
- Hyperelliptic curves have very well understood ramification.
- It is relatively easy to classify the hyperelliptic function fields corresponding to a sequence $(n_1, \ldots, n_g)$, if any exist.
Quadratic vs. non-quadratic

- Quadratic function fields $\leadsto$ hyperelliptic curves.
- Hyperelliptic curves have very well understood ramification.
- It is relatively easy to classify the hyperelliptic function fields corresponding to a sequence $(n_1, \ldots, n_g)$, if any exist.
- To study non-hyperelliptic curves, we consider the canonical embedding $C \hookrightarrow \mathbb{P}^{g-1}$ and try to classify it.
Classifying canonical curves

Let $C$ be a smooth non-hyperelliptic curve.
**Classifying canonical curves**

Let \( C \) be a smooth non-hyperelliptic curve.

<table>
<thead>
<tr>
<th>Theorem (Petri)</th>
</tr>
</thead>
<tbody>
<tr>
<td>If ( g(C) \geq 4 ), then the canonical embedding of ( C ) is cut out by quadrics, unless it is trigonal or a plane quintic curve ( (g = 6) ), in which case it is cut out by quadrics and cubics.</td>
</tr>
</tbody>
</table>
Classifying canonical curves

Let $C$ be a smooth non-hyperelliptic curve.

**Theorem (Petri)**

If $g(C) \geq 4$, then the canonical embedding of $C$ is cut out by quadrics, unless it is trigonal or a plane quintic curve ($g = 6$), in which case it is cut out by quadrics and cubics.

Some special cases of small genus:
Let $C$ be a smooth non-hyperelliptic curve.

**Theorem (Petri)**

If $g(C) \geq 4$, then the canonical embedding of $C$ is cut out by quadrics, unless it is trigonal or a plane quintic curve ($g = 6$), in which case it is cut out by quadrics and cubics.

Some special cases of small genus:

- **Genus 3**: $C$ embeds as a smooth quartic curve.
Classifying canonical curves

Let $C$ be a smooth non-hyperelliptic curve.

**Theorem (Petri)**

If $g(C) \geq 4$, then the canonical embedding of $C$ is cut out by quadrics, unless it is trigonal or a plane quintic curve ($g = 6$), in which case it is cut out by quadrics and cubics.

Some special cases of small genus:

- **Genus 3**: $C$ embeds as a smooth quartic curve.
- **Genus 4**: $C$ is the complete intersection of a quadric and a cubic surface.
Classifying canonical curves

Let $C$ be a smooth non-hyperelliptic curve.

**Theorem (Petri)**

If $g(C) \geq 4$, then the canonical embedding of $C$ is cut out by quadrics, unless it is trigonal or a plane quintic curve ($g = 6$), in which case it is cut out by quadrics and cubics.

Some special cases of small genus:

- **Genus 3**: $C$ embeds as a smooth quartic curve.
- **Genus 4**: $C$ is the complete intersection of a quadric and a cubic surface.
- **Genus 5**: $C$ is either trigonal or the complete intersection of 3 quadrics.
Fix $h = 3$ and $q = 2$ and use Magma to compute all admissible $g$ and their corresponding $(n_1, \ldots, n_g)$, excluding any which are automatically hyperelliptic (e.g. if $n_2 \geq 4$).
Fix $h = 3$ and $q = 2$ and use Magma to compute all admissible $g$ and their corresponding $(n_1, \ldots, n_g)$, excluding any which are automatically hyperelliptic (e.g. if $n_2 \geq 4$).

In this case, we only need to consider $g = 3, 4, \text{ or } 6$. 

Fix \( h = 3 \) and \( q = 2 \) and use Magma to compute all admissible \( g \) and their corresponding \((n_1, \ldots, n_g)\), excluding any which are automatically hyperelliptic (e.g. if \( n_2 \geq 4 \)).

In this case, we only need to consider \( g = 3, 4, \) or 6.

When possible, use the \( n_i \) to study the canonical class \( |K| \) and write down the “shape” of the canonical curve.
Fix \( h = 3 \) and \( q = 2 \) and use Magma to compute all admissible \( g \) and their corresponding \((n_1, \ldots, n_g)\), excluding any which are automatically hyperelliptic (e.g. if \( n_2 \geq 4 \)).

In this case, we only need to consider \( g = 3, 4, \) or 6.

When possible, use the \( n_i \) to study the canonical class \(|K|\) and write down the “shape” of the canonical curve.

Otherwise, use Magma to run through all possible remaining curves.
Outline of Proof

- Fix $h = 3$ and $q = 2$ and use Magma to compute all admissible $g$ and their corresponding $(n_1, \ldots, n_g)$, excluding any which are automatically hyperelliptic (e.g. if $n_2 \geq 4$).
- In this case, we only need to consider $g = 3, 4, \text{ or } 6$.
- When possible, use the $n_i$ to study the canonical class $|K|$ and write down the “shape” of the canonical curve.
- Otherwise, use Magma to run through all possible remaining curves.
- Use Magma to check for duplicates and return a list up to isomorphism.
An Example of the “hands on” approach

- $q = 2$, $h = 3$, $g = 3$, $(n_1, n_2, n_3) = (1, 0, 4)$
An Example of the “hands on” approach

- \( q = 2, \; h = 3, \; g = 3, \; (n_1, n_2, n_3) = (1, 0, 4) \)
- Let \( P \) be the unique degree 1 point and let \( \{Q_i\} \) be the 4 degree 3 points.
An Example of the “hands on” approach

- \( q = 2, h = 3, g = 3, (n_1, n_2, n_3) = (1, 0, 4) \)
- Let \( P \) be the unique degree 1 point and let \( \{ Q_i \} \) be the 4 degree 3 points.
- We have that \( \dim |K| = 2 \), so (in the non-hyperelliptic case) \( \dim |K - P| = 1 \) and \( \dim |K - 2P| = 0 \).
An Example of the “hands on” approach

- \( q = 2, \ h = 3, \ g = 3, \ (n_1, n_2, n_3) = (1, 0, 4) \)
- Let \( P \) be the unique degree 1 point and let \( \{Q_i\} \) be the 4 degree 3 points.
- We have that \( \dim |K| = 2 \), so (in the non-hyperelliptic case) \( \dim |K - P| = 1 \) and \( \dim |K - 2P| = 0 \).
- It is easy to deduce that, up to relabeling,

\[
|K - P| = \{3P, Q_1, Q_2\}, \text{ and } |K| = \{4P, Q_1 + P, Q_2 + P\} \cup \{\text{four degree 4 points}\}.
\]
An Example of the “hands on” approach

- $q = 2$, $h = 3$, $g = 3$, $(n_1, n_2, n_3) = (1, 0, 4)$
- Let $P$ be the unique degree 1 point and let $\{Q_i\}$ be the 4 degree 3 points.
- We have that $\dim |K| = 2$, so (in the non-hyperelliptic case) $\dim |K - P| = 1$ and $\dim |K - 2P| = 0$.
- It is easy to deduce that, up to relabeling,

$$|K - P| = \{3P, Q_1, Q_2\}, \text{ and}$$

$$|K| = \{4P, Q_1 + P, Q_2 + P\} \cup \{\text{four degree 4 points}\}.$$ 

- Set $(x) = Q_1 - 3P$ and $(y) = R - 4P$, where $R \sim K$ is a degree 4 point.
Recall $\mathcal{L}(nP) = \{ f \in \mathbb{F}_q(C) : \text{div } f + nP \geq 0 \}$. 
- Recall $\mathcal{L}(nP) = \{f \in \mathbb{F}_q(C) : \text{div } f +nP \geq 0\}$.

- By Riemann-Roch, $\dim \mathcal{L}(3P) = 2$ and $\dim \mathcal{L}(4P) = 3$, so we can let $\{1, x\}$ and $\{1, x, y\}$ be their bases, respectively.
Recall $\mathcal{L}(nP) = \{f \in \mathbb{F}_q(C) : \text{div} f +nP \geq 0\}$.

By Riemann-Roch, $\dim \mathcal{L}(3P) = 2$ and $\dim \mathcal{L}(4P) = 3$, so we can let $\{1, x\}$ and $\{1, x, y\}$ be their bases, respectively.

Since $\dim \mathcal{L}(12P) = 10$, and it contains the 11 functions $\{1, x, x^2, x^3, x^4, y, y^2, y^3, xy, x^2y, xy^2\}$, we have a relation of the form

$$ay^3 + \varphi_1(x)y^2 + \varphi_2(x)y + \varphi_4(x) = 0, \quad \deg \varphi_i(x) \leq i.$$ 

Moreover, the function $x$ vanishes at the cubic point $Q_1$, so $ay^3 + b_0y^2 + c_0y + d_0$ must be an irreducible cubic.
Recall $\mathcal{L}(nP) = \{ f \in F_q(C) : \text{div} f +nP \geq 0 \}$.

By Riemann-Roch, $\dim \mathcal{L}(3P) = 2$ and $\dim \mathcal{L}(4P) = 3$, so we can let $\{1, x\}$ and $\{1, x, y\}$ be their bases, respectively.

Since $\dim \mathcal{L}(12P) = 10$, and it contains the 11 functions $\{1, x, x^2, x^3, x^4, y, y^2, y^3, xy, x^2y, xy^2\}$, we have a relation of the form

$$ay^3 + \varphi_1(x)y^2 + \varphi_2(x)y + \varphi_4(x) = 0, \quad \deg \varphi_i(x) \leq i.$$

Moreover, the function $x$ vanishes at the cubic point $Q_1$, so $ay^3 + b_0y^2 + c_0y + d_0$ must be an irreducible cubic.

Similarly, $y$ vanishes at the quartic point $R$, so $\varphi_4(x)$ must be an irreducible quartic.
Recall $\mathcal{L}(nP) = \{ f \in \mathbf{F}_q(C) : \text{div } f +nP \geq 0 \}$.

By Riemann-Roch, $\dim \mathcal{L}(3P) = 2$ and $\dim \mathcal{L}(4P) = 3$, so we can let $\{1, x\}$ and $\{1, x, y\}$ be their bases, respectively.

Since $\dim \mathcal{L}(12P) = 10$, and it contains the 11 functions $\{1, x, x^2, x^3, x^4, y, y^2, y^3, xy, x^2y, xy^2\}$, we have a relation of the form

$$ay^3 + \varphi_1(x)y^2 + \varphi_2(x)y + \varphi_4(x) = 0, \quad \deg \varphi_i(x) \leq i.$$

Moreover, the function $x$ vanishes at the cubic point $Q_1$, so $ay^3 + b_0y^2 + c_0y + d_0$ must be an irreducible cubic.

Similarly, $y$ vanishes at the quartic point $R$, so $\varphi_4(x)$ must be an irreducible quartic.

Up to isomorphism, the only curve satisfying these properties is $y^3 + y + (x^4 + x + 1) = 0$. 
Because this method relies heavily on implementations in Magma, I would like to check it against computations in Sage, as well as convince myself of its accuracy (especially given the history of this problem).
Some final remarks

- Because this method relies heavily on implementations in Magma, I would like to check it against computations in Sage, as well as convince myself of its accuracy (especially given the history of this problem).
- This is also why a careful analysis of the canonical class is nice to have, as it provides a much-needed sanity check.
Some final remarks

- Because this method relies heavily on implementations in Magma, I would like to check it against computations in Sage, as well as convince myself of its accuracy (especially given the history of this problem).
- This is also why a careful analysis of the canonical class is nice to have, as it provides a much-needed sanity check.
- It took 6 days to run the code for the genus 4 case, but I believe the code can be made more efficient.
Some final remarks

- Because this method relies heavily on implementations in Magma, I would like to check it against computations in Sage, as well as convince myself of its accuracy (especially given the history of this problem).
- This is also why a careful analysis of the canonical class is nice to have, as it provides a much-needed sanity check.
- It took 6 days to run the code for the genus 4 case, but I believe the code can be made more efficient.
- It took 3.5 hours to run the code to check that there are no genus 6 curves. In this case, there simply were no \((n_1, \ldots, n_6)\) which work.