An improvement of the Hasse-Weil-Serre bound and construction of optimal curves of genus 3

Alexey Zaytsev

Claude Shannon Institute and
School of Mathematical Sciences
University College Dublin
Ireland

April 2011, Télécom ParisTech

Definitions

Definition

A **curve** $C/\mathbb{F}_q$ is a non-singular projective absolutely irreducible algebraic variety of dimension 1 over $\mathbb{F}_q$.

Definition

$$N_q(g) := \max\{\#C(\mathbb{F}_q) |\ C/\mathbb{F}_q \text{ a curve of genus } g\}$$

What is "a curve with many rational points"?

Definitions

Definition

A **curve** $C/\mathbb{F}_q$ is a non-singular projective absolutely irreducible algebraic variety of dimension 1 over $\mathbb{F}_q$.

Definition

$$N_q(g) := \max\{\#C(\mathbb{F}_q)|\ C/\mathbb{F}_q \text{ a curve of genus } g\}$$

What is "a curve with many rational points"?
By "a curve with many rational points" we mean a curve $C/\mathbb{F}_q$ so that the number of $\mathbb{F}_q$-rational points is close to $N_q(g)$.

$N_q(g)$

How we can find the number $N_q(g)$?

$N_q(g)$

How we can find the number $N_q(g)$? We can estimate it by numbers a and b, such that

$$a \leq N_q(g) \leq b.$$

methods

$$\left.\begin{array}{r} \text{Explicit Examples and Constructions.} \\ \text{Class Field Theory} \\ \text{Kummer extensions} \\ \text{Artin-Shreier extensions} \\ \text{Maximal curves} \\ \text{Modular Curves} \\ \text{Drinfeld-Modular Curves, etc.} \end{array}\right. \leq N_q(g)$$

Explicit Examples and Constructions.
Class Field Theory
Kummer extensions
Artin-Shreier extensions $\leq N_q(g)$
Maximal curves
Modular Curves
Drinfeld-Modular Curves, etc.

Theoretical approach.
the Hasse-Weil bound
the Hasse-Weil-Serre bound
$N_q(g) \leq$ Oesterlé bound
Stöhr-Voloch approach
Defect Theory
Galois Descent, etc.

Maximal curves

The **Hasse-Weil** bound: Let $C/\mathbb{F}_q$ be a curve of genus g then the number of $\mathbb{F}_q$-rational points satisfies the following inequality

$$\#C(\mathbb{F}_q) \leq q + 1 + 2g\sqrt{q}.$$

Maximal curves

The **Hasse-Weil** bound: Let $C/\mathbb{F}_q$ be a curve of genus g then the number of $\mathbb{F}_q$-rational points satisfies the following inequality

$$\#C(\mathbb{F}_q) \leq q + 1 + 2g\sqrt{q}.$$

if q is not square then it can be improved (it was done by J-P. Serre)

$$\#C(\mathbb{F}_q) \leq q + 1 + g[2\sqrt{q}]$$

and now it is called the **Hasse-Weil-Serre** bound.

Maximal curves

The **Hasse-Weil** bound: Let $C/\mathbb{F}_q$ be a curve of genus g then the number of $\mathbb{F}_q$-rational points satisfies the following inequality

$$\#C(\mathbb{F}_q) \leq q + 1 + 2g\sqrt{q}.$$

if q is not square then it can be improved (it was done by J-P. Serre)

$$\#C(\mathbb{F}_q) \leq q + 1 + g[2\sqrt{q}]$$

and now it is called the **Hasse-Weil-Serre** bound.

Definition

A curve $C/\mathbb{F}_q$ is called **maximal curve** if

$$\#C(\mathbb{F}_q) = q + 1 + g[2\sqrt{q}].$$

Maximal curves

The **Hasse-Weil** bound: Let $C/\mathbb{F}_q$ be a curve of genus g then the number of $\mathbb{F}_q$-rational points satisfies the following inequality

$$\#C(\mathbb{F}_q) \leq q + 1 + 2g\sqrt{q}.$$

if q is not square then it can be improved (it was done by J-P. Serre)

$$\#C(\mathbb{F}_q) \leq q + 1 + g[2\sqrt{q}]$$

and now it is called the **Hasse-Weil-Serre** bound.

Definition

A curve $C/\mathbb{F}_q$ is called **maximal curve** if

$$\#C(\mathbb{F}_q) = q + 1 + g[2\sqrt{q}].$$

In works of F. Torres. A. Garcia and H. Stichtenoth, a maximal curve is that reaches the Hasse-Weil bound, i. e. it is always defined over $\mathbb{F}_{q^2}$

Theorem

Drinfeld-Vlăduț

$$lim_{g \to \infty}\ sup \frac{N_q(g)}{g} \leq \sqrt{q} - 1,$$

and if q is a square then

$$lim_{g \to \infty}\ sup \frac{N_q(g)}{g} = \sqrt{q} - 1,$$

Drinfeld-Vlăduț theorem

Theorem

Drinfeld-Vlăduț

$$lim_{g\to\infty}\ sup\frac{N_q(g)}{g} \leq \sqrt{q}-1,$$

and if q is a square then

$$lim_{g\to\infty}\ sup\frac{N_q(g)}{g} = \sqrt{q}-1,$$

The Drinfeld-Vlăduț upper-bound shows that

$$N_q(g) \backsim g(\sqrt{q}-1).$$

It easy to see that inequality

$$N_q(g) \leq g([2\sqrt{q}]),$$

obtained via the Hasse-Weil-Serre bound is weaker.

The Deuring's Theorem describes all isogeny classes of elliptic curves over finite fields. As a consequence, we can find the maximal number of rational points on elliptic curves, i. e. $N_q(1)$.

The Deuring's Theorem describes all isogeny classes of elliptic curves over finite fields. As a consequence, we can find the maximal number of rational points on elliptic curves, i. e. $N_q(1)$.

Theorem

Let $q = p^a$ for a prime number p and $m = [2\sqrt{q}]$. Then if a is odd, $a \geq 3$ and $p|m$ then

$$N_q(1) = q + 1 + m - 1,$$

while

$$N_q(1) = q + 1 + m$$

for all other cases.

Curves of genus 2

The case of genus 2 curves was managed by J-P. Serre.

Definition

The positive integer number q is called *special* if either $\mathrm{char}(\mathbb{F}_q)$ divides $m = [2\sqrt{q}]$ or q is of the form $a^2 + 1$, $a^2 + a + 1$ or $a^2 + a + 2$ for some integer a.

Theorem

Let $q = p^e$ and $m = [2\sqrt{q}]$. Then we have:
If e is even, then

- *if $q = 4$ then $N_4(2) = 10 = q + 1 + 2m - 3$,*
- *if $q = 9$ then $N_9(2) = 20 = q + 1 + 2m - 2$,*
- *for all other q one has $N_q(2) = q + 1 + 2m$.*

If e is odd then:

- *if q is special and $\{2\sqrt{q}\} \geq (\sqrt{5} - 1)/2$, then $N_q(2) = q + 1 + 2m - 1$,*
- *if q is special and $\{2\sqrt{q}\} < (\sqrt{5} - 1)/2$, then $N_q(2) = q + 1 + 2m - 2$,*
- *for all other q one has $N_q(2) = q + 1 + 2m$,*

where $\{\cdot\}$ denotes the fractional part.

J. Top proved the following proposition by using the approach of K. O. Stöhr and J. F. Voloch.

If C is a curve of genus 3 over $\mathbb{F}_q$ and $\#C(\mathbb{F}_q) > 2q+6$, then $q \in \{8,9\}$. Moreover, C is isomorphic over $\mathbb{F}_q$ either to the plane curve over $\mathbb{F}_8$ given by

$$x^4+y^4+z^4+x^2y^2+y^2z^2+x^2z^2+x^2yz+xy^2z+xyz^2=0,$$

with 24 $\mathbb{F}_8$-rational points, or to the quartic Fermat curve

$$x^4+y^4+z^4=0$$

over $\mathbb{F}_9$ with 28 $\mathbb{F}_9$-rational points.

In the same article, J. Top gives a table of $N_q(3)$ for all $q<100$.

An alternative approach of finding the number $N_q(g)$, is due to J-P. Serre and it is based on the theory of hermitian modules. Using this approach K. Lauter obtains the following result.

Theorem

For every finite field $\mathbb{F}_q$ there exists a curve C of genus $g(C) = 3$ over $\mathbb{F}_q$, such that,

$$|\#C(\mathbb{F}_q) - (q+1)| \geq 3m - 3.$$

In particular, we have that

$$N_q(3) \geq q + 1 + 3m - 3.$$

Maximal Curves

Definition

If a curve $H/\mathbb{F}_{q^2}$ can be given by equation

$$y^q + y = x^{q+1}$$

then it is called **hermitian** curve.

Theorem

The genus of a hermitian curve is $q(q-1)/2$ and the number of $\mathbb{F}_{q^2}$-rational points is

$$q^3 + 1 = q^2 + 1 + 2gq.$$

Next result on estimation of genus of maximal curves over $\mathbb{F}_{q^2}$ is due to R. Fuhrmann, A. Garcia and H. Stichtenoth.

Theorem

If $C/\mathbb{F}_{q^2}$ is a maximal curve of genus g then $g = q(q-1)/2$ or $g \leq (q-1)^2/4$.

There was a conjecture that every maximal curve over $\mathbb{F}_{q^2}$ is covered by a hermitian curve. M. Giulietti, G. Korchmaros have found a counter example (see paper "A new family of maximal curves over a finite field").

Examples of maximal curves

The Klein quartic curve $C/\mathbb{F}_{2^n}$ is given by equation

$$x^3y + y^3z + xz^3 = 0.$$

The genus of the Klien curve is 3 and it has $24 = 8 + 1 + 3[2\sqrt{8}]$ rational points.
(An example of a maximal curve over $\mathbb{F}_{47}$ form my work.) A curve $C/\mathbb{F}_{47}$, which is given by the equation

$$z^4 - (20x^2 - 2x - 16)z^2 + (10x^2 - x - 8)^2 - x^3 - x - 38 = 0,$$

is a maximal curve of genus 3 with $64 = 47 + 1 + 3[2\sqrt{47}]$ rational points.

Optimal curves of low genus over finite fields

Now, I am presenting some my results from paper "Optimal curves of low genus over finite fields".

Optimal curves of low genus over finite fields

Now, I am presenting some my results from paper "Optimal curves of low genus over finite fields".

Definition

Let $\mathbb{F}_q$ be a finite field, the number $d(\mathbb{F}_q) = [2\sqrt{q}]^2 - 4q$ is called the **discriminant** of $\mathbb{F}_q$.

Now, I am presenting some my results from paper "Optimal curves of low genus over finite fields".

Definition

Let $\mathbb{F}_q$ be a finite field, the number $d(\mathbb{F}_q) = [2\sqrt{q}]^2 - 4q$ is called the **discriminant** of $\mathbb{F}_q$.

Example

$$\{q|\ d(\mathbb{F}_q) = -11\} = \{23,\ 59,\ 113,\ 243, \ldots\}$$

Example

$$\{q|\ d(\mathbb{F}_q) = -7\} = \{2^3,\ 2^5, 2^{13}\}$$

Definition

A curve $C/\mathbb{F}_q$ is called **optimal** if

$$\#C(\mathbb{F}_q) = q + 1 \pm g[2\sqrt{q}].$$

We have seen above that the Hasse-Weil-Serre bound can improved by different methods if genus of curve much lager than the cardinality of a finite field. However if genus of a curve is relatively small (compare to q) in many cases this bound is the best possible. In general, the problem to improve the Hasse-Weil-Serre bound for low genera is very difficult.

Theorem

Let C be a curve of genus g over a finite field $\mathbb{F}_q$ of characteristic p. Then we have that

$$|\#C(\mathbb{F}_q) - q - 1| \le g[2\sqrt{q}] - 2,$$

if one of the lines of the conditions in the following table holds:

$d(\mathbb{F}_q)$	q	g
-3	$q \neq 3$	$3 \le g \le 10$
-4	$q \neq 2$	$3 \le g \le 10$
-7		$4 \le g \le 7$
-8	$p \neq 3$	$3 \le g \le 7$
-11	$p \neq 3,\ q < 10^4$	$g = 4$
-11	$p > 5$	$g = 5$
-19	$q < 10^4$	$g = 4$
-19	$q \not\equiv 1 \pmod 5$	$g = 5$

One result from the Defect Theory:

Proposition

Let $C/\mathbb{F}_q$ be a curve of genus g and $g \geq 3$ then

$$\#C(\mathbb{F}_q) \neq q + 1 \pm g[2\sqrt{q}] \mp 1.$$

One result from the Defect Theory:

Proposition

Let $C/\mathbb{F}_q$ be a curve of genus g and $g \geq 3$ then

$$\# C(\mathbb{F}_q) \neq q + 1 \pm g[2\sqrt{q}] \mp 1.$$

If C is an optimal curve of genus g over a finite field $\mathbb{F}_q$, then by the Honda-Tate theory and the Defect Theory it follows that

$$\mathrm{Jac}(C) \sim E^g \quad \text{over} \quad \mathbb{F}_q,$$

where E is an optimal (maximal or
 minimal) elliptic curve over $\mathbb{F}_q$. If the elliptic curve $E/\mathbb{F}_q$ is an ordinary (and hence $\mathrm{Jac}(C)$ is an ordinary abelian variety), then one can describe optimal curves via an equivalence of categories.

An Equivalence of Categories

Let $m = [2\sqrt{q}]$, $R = Z[X]/(X^2 - mX + q)$ and E is an optimal elliptic curve over $\mathbb{F}_q$.
$\mathrm{Ab}(m,q) = \{A/\mathbb{F}_q \mid A$ – abelian variety, $A \sim E^g\}$

$$\mathrm{Mod}(R) = \begin{array}{l} \{T \mid T \text{ is torsion free} \\ R - \text{module of finite type}\} \end{array}$$

Functor:

$$T : \left\{ \begin{array}{rcl} \mathrm{Ab}(m,q) & \rightarrow & \mathrm{Mod}(R) \\ A & \mapsto & T(A) = \mathrm{Hom}(E, A) \end{array} \right.$$

inverse functor

$$T : \left\{ \begin{array}{rcl} \mathrm{Mod}(R) & \rightarrow & \mathrm{Ab}(m,q) \\ T & \mapsto & E \otimes_R T \end{array} \right.$$

Polarization

If $\phi : A \to A^\vee$ is a polarization then it corresponds to R-hermitian form

$$h : T(A) \times T(A) \to R.$$

Moreover, if $T(A)$ is a free R-module then degree of polarization ϕ equals to $\det(h)$.

Conditions

On conditions that

1) $E/\mathbb{F}_q$ is an ordinary $\Leftrightarrow \mathrm{char}(\mathbb{F}_q) \not| \#E(\mathbb{F}_q) - 1$,

Conditions

On conditions that
1) $E/\mathbb{F}_q$ is an ordinary $\Leftrightarrow \mathrm{char}(\mathbb{F}_q) \not| \#E(\mathbb{F}_q) - 1$,
2) $d(\mathbb{F}_q) \in \{-3, -4, -7, -8, -11, -19\}$

On conditions that
1) $E/\mathbb{F}_q$ is an ordinary $\Leftrightarrow \mathrm{char}(\mathbb{F}_q) \not| \# E(\mathbb{F}_q) - 1$,
2) $d(\mathbb{F}_q) \in \{-3,\ -4,\ -7,\ -8,\ -11,\ -19\}$
there exits an isomorphism

$$\mathrm{Jac}(C) \cong E^g \quad \text{over} \quad \mathbb{F}_q.$$

and $(\mathrm{Jac(C)},\ \Theta)$ corresponds to $(\mathcal{O}_K^g,\ h)$, where $\mathcal{O}_K$ is the ring of integers in $K = Q(\sqrt{d})$ and $h : \mathcal{O}_K^g \times \mathcal{O}_K^g \to \mathcal{O}_K$ is $\mathcal{O}_K$-hermitian form.
The classification of such hermitian modules was done by A. Schiemann.

Projections and Automorphism groups

Theorem

Let C be an optimal curve over $\mathbb{F}_q$. Then the degree of the k-th projection

$$f_k : C \hookrightarrow \mathrm{Jac}(C) \cong E^g \xrightarrow{pr_k} E$$

equals $\det(h_{ij})_{i,j \neq k}$.

Theorem

Let C be an optimal curve over $\mathbb{F}_q$. Then the degree of the k-th projection

$$f_k : C \hookrightarrow \mathrm{Jac}(C) \cong E^g \xrightarrow{pr_k} E$$

equals $\det(h_{ij})_{i,j\neq k}$.

For finite characteristic, P. Roquette proved

$$\#\mathrm{Aut}_{\bar{\mathbb{F}}_q}(C) \leq 84(g-1)$$

under the conditions that $g \geq 2$, $p > g+1$ and the curve C is not given by an equation of the form $y^2 = x^p - x$. The upper bound for small p (i.e. $p \leq 2g+1$) was obtained by B. Singh

$$\#\mathrm{Aut}_{\bar{\mathbb{F}}_q}(C) \leq \frac{4pg^2}{p-1}\left(\frac{2g}{p-1}+1\right)\left(\frac{4pg^2}{(p-1)^2}+1\right).$$

Projections and Automorphism groups

Using Torelli's theorem we obtain upper bounds on the number of automorphisms of irreducible unimodular hermitian modules $(\mathcal{O}_K^g, h)$. For example,

$$\#\mathrm{Aut}(\mathcal{O}_K^g, h) \leq \begin{cases} 84(g(C)-1) & C \text{ is hyperelliptic,} \\ 168(g(C)-1) & \text{otherwise.} \end{cases}$$

Let $d(\mathbb{F}_q) = -7$ **and** $g = 4$ then $\#\mathrm{Aut}(\mathcal{O}_K^4, h) = 2^7 \cdot 3^2$.
If we assume that there exists an optimal curve of genus 4. Then we study an automorphism group of the optimal curve.
Let τ be an involution from the center of Sylow 2-subgroup of $\mathrm{Aut}_{\mathbb{F}_q}(\mathrm{C})$. Then $C/\langle\tau\rangle \ncong E$, since $\#\mathrm{Aut}_{\mathbb{F}_q}(C/\langle\tau\rangle) > 2$ and $\mathrm{Aut}(E) = \{\pm 1\}$. On the other hand there is a projection f_k of degree 2 and hence there exists an involution σ such that $C/\langle\sigma\rangle \cong E$.

Then $\langle \sigma, \tau \rangle \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ and we have the following diagram of coverings of degree 2

$$\begin{tikzcd}
 & C \arrow[dl] \arrow[d] \arrow[dr] & \\
C/\langle \sigma \rangle \arrow[dr] & C/\langle \sigma\tau \rangle \arrow[d] & C/\langle \tau \rangle \arrow[dl] \\
 & C/\langle \sigma, \tau \rangle &
\end{tikzcd}$$

Moreover, we have the following isogeny

$$\begin{gathered}
\mathrm{Jac}(C) \times \mathrm{Jac}(C/\langle \sigma, \tau \rangle)^2 \sim \\
\sim \mathrm{Jac}(C/\langle \sigma \rangle) \times \mathrm{Jac}(C/\langle \sigma\tau \rangle) \times \mathrm{Jac}(C/\langle \tau \rangle).
\end{gathered}$$

According to Hurwitz's formula and non-existence of optimal curve of genus 2 we have that on hand the isogeny

$$E^4 \times \mathrm{Jac}(C/\langle\sigma, \tau\rangle) \sim E \times \mathrm{Jac}(C/\langle\sigma\rangle)) \times \mathrm{Jac}(C/\langle\tau\rangle)$$

and on the other hand

$$\dim(E^4 \times \mathrm{Jac}(C/\langle\sigma, \tau\rangle)) \geq 4,$$

$$\dim(E \times \mathrm{Jac}(C/\langle\sigma\rangle)) \times \mathrm{Jac}(C/\langle\tau\rangle) \leq 3.$$

Therefore there is no optimal curve of genus 4 over finite field with the discriminant -7.

Equations of Optimal Curves of Genus 3 over Finite Fields with Discriminant $-19, -43, -67, -163$

Coauthors

E. Alekseenko *Immanuel Kant State University of Russia*
S. Aleshnikov *Immanuel Kant State University of Russia*
N. Markin *Claude Shannon Institute (now Nanyang Technological University)*

Projections and Automorphism groups

Theorem

Let C be an optimal curve over $\mathbb{F}_q$. Then the degree of the k-th projection

$$f_k : C \hookrightarrow \mathrm{Jac}(C) \cong E^g \xrightarrow{pr_k} E$$

equals $\det(h_{ij})_{i,j\neq k}$.

Example

if

$$h := \begin{pmatrix} 2 & 1 & -1 \\ 1 & 3 & \frac{-3+\sqrt{-19}}{2} \\ -1 & \frac{-3-\sqrt{-19}}{2} & 3 \end{pmatrix}$$

then

$$\det \begin{pmatrix} 3 & \frac{-3+\sqrt{-19}}{2} \\ \frac{-3-\sqrt{-19}}{2} & 3 \end{pmatrix} = 2.$$

Therefore there is a degree two map $C \to E$.

Discriminant and Hermitain Form

$d = -19$

$$\begin{pmatrix} 2 & 1 & -1 \\ 1 & 3 & \frac{-3+\sqrt{-19}}{2} \\ -1 & \frac{-3-\sqrt{-19}}{2} & 3 \end{pmatrix}$$

$d = -43$

$$\begin{pmatrix} 3 & \frac{3-\sqrt{-43}}{2} & \frac{3+\sqrt{-43}}{2} \\ \frac{3+\sqrt{-43}}{2} & 5 & \frac{-5+\sqrt{-43}}{2} \\ \frac{3-\sqrt{-43}}{2} & \frac{-5-\sqrt{-43}}{2} & 5 \end{pmatrix}$$

$d = -67$

$$\begin{pmatrix} 2 & 0 & -1 \\ 0 & 2 & \frac{-3-\sqrt{-67}}{2} \\ -1 & \frac{-3+\sqrt{-67}}{2} & 7 \end{pmatrix}$$

$d = -163$

$$\begin{pmatrix} 2 & 1 & \frac{-1+\sqrt{-163}}{2} \\ 1 & 2 & \frac{1+\sqrt{-163}}{2} \\ \frac{-1-\sqrt{-163}}{2} & \frac{1-\sqrt{-163}}{2} & 28 \end{pmatrix}$$

All hermitian modules above have an automorphism group of order 12.

Theorem

If the discriminant $\mathrm{d}(\mathbb{F}_q) \in \{-19, -43, -67, -163\}$ *then there is an optimal curve* C *of genus* 3 *over a finite field* $\mathbb{F}_q$ *such that a polarization of its Jacobian corresponds to one of hermitian form above and*

- *the curve* C *is a double covering of a maximal or minimal elliptic curve, respectively,*
- *the* C *is non-hyperelliptic,*
- *the Hermitian modules can not correspond to maximal and minimal curves simultaneously,*
- *the automorphism group of curve* C *is isomorphic to the dihedral group of order* 6*.*

Remark

Although we know that an optimal curve exists but we do not know whether it is maximal or minimal (it depends not only on polarization of Jacobian but also on a finite field). A recent result of Christophe Ritzenthaler in "Explicit computations of Serre's obstruction for genus 3 curves and application to optimal curves " can be used to detect which type of curve exists for each q.

Theorem

Let C be an optimal curve over $\mathbb{F}_q$. Then C can be given by a system of equations of the following forms:

$$\begin{cases} z^2 = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \beta_0 y, \\ y^2 = x^3 + ax + b, \end{cases}$$

$$\begin{cases} z^2 = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + (\beta_0 + \beta_1 x) y, \\ y^2 = x^3 + ax + b, \end{cases}$$

$$\begin{cases} z^2 = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \alpha_3 x^3 + (\beta_0 + \beta_1 x) y, \\ y^2 = x^3 + ax + b, \end{cases}$$

with coefficients in $\mathbb{F}_q$ and the equation $y^2 = x^3 + ax + b$ corresponding to an optimal elliptic curve.

Let C be an optimal curve of genus 3 over a finite field $\mathbb{F}_q$ and let $f : C \to E$ be a double covering of C with the equation $y^2 = x^3 + ax + b$. Set $D = f^{-1}(\infty') = \sum_{P|\infty'} e(P|\infty') \cdot P \in \mathrm{Div}(C)$, where $\infty' \in E$ lies over $\infty \in \mathbb{P}^1$ by the action $E \to \mathbb{P}^1$, $\deg D = 2$.
By Riemann-Roch Theorem

$$\dim D = \deg D + 1 - g + \dim(W - D) = \dim(W - D),$$

where W is a canonical divisor of the curve C. Consequently, D is equivalent to the positive divisor $W - D_1$, where $\deg D_1 = 2$. Conclude $\dim D = \dim(W - D) < \dim W = 3$. Taking into account that C is a non-hyperelliptic curve and $\deg D = 2$, we conclude $\dim D = 1$.

There are three case, namely

- $\dim(2D) = 3$,

There are three case, namely

- $\dim(2D) = 3$,
- $\dim(2D) = 2$ and $D = Q_1 + Q_2$, where $Q_1 \neq Q_2$, $Q_1, Q_2 \in C(\bar{\mathbb{F}}_q)$,

There are three case, namely

- $\dim(2D) = 3$,
- $\dim(2D) = 2$ and $D = Q_1 + Q_2$, where $Q_1 \neq Q_2$, $Q_1, Q_2 \in C(\bar{\mathbb{F}}_q)$,
- Suppose $\dim(2D) = 2$ and $D = Q_1 + Q_2 = 2Q$, where $Q_1 = Q_2 = Q \in C(\bar{\mathbb{F}}_q)$.

Here we consider only the third one.
In order to manage this case we prove that the elements $1, x, z, y, x^2, z^2, xy, xz$ are linearly dependent over $\mathbb{F}_q$. As a corollary of this fact we obtain the equation of the second type.
In this case the functions $x \in L(2D)$, $y \in L(3D)$ have pole divisors $(x)_\infty = 4Q$, $(y)_\infty = 6Q$, and there is a function $z \in L(2D + Q)$ such that $(z)_\infty = 5Q$.

The element z is an integral element over $\mathbb{F}_q[x, y]$. Indeed, either

$$1, x, z, y, x^2, z^2, xy, xz \in L(10D)$$

or

$$1, x, y, z, x^2, zx, xy, z^2, zy, x^3, zx^2, xyz, z^3 \in L(15Q)$$

are linearly dependent and in both cases we have relations with nonzero leading coefficients at highest power in z. This yields that z is integral over $\mathbb{F}_q[x, y]$.
It is clear that $z \notin \mathbb{F}_q(x, y)$ (otherwise 2 divides $v_Q(z) = 5$).
The minimal polynomial of z has degree 2 and coefficients in $\mathbb{F}_q[x, y]$, since the degree of extension $[\mathbb{F}_q(C) : \mathbb{F}_q(x, y)]$ is 2.
Therefore we have that

$$z^2 + \sum_{i \geq 0} a_i zyx^i + \sum_{j \geq 0} b_j zx^j + \sum_{l \geq 0} c_l x^l + \sum_{s \geq 0} d_s yx^s = 0,$$

and hence

$$\begin{gathered} z^2 + c_0 + c_1 x + c_2 x^2 + d_0 y + b_0 z + b_1 zx + d_1 xy = \\ = -z(b_2 x^2 + \ldots) + zy(a_0 + a_1 x + \ldots) + \\ +(c_4 x^4 + \ldots) + y(d_2 x^2 + \ldots). \end{gathered}$$

Furthermore, we have

- $v_Q(zx^i) = -5 - 4i \equiv 3 \mod 4$
- $v_Q(zyx^j) = -5 - 6 - 4i \equiv 1 \mod 4$
- $v_Q(x^l) = -4l \equiv 0 \mod 4$
- $v_Q(yx^i) = -6 - 4i \equiv 2 \mod 4.$

If the right part of the equation above is non-zero, then we can apply the strict triangle inequality. As a consequence we get that on the one hand

$$v_Q(z^2 + c_0 + c_1 x + c_2 x^2 + d_0 y + b_0 z + b_1 zx + d_1 xy) \leq -11$$

and on the other hand

$$v_Q(z^2 + c_0 + c_1x + c_2x^2 + d_0y + b_0z + b_1zx + d_1xy) \geq -10.$$

Therefore the right part of the equation above is zero, i. e. the elements $1, x, z, y, x^2, z^2, xy, xz$ are linearly dependent.

Examples of Maximal and Minimal Curves

Here we use the following abbreviations:
we write $[a, b]$ instead of $y^2 = x^3 + ax + b$,
and (A, B, C, D) instead of $z^2 = Ax^2 + Bx + C + Dy$.

Discriminant is -19

q	Maximal curve	Minimal curve
47	$[1, 38]$, $(10, 46, 39, 1)$	-
61	$[6, 29]$, $(1, 54, 38, 3)$	-
137	$[1, 36]$, $(3, 95, 92, 10)$	-
277	$[2, 61]$, $(1, 33, 212, 5)$	-
311	$[18, 308]$, $(11, 222, 32, 65)$	-
347	-	$[174, 12]$, $(2, 310, 219, 94)$
467	$[2, 361]$, $(2, 38, 242, 159)$	-
557	-	$4y^2 = x^3 + 2x + 151$, $(5, 322, 439, 122)$

Discriminant is -43

q	Maximal curve	Minimal curve
167		$[5, 41]$, $(1, 128, 27, 58)$
193		$[10, 39]$, $(1, 28, 5, 93)$
251	$[1, 243]$, $(1, 74, 184, 5)$	
317	$[5, 86]$, $(1, 246, 164, 24)$	
431	$[1, 296]$, $(1, 44, 317, 185)$	
563		$[2, 200]$, $(1, 24, 383, 99)$

Discriminant is -67

q	Maximal curve	Minimal curve
359		$[1, 172]$, $(7, 25, 158, 123)$
397	$[3, 130]$, $(1, 70, 125, 154)$	
479		$[1, 351]$, $(1, 148, 195, 135)$
523		$[1, 112]$, $(1, 115, 76, 102)$

Another approach

Since we are working with ordinary abelian variety, we can use Deligne's description of ordinary abelian varieties. So we can lift a maximal or minimal curve to complex field with endomorphism ring. The classification of Riemann surfaces along with its automorphism group provides that an equation of a lifted curve is

$$a(x^4+y^4+1)+b(x^3y+xy^3+x^3+y^3+x+y)+c(x^2y^2+x^2+y^2)=0$$

However the reduction of this can give us not the desirable but its twist over $\bar{\mathbb{F}}_q$, therefore if a reduced curve is not optimal we shall check all twisted curves.

Now, we can search a curve over a finite field using this equation.

Example

A minimal curve C over $\mathbb{F}_{997}$ is given by equation

$$306(x^4+y^4+1)+589(x^3y+xy^3+x^3+y^3+x+y)+(x^2y^2+x^2+y^2)=0,$$

$$\#C(\mathbb{F}_{997})=809$$

Thank you for your attention!