A method of finding explicit equation for optimal curve of genus 4

E. Alekseenko

Immanuel Kant Baltic Federal University
Kaliningrad

September 11, 2014
ACCT-2014

Introduction

Curves over $\mathbb{F}_q$ with many rational points $\longmapsto$ long AG-codes.

Curves over $\mathbb{F}_q$ with many rational points $\longmapsto$ long AG-codes.

Definition

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

Introduction

Curves over $\mathbb{F}_q$ with many rational points $\longmapsto$ long AG-codes.

Definition

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

Definition

$C/\mathbb{F}_q$ is called a curve with many rational points if $\#C(\mathbb{F}_q)$ is close to $N_q(g) := \max\{\#C(\mathbb{F}_q) | C/\mathbb{F}_q$ - curve of genus $g\}$.

Introduction

Elliptic curves

M. Deuring

Curves of genus 2

J.-P. Serre

Curves of genus 3

J. Top, J.-P. Serre, K. Lauter.

Introduction

Hasse-Weil-Serre bound

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

Introduction

Hasse-Weil-Serre bound

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

Definition

If a number of rational points of $C/\mathbb{F}_q$ satisfies one of the conditions

$$\#C(\mathbb{F}_q) = q + 1 \pm \lfloor 2\sqrt{q} \rfloor g,$$

then the curve is called **an optimal curve** (**maximal** or **minimal** respectively).

Introduction

Explicit equations of optimal curves of genus 3 over some finite fields

- E. Alekseenko, S. Aleshnikov, N. Markin, A. Zaytsev.
  Optimal curves over finite fields with discriminant -19.
  Finite Fields and Their Applications, 17, 2011, 350–358.
- E. Alekseenko, A. Zaytsev.
  New method of constructing optimal curves of genus 3 *over certain finite fields*.
  AGCT-14, 2013.

Introduction

Explicit equations of optimal curves of genus 3 over some finite fields

- E. Alekseenko, S. Aleshnikov, N. Markin, A. Zaytsev.
  Optimal curves over finite fields with discriminant -19.
  Finite Fields and Their Applications, 17, 2011, 350–358.
- E. Alekseenko, A. Zaytsev.
  New method of constructing optimal curves of genus 3 *over certain finite fields*.
  AGCT-14, 2013.

Definition

$d(\mathbb{F}_q) = \lfloor 2\sqrt{q} \rfloor^2 - 4q$ is called the discriminant of $\mathbb{F}_q$.

Introduction

Explicit equations of optimal curves of genus 3 over some finite fields

- E. Alekseenko, S. Aleshnikov, N. Markin, A. Zaytsev.
  Optimal curves over finite fields with discriminant -19.
  Finite Fields and Their Applications, 17, 2011, 350–358.
- E. Alekseenko, A. Zaytsev.
  New method of constructing optimal curves of genus 3 *over certain finite fields.*
  AGCT-14, 2013.

Definition

$d(\mathbb{F}_q) = \lfloor 2\sqrt{q} \rfloor^2 - 4q$ is called the discriminant of $\mathbb{F}_q$.

What about optimal curves of genus 4?

Notation

$E/\mathbb{F}_q : y^2 = x^3 + ax + b$ – optimal elliptic curve.

Notation

$E/\mathbb{F}_q : y^2 = x^3 + ax + b$ – optimal elliptic curve.

$H/\mathbb{F}_q$ – curve of genus 2.

Notation

$E/\mathbb{F}_q : y^2 = x^3 + ax + b$ – optimal elliptic curve.

$H/\mathbb{F}_q$ – curve of genus 2.

$f : H \to E$ – double covering of E:

$$H : z^2 = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \beta y.$$

Main result

- $$H : z^2 = f, \quad f \in \mathbb{F}_q(E).$$

Main result

- $$H : z^2 = f, \quad f \in \mathbb{F}_q(E).$$
- H is ramified over two points $P_1, P_2 \in E(\mathbb{F}_q)$:
$$\mathrm{div}(f) = P_1 + P_2 + 2D,$$
$D \in \mathrm{Div}(E)$, $\deg D = -1$.

Main result

- $$H : z^2 = f, \quad f \in \mathbb{F}_q(E).$$

- H is ramified over two points $P_1, P_2 \in E(\mathbb{F}_q)$:

  $$\mathrm{div}(f) = P_1 + P_2 + 2D,$$

  $D \in \mathrm{Div}(E)$, $\deg D = -1$.

- $\exists Q \in E(\mathbb{F}_q)$ and $\exists g \in \mathbb{F}_q(E)$:

  $$\mathrm{div}(g) = Q - D - 2\mathcal{O}.$$

Main result

- $$H : z^2 = f, \quad f \in \mathbb{F}_q(E).$$
- H is ramified over two points $P_1, P_2 \in E(\mathbb{F}_q)$:
  $$\mathrm{div}(f) = P_1 + P_2 + 2D,$$
  $D \in \mathrm{Div}(E)$, $\deg D = -1$.
- $\exists Q \in E(\mathbb{F}_q)$ and $\exists g \in \mathbb{F}_q(E)$:
  $$\mathrm{div}(g) = Q - D - 2\mathcal{O}.$$
- $$z^2 = f \Rightarrow (zg)^2 = fg^2.$$

Main result

- $$H : z^2 = f, \quad f \in \mathbb{F}_q(E).$$
- H is ramified over two points $P_1, P_2 \in E(\mathbb{F}_q)$:
$$\mathrm{div}(f) = P_1 + P_2 + 2D,$$
$D \in \mathrm{Div}(E)$, $\deg D = -1$.
- $\exists Q \in E(\mathbb{F}_q)$ and $\exists g \in \mathbb{F}_q(E)$:
$$\mathrm{div}(g) = Q - D - 2\mathcal{O}.$$
- $$z^2 = f \Rightarrow (zg)^2 = fg^2.$$
- $$\mathrm{div}(fg^2) = \mathrm{div}(f) + 2\mathrm{div}(g) = P_1 + P_2 + 2Q - 4\mathcal{O}.$$

Main result

- If

$$fg^2 \mapsto h, \quad zg \mapsto w,$$

Main result

- If

$$fg^2 \mapsto h, \quad zg \mapsto w,$$

- then

$$H : w^2 = h.$$

Main result

- If

$$fg^2 \mapsto h, \quad zg \mapsto w,$$

- then

$$H : w^2 = h.$$

-

$$\mathrm{div}(w^2) = \mathrm{div}(h) = P_1 + P_2 + 2Q - 4\mathcal{O}.$$

$$\Downarrow$$

$$h \in L(4\mathcal{O}) = \{1, x, x^2, y\}.$$

Main result

- Any genus 2 double cover H of curve E is given by equation

$$z^2 = f, \quad \mathrm{div}(f) = P_1 + P_2 - 2R,$$

$R \in E(\mathbb{F}_q)$.

Main result

- Any genus 2 double cover H of curve E is given by equation
$$z^2 = f, \quad \mathrm{div}(f) = P_1 + P_2 - 2R,$$
$R \in E(\mathbb{F}_q)$.
- $$R \mapsto \mathcal{O},$$
$$P_1 \mapsto P_1 - R + \mathcal{O},$$
$$P_2 \mapsto -P_1 - R + \mathcal{O}$$
$$\Downarrow$$
$$\{\text{ double cover } z^2 = f\} \cong \{\text{ double cover } w^2 = g\},$$
$$\mathrm{div}(g) = P + (-P) - 2\mathcal{O}.$$

Main result

- $$\{\text{genus 2 double covers of } E\}$$
  $$\updownarrow$$
  $$\{\text{pairs of points } \{P, -P\} \notin E[2]\}$$

Main result

- $$\{\text{genus 2 double covers of } E\}$$
  $$\updownarrow$$
  $$\{\text{pairs of points } \{P, -P\} \notin E[2]\}$$

- If $\{H \to E\} \quad \longleftrightarrow \quad \{P, -P\}$, then
  $$H : z^2 = f, \quad \mathrm{div}(f) = (R + P) + (R - P) - 2R,$$
  $R \in E(\mathbb{F}_q)$.

Main result

- $$H_1 \leftrightarrow \{P_1, -P_1\}, \quad H_2 \leftrightarrow \{P_2, -P_2\}, \quad H_3 \leftrightarrow \{P_3, -P_3\}.$$

Main result

- $$H_1 \leftrightarrow \{P_1, -P_1\}, \quad H_2 \leftrightarrow \{P_2, -P_2\}, \quad H_3 \leftrightarrow \{P_3, -P_3\}.$$

- $$H_1 : z_1^2 = f_1, \quad \mathrm{div}(f_1) = (R_1 + P_1) + (R_1 - P_1) - 2R_1;$$
$$H_2 : z_2^2 = f_2, \quad \mathrm{div}(f_2) = (R_2 + P_2) + (R_2 - P_2) - 2R_2;$$
$$H_3 : z_3^2 = f_3, \quad \mathrm{div}(f_3) = (R_3 + P_3) + (R_3 - P_3) - 2R_3.$$

Main result

- $$H_1 \leftrightarrow \{P_1, -P_1\}, \quad H_2 \leftrightarrow \{P_2, -P_2\}, \quad H_3 \leftrightarrow \{P_3, -P_3\}.$$

- $$H_1 : z_1^2 = f_1, \quad \mathrm{div}(f_1) = (R_1 + P_1) + (R_1 - P_1) - 2R_1;$$
$$H_2 : z_2^2 = f_2, \quad \mathrm{div}(f_2) = (R_2 + P_2) + (R_2 - P_2) - 2R_2;$$
$$H_3 : z_3^2 = f_3, \quad \mathrm{div}(f_3) = (R_3 + P_3) + (R_3 - P_3) - 2R_3.$$

- $$\left.\begin{aligned} R_1 + P_1 &= R_2 - P_2 \\ R_2 + P_2 &= R_3 - P_3 \\ R_3 + P_3 &= R_1 - P_1 \end{aligned}\right\} \Rightarrow 2(P_1 + P_2 + P_3) = \mathcal{O}.$$

Main result

- Consider an elliptic curve E with $d(E) = -19$. This curve is unique up to isomorphism.

Main result

- Consider an elliptic curve E with $d(E) = -19$. This curve is unique up to isomorphism.
- Let $H \cong E \times E'$, $E' \cong E$.

Main result

- Consider an elliptic curve E with $d(E) = -19$. This curve is unique up to isomorphism.
- Let $H \cong E \times E'$, $E' \cong E$.
- If $E/\mathbb{F}_p : y^2 = f(x)$, then $E'/\mathbb{F}_p : y^2 = (\alpha x + \beta)f(x)$.

Main result

- Consider an elliptic curve E with $d(E) = -19$. This curve is unique up to isomorphism.
- Let $H \cong E \times E'$, $E' \cong E$.
- If $E/\mathbb{F}_p : y^2 = f(x)$, then $E'/\mathbb{F}_p : y^2 = (\alpha x + \beta)f(x)$.
- $\exists \varphi \in \mathrm{Aut}_{\mathbb{F}_p}(E)$, $\varphi : E \to E'$:

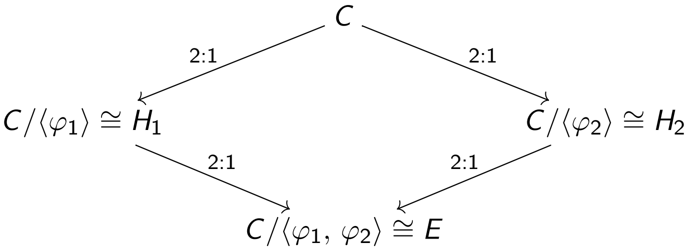
$$\varphi : \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ \infty \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \\ x_0 \\ -\beta/\alpha \end{pmatrix} \quad \text{or} \quad \varphi : \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ \infty \end{pmatrix} = \begin{pmatrix} x_2 \\ x_0 \\ x_1 \\ -\beta/\alpha \end{pmatrix}.$$

Therefore there are at most two coverings $H \to E$ up to isomorphism.

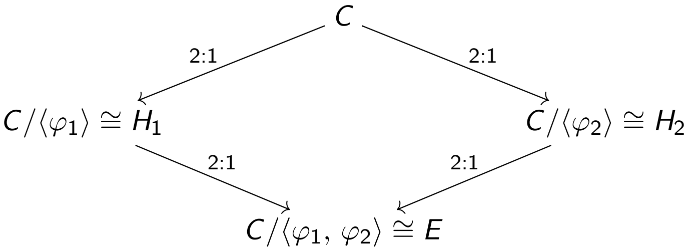
Main result

- $\{P_1, -P_1\}$ and $\{P_2, -P_2\}$ give this covers.

Main result

- $\{P_1, -P_1\}$ and $\{P_2, -P_2\}$ give this covers.
- 

Main result

- $\{P_1, -P_1\}$ and $\{P_2, -P_2\}$ give this covers.
- 

- $$\left.\begin{aligned} 6P_1 &= \mathcal{O} \\ 6P_2 &= \mathcal{O} \\ 4P_1 + 2P_2 &= \mathcal{O} \\ 2P_1 + 4P_2 &= \mathcal{O} \end{aligned}\right\} \Rightarrow \begin{aligned} P_1 = Q + S, &\quad \operatorname{ord} Q = 3, \operatorname{ord} S = 2. \\ P_2 = Q + T, &\quad \operatorname{ord} Q = 3, \operatorname{ord} T = 2. \end{aligned}$$

Example

- $E/\mathbb{F}_5 : y^2 = x^3 + 2x + 4.$
- $H_1/\mathbb{F}_5 : w^2 = x,\ H_2/\mathbb{F}_5 : z^2 = y + x^2 + 2x + 3.$

Example

- $E/\mathbb{F}_5 : y^2 = x^3 + 2x + 4.$
- $H_1/\mathbb{F}_5 : w^2 = x,\ H_2/\mathbb{F}_5 : z^2 = y + x^2 + 2x + 3.$
- Optimal curve of genus 4 over $\mathbb{F}_{5^7}$:

$$z^4 + 3z^2w^4 + z^2w^2 + 4z^2 + w^8 + 3w^6 = 0.$$

Thank you for your attention!