Fourteenth International Workshop on Algebraic and Combinatorial Coding Theory
September 7–13, 2014, Svetlogorsk (Kaliningrad region), Russia *pp. 14–17*

A method of finding explicit equation for optimal curve of genus 4 [1]

Ekaterina Alekseenko ealekseenko@kantiana.ru
I. Kant Baltic Federal University, Kaliningrad, Russia

Abstract. In this paper we deduce a new method of finding of an equation for an optimal curve of genus 4. This curve is obtained as a double cover of an optimal elliptic curve which is defined over an extension of prime finite field.

1 Main result

We start with reminding that by an optimal curve we mean a curve whose number of rational points reaches the Hasse-Weil-Serre bound (cf. details in [1]).

Let's consider an optimal elliptic curve E over a finite field $\mathbb{F}_q$ which given by equation

$$y^2 = x^3 + ax + b.$$

Let H be a curve of genus 2 over a finite field $\mathbb{F}_q$ and let $f : H \to E$ be a double covering of H.

Set $\mathcal{O} = f^{-1}(\infty') = \sum_{P|\infty'} e(P|\infty') \cdot P \in \mathrm{Div}(H)$, where $\infty' \in E$ lies over $\infty \in \mathbb{P}^1$ by the action $E \to \mathbb{P}^1$ and $\deg\mathcal{O} = 2$.

Consider the divisor $4\mathcal{O}$. By the Clifford's theorem $\dim 4\mathcal{O} \leq 5$ and applying the method which was described in paper [1] we have $L(4\mathcal{O}) = \{1, x, x^2, y\}$ and double cover H of genus 2 has the equation

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

It is known that the double cover is ramified over two points of curve E. Let P_1 and P_2 be these points. So the cover H is given by $z^2 = f$ for a function f on the curve E. Then by the Hurwitz-Riemann formula it follows

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

for some divisor D of degree -1 on E. By corollary 3.5 [2] there exist a point Q and a function g on E so that

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

[1] This research is partially supported by grant of Dynasty Foundation (2013)

where $\mathcal{O}$ is a point in infinity. Then $D + \mathrm{div}(g) = Q - 2\mathcal{O}$.

We have $z^2 = f$, therefore $(zg)^2 = fg^2$ and holds following

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

If we set $fg^2 = h$, $zg = w$, then the cover with the equation $w^2 = h$ is the cover H. As $\mathrm{div}(h) = P_1 + P_2 + 2Q - 4\mathcal{O}$, then $h \in L(4\mathcal{O}) = \{1, x, x^2, y\}$. So any genus 2 double cover H of curve E is given by equation

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

with R is the rational point of E. By changing coordinates

$$R \mapsto \mathcal{O},$$

$$P_1 \mapsto P_1 - R + \mathcal{O},$$

$$P_2 \mapsto -P_1 - R + \mathcal{O}$$

the double cover with the equation $z^2 = f$ will be isomorphic to double cover given by $w^2 = g$ with $\mathrm{div}(g) = P + (-P) - 2\mathcal{O}$. We get the following correspondence

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

If the cover $H \to E$ corresponds to $\{P, -P\}$, then the cover H is given by equation

$$z^2 = f \quad \text{with } \mathrm{div}(f) = (R + P) + (R - P) - 2R \text{ for some point } R$$

up to isomorphism over E.

Set H_1, H_2 and H_3 are double covers of E. And the following correspondences hold

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

Then

$$H_1 : z_1^2 = f_1, \quad \mathrm{div}(f_1) = (R_1 + P_1) + (R_1 - P_1) - 2R_1;$$

$$H_2 : z_2^2 = f_2, \quad \mathrm{div}(f_2) = (R_2 + P_2) + (R_2 - P_2) - 2R_2;$$

$$H_3 : z_3^2 = f_3, \quad \mathrm{div}(f_3) = (R_3 + P_3) + (R_3 - P_3) - 2R_3.$$

Since f_1, f_2,f_3 are squares, we have the following equalities up to choice of sign

$$R_1 + P_1 = R_2 - P_2,$$

$$R_2 + P_2 = R_3 - P_3,$$

$$R_3 + P_3 = R_1 - P_1.$$

So $2(P_1 + P_2 + P_3) = \mathcal{O}$.

Let us consider an elliptic curve E with $d(E) = -19$. This curve is unique up to isomorphism and let H be genus 2 curve such that $H \cong E \times E'$ and $E' \cong E$. If the curve E is given by equation $y^2 = f(x)$ with irreducible polynomial $f(x)$ over $\mathbb{F}_q$, then the curve E' has the equation $y^2 = (\alpha x + \beta) f(x)$ where $\alpha, \beta \in \mathbb{F}_q$ (see Proposition 4.4. [3]). There exists an automorphism $\varphi \in \mathrm{Aut}_{\mathbb{F}_q}(E)$, $\varphi : E \to E'$. It commutes with Frobenius and acts on the roots x_0, x_1, x_2 in the extension $\mathbb{F}_q$ as following

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

or

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

Obviously that an order of φ is 3. Therefore there are at most two covers $H \to E$ up to isomorphism. We set that pairs of points $\{P_1, -P_1\}$ и $\{P_2, -P_2\}$ give this covers. Considering some combination of these covers we can fit them in a diagram

$$\begin{tikzcd} & C \arrow[dl, "2:1"'] \arrow[dr, "2:1"] & \\ C/\langle\sigma\rangle \cong H_1 \arrow[dr, "2:1"'] & & C/\langle\delta\rangle \cong H_2 \arrow[dl, "2:1"] \\ & C/\langle\sigma,\, \delta\rangle \cong E & \end{tikzcd}$$

Up to choice of sign we obtain correspondences

$$6P_1 = \mathcal{O},$$

$$6P_2 = \mathcal{O},$$

$$4P_1 + 2P_2 = \mathcal{O},$$

$$2P_1 + 4P_2 = \mathcal{O}.$$

By looking at curves E and H in the fields of characteristic 0, we can see when these equations hold by module p. Then we can get finite list of characteristics.

Example 1. Consider an elliptic curve

$$E : y^2 = x^3 + 2x + 4$$

over $\mathbb{F}_5$ and two genus 2 double covers

$$w^2 = x, \quad z^2 = y + x^2 + 2x + 3.$$

By checking we have that the Weil polynomial of the compositium curve of genus 4 is equal

$$(T^2 + T + 5)^5,$$

and the characteristic polynomial with discriminant -19 over $\mathbb{F}_{5^7}$ is equal

$$(T^2 - 559T + 78125)^4.$$

Therefore the curve is given by the equation

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

is an optimal curve of genus 4 over a finite field with discriminant -19.

References

[1] 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.

[2] J. H. Silverman, The arithmetic of elliptic curves, New York, etc.:Springer-Verlag, GTM 106, 1986.

[3] A. Zaytsev, Optimal curves of low genus over finite fields, *http://arxiv.org/abs/0706.4203,* 2007.