представительное множество. Оно может быть найдено путём попарного сравнения частотных классов системы $\mathfrak{K}$ по отношению представительности с использованием леммы 3. Мощность системы $\mathfrak{K}$ ограничена числом частотных классов с длиной слов не выше l, которое не превосходит $l^{|A|}$, где $|A|$ — мощность алфавита A, а число пар классов из $\mathfrak{K}$ не больше $l^{2|A|}$. Поскольку $|A|$ — константа, а трудоёмкость сравнения одной пары по представительности полиномиальна, процедура выделения минимального представительного множества полиномиальна по l. ■

ЛИТЕРАТУРА

1. *Шоломов Л. А.* Элементы теории недоопределённой информации // Прикладная дискретная математика. Приложение. 2009. № 2. С. 18–42.
2. *Шоломов Л. А.* О функционалах, характеризующих сложность систем недоопределенных булевых функций // Проблемы кибернетики. Вып. 19. М.: Физматлит, 1967. С. 123–139.
3. *Нечипорук Э. И.* О сложности вентильных схем, реализующих булевские матрицы с неопределенными элементами // ДАН СССР. 1965. Т. 163. № 1. С. 40–42.
4. *Адельсон-Вельский Г. М., Диниц Е. А., Карзанов А. В.* Потоковые алгоритмы. М.: Наука, 1975.

UDC 512.772.7 DOI 10.17223/2226308X/12/12

CHARACTERISTIC POLYNOMIALS OF THE CURVE $y^2 = x^7 + ax^4 + bx$ OVER FINITE FIELDS

S. A. Novoselov[1], Y. F. Boltnev

In this work, we list all possible characteristic polynomials of the Frobenius endomorphism for genus 3 hyperelliptic curves of type $y^2 = x^7 + ax^4 + bx$ over finite field $\mathbb{F}_q$ of characteristic $p > 3$.

Keywords: *hyperelliptic curves, characteristic polynomials, point-counting, genus* 3.

Introduction

Let $\mathbb{F}_q$ be a finite field of size $q = p^n$, $p > 2$. In this note, we study the hyperelliptic curves of genus $g = 3$ of the form

$$C : y^2 = x^{2g+1} + ax^{g+1} + bx.$$

The Jacobian J_C of the curves is split [1] over certain finite field extension:

$$J_C \sim J_{D_1} \times J_{D_2},$$

where D_1 and D_2 are explicitly given curves. This fact allows us to reduce the problem of point-counting on the curve C to counting points on the curves D_1 and D_2.

For genus 2 case it was done in the works [2, 3]. The work [1] contains algorithms for $g > 2$ case. In this work, we give explicit formulae for the number of points on the Jacobian in the case of $g = 3$.

The point-counting on the curve is equivalent to finding of zeta-function of the curve

$$Z(C/\mathbb{F}_q;T) = \exp\left(\sum_{k=1}^{\infty} \#C(\mathbb{F}_{q^k})\frac{T^k}{k}\right) = \frac{L_{C,q}(T)}{(1-T)(1-qT)},$$

[1]The author is supported by RFBR according to the research project No. 18-31-00244.

where $L_{C,q}(T) = q^g T^{2g} + a_1 q^{g-1} T^{2g-1} + \ldots + a_g T^g + a_{g-1} T^{g-1} + \ldots + a_1 T + 1$ and $a_i \in \mathbb{Z}$, $|a_i| \leqslant \binom{2g}{i} q^{i/2}$ for $i = 1, \ldots, g$.

Let $\chi_{C,q}(T)$ be a characteristic polynomial of the Frobenius endomorphism. Then $L_{C,q}(T) = T^{2g}\chi_{C,q}(1/T)$ and $\#J_C(\mathbb{F}_q) = L_{C,q}(1) = \chi_{C,q}(1)$. Therefore, the computation of $\#J_C(\mathbb{F}_q)$ is equivalent to the computation of the characteristic polynomial.

In this work, we enumerate all possible characteristic polynomials for the curve C in the case of $g = 3$.

1. Characteristic polynomials for genus 3 curves

Let $C : y^2 = x^7 + ax^4 + bx$ be a genus 3 hyperelliptic curve defined over a finite field $\mathbb{F}_q$, $q = p^n$, $p > 3$. Since, there is a map

$$(x, y) \mapsto (x^3, xy)$$

from C to an elliptic curve $E_1 : y^2 = x^3 + ax^2 + bx$, we have

$$J_C \sim E_1 \times A$$

over $\mathbb{F}_q$ for some abelian surface A. Therefore,

$$\chi_{C,q}(T) = \chi_{E_1,q}(T)\chi_{A,q}(T).$$

The characteristic polynomial for E_1 can be efficiently computed using SEA-algorithm [4]. So, we only have to determine the coefficients of $\chi_{A,q}(T) = T^4 - b_1 T^3 + b_2 T^2 - b_1 q T + q^2$.

From [1, Th. 2], we have

$$J_C \sim E_2 \times J_D$$

over $\mathbb{F}_q[\sqrt[3]{b}]$, where E_2 is an elliptic curve with equation

$$y^2 = x^3 - 3\sqrt[3]{b}x + a$$

and D is a hyperelliptic curve with equation

$$y^2 = (x^2 - 4\sqrt[3]{b})(x^3 - 3\sqrt[3]{b}x + a).$$

Moreover, the Jacobian J_D is also split, since $E_1 \not\sim E_2$ in general.

First we describe the characteristic polynomials in the simplest case when b is a cubic residue. In this case for each cubic root, we have a map to an elliptic curve, so we obtain the following theorem.

Theorem 1. Let $C : y^2 = x^7 + ax^4 + bx$ be a genus 3 hyperelliptic curve defined over a finite field $\mathbb{F}_q$, $q = p^n$, $p > 3$, and let b be a cubic residue. Then

1) if $q \equiv 1 \pmod 6$, then $J_C \sim E_1 \times E_2^2$ over $\mathbb{F}_q$ and

$$\chi_{C,q}(T) = (T^2 - t_1 T + q)(T^2 - t_2 T + q)^2,$$

where $E_1 : y^2 = x^3 + ax^2 + bx$, $E_2 : y^2 = x^3 - 3\sqrt[3]{b}x + a$ are elliptic curves and t_1, t_2 are their traces of the Frobenius endomorphism;

2) if $q \equiv 5 \pmod 6$, then $J_C \sim E_1 \times E_2 \times \tilde{E}_2$ over $\mathbb{F}_q$ and

$$\chi_{C,q}(T) = (T^2 - t_1 T + q)(T^2 - t_2 T + q)(T^2 + t_2 T + q),$$

where $\tilde{E}_2$ is a quadratic twist of E_2.

In general case, we have $J_C \sim E_1 \times A$, where A can be simple.

Theorem 2. Let $C : y^2 = x^7 + ax^4 + bx$ be a genus 3 hyperelliptic curve defined over a finite field $\mathbb{F}_q$, $q = p^n$, $p > 3$. Then

1) $J_C \sim E_1 \times A$ over $\mathbb{F}_q$, where E_1 is an elliptic curve with equation $y^2 = x^3 + ax^2 + bx$ and A is an abelian surface;
2) if $q \equiv 5 \pmod 6$, we have $J_C \sim E_1 \times E_2 \times \tilde{E}_2$ and
$$\chi_{C,q}(T) = (T^2 - t_1T + q)(T^2 - t_2T + q)(T^2 + t_2T + q),$$
where E_1, E_2, t_1, t_2 are the same as in Theorem 1;
3) if $q \equiv 1 \pmod 6$ and $\sqrt[3]{b} \in \mathbb{F}_q$, then $J_C \sim E_1 \times E_2^2$ over $\mathbb{F}_q$ and
$$\chi_{C,q}(T) = (T^2 - t_1T + q)(T^2 - t_2T + q)^2;$$
4) if $q \equiv 1 \pmod 6$, $\sqrt[3]{b} \notin \mathbb{F}_q$ and E_2 is ordinary, then $\chi_{C,q}(T) = (T^2 - t_1T + q)\chi_A(T)$, where $\chi_A(T)$ is one of the following polynomials:
   - $(T^4 - \tilde{t}_2T^3 + (\tilde{t}_2^2 - q)T^2 - \tilde{t}_2qT + q^2)$, $\sqrt{b} \notin \mathbb{F}_q$;
   - $(T^4 + \tilde{t}_2T^3 + (\tilde{t}_2^2 - q)T^2 + \tilde{t}_2qT + q^2)$, $\sqrt{b} \in \mathbb{F}_q$;
   - $(T^4 - 2\tilde{t}_2T^3 + (\tilde{t}_2^2 + 2q)T^2 - 2\tilde{t}_2qT + q^2)$, $\sqrt{b} \notin \mathbb{F}_q$, A is split;
   - $(T^4 + 2\tilde{t}_2T^3 + (\tilde{t}_2^2 + 2q)T^2 + 2\tilde{t}_2qT + q^2)$, $\sqrt{b} \in \mathbb{F}_q$, A is split.

   Here, $\tilde{t}_2$ is a trace of Frobenius of elliptic curve $\tilde{E}_2 : y^2 = x^3 - 3bx + ab$;
5) if $q \equiv 1 \pmod 6$, $\sqrt[3]{b} \notin \mathbb{F}_q$ and E_2 is supersingular, then A is supersingular and $\chi_{C,q}(T) = (T^2 - t_1T + q)\chi_{A,q}(T)$ where $\chi_{A,q}(T)$ is one of the following polynomials:
   - $(T^4 - qT^2 + q^2)$;
   - $(T^4 + 2qT^2 + q^2)$;
   - $(T^2 + q)(T \pm \sqrt{q})^2$, $p \equiv 7 \pmod{12}$, n is even, A is split;
   - $(T \pm \sqrt{q})^2$, n is even, A is split;
   - $(T^2 \pm T\sqrt{q} + q)^2$, n is even, A is simple;
   - $(T^4 + \sqrt{q}T^3 + qT^2 + q^{3/2}T + q^2)$, $p \not\equiv 1 \pmod 5$, n is even, A is simple;
   - $(T^4 - \sqrt{q}T^3 + qT^2 - q^{3/2}T + q^2)$, $p \not\equiv 1 \pmod{10}$, n is even, A is simple.

Conclusion

In this work, we obtained the complete list of the characteristic polynomials for the genus 3 curve $y^2 = x^7 + ax^4 + bx$ in terms of traces of Frobenius of certain elliptic curves. Since $\#J_C(\mathbb{F}_q) = \chi_{C,q}(T)$, this gives us the explicit formulae for the number of points on the Jacobian.

REFERENCES

1. *Novoselov S. A.* Counting Points on Hyperelliptic Curves of Type $y^2 = x^{2g+1} + ax^{g+1} + bx$. `https://arxiv.org/abs/1902.05992`. 2019.
2. *Satoh T.* Generating genus two hyperelliptic curves over large characteristic finite fields. LNCS, 2009, vol. 5479, pp. 536–553.
3. *Guillevic A. and Vergnaud D.* Genus 2 hyperelliptic curve families with explicit Jacobian order evaluation and pairing-friendly constructions. LNCS, 2012, vol. 7708, pp. 234–253.
4. *Schoof R.* Counting points on elliptic curves over finite fields. J. de théorie des nombres de Bordeaux, 1995, vol. 7, no. 1, pp. 219–254.