sciendo

uniform distribution theory

DOI: 10.2478/UDT-2022-0010
Unif. Distrib. Theory **17** (2022), no.2, 1–20

LINEAR COMPLEXITY OF SEQUENCES ON KOBLITZ CURVES OF GENUS 2

Vishnupriya Anupindi

Johann Radon Institute for Computational and Applied Mathematics,
Austrian Academy of Sciences, Linz, AUSTRIA

ABSTRACT. In this paper, we consider the hyperelliptic analogue of the Frobenius endomorphism generator and show that it produces sequences with large linear complexity on the Jacobian of genus 2 curves.

Communicated by Arne Winterhof

1. Introduction

An important operation in elliptic curve based cryptosystems is to compute scalar multiples of a given group element. The standard method for computing scalar multiples is the *double-and-add-method*, but faster methods have been suggested by using the Frobenius endomorphism on special curves known as Koblitz curves, see [8, 17, 20, 21]. The ideas for fast computation of scalar multiples on elliptic Koblitz curves have been generalized to hyperelliptic curves of genus 2, see [5].

In [12], Lange and Shparlinski investigated the problem of choosing random elements from elliptic and hyperelliptic curves, see also [14, 16]. One can choose such elements by computing random scalar multiples of an initial element fixed in advance. However, Lange and Shparlinski [12], by taking advantage of fast

2020 Mathematics Subject Classification: 11G05, 11G20, 11K45, 11T71.
Keywords: elliptic curve, hyperelliptic curve, linear complexity, frobenius generator.
The author was supported by the Austrian Science Fund FWF Project P31762.

computation of scalar multiplication on Koblitz curves, introduced a more efficient and direct way to obtain random-looking elements, called *Frobenius endomorphism generator*.

In this paper, we study some properties of pseudorandomness of sequences derived from hyperelliptic curves of genus 2 using the Frobenius endomorphism generator. In particular, we investigate the level of randomness of such sequences in terms of linear complexity. We recall, that the *linear complexity* of a sequence (s_n) of length N over the finite field $\mathbb{F}_q$ is defined as the smallest non-negative integer L such that the first N terms of the sequence (s_n) can be generated by a linear recurrence relation over $\mathbb{F}_q$ of order L, i.e., there exist

$$c_0, c_1, \dots, c_{L-1} \in \mathbb{F}_q$$

such that

$$s_{n+L} = c_0 s_n + c_1 s_{n+1} + \cdots + c_{L-1} s_{n+L-1}, \qquad 0 \le n \le N - L - 1.$$

The linear complexity measures the unpredictability of a sequence, hence for applications in cryptography, a large linear complexity is desired. However, a large linear complexity is not a sufficient condition for the unpredictability of a sequence. For more details, see [15, 19, 23].

In Section 2, we recall some properties of hyperelliptic curves and in Section 3, we define the Frobenius endomorphism generator and state the main result. In Section 4, we collect auxiliary results which are used in the proof. In particular, we recall the Grant representation [4] of the Jacobian of a hyperelliptic curve of genus 2 and some results from [1]. Finally, in Section 5, we prove the main result.

2. Hyperelliptic curves

Let $\mathbb{F}_q$ be a finite field with characteristic $p \ge 3$ and $\mathbb{F}_{q^n}$ be an extension field of $\mathbb{F}_q$ with $n \ge 1$. Let $\overline{\mathbb{F}}_q$ be the algebraic closure of $\mathbb{F}_q$.

2.1. Points on hyperelliptic curves

Let C be a hyperelliptic curve of genus $g \ge 1$ defined over the base field $\mathbb{F}_q$ by

$$C : Y^2 = h(X), \tag{1}$$

where $h(X) \in \mathbb{F}_q[X]$ is a polynomial of degree $2g+1$. For details on hyperelliptic curves, see [2, 3, 9]. We denote the $\mathbb{F}_{q^n}$-rational points of C by $C(\mathbb{F}_{q^n})$, which are the solutions over $\mathbb{F}_{q^n}$ of the defining equation (1) together with a point $\mathcal{O}$ at infinity. By the Hasse-Weil bound [22, Theorem 5.2.3], we have

$$\big| |C(\mathbb{F}_{q^n})| - (q^n + 1) \big| \le 2g q^{n/2}. \tag{2}$$

2.2. Jacobian of hyperelliptic curves

For an affine point $P = (x, y) \in C$, we write $-P = (x, -y)$ and $-\mathcal{O} = \mathcal{O}$ for the point at infinity. A *divisor* D of C is an element of the free abelian group over the points of C, e.g., $D = \sum_{P \in C} n_P P$ with $n_P \in \mathbb{Z}$ and $n_P = 0$ for almost all points P. A *reduced divisor* is given by

$$D = P_1 + \cdots + P_r - r\mathcal{O}, \tag{3}$$

where

$$1 \leq r \leq g, \quad P_1, \ldots, P_r \in C, \quad P_i \neq \mathcal{O} \quad \text{for } 1 \leq i \leq r$$

and

$$P_i \neq -P_j \quad \text{for } 1 \leq i < j \leq r.$$

The *Jacobian* J_C of the curve C is the set of reduced divisors. One can define an addition operation on the set of reduced divisors, denoted by $+$, with the identity element $\mathcal{O}$, which makes J_C into a group. The elements of the curve $C(\mathbb{F}_q)$ are represented in the Jacobian by the set

$$\Theta(\mathbb{F}_q) = \{D \in J_C(\mathbb{F}_q) : D = P - \mathcal{O}, P \in C(\mathbb{F}_q)\} \cup \{\mathcal{O}\}. \tag{4}$$

We also write $\Theta = \Theta(\overline{\mathbb{F}}_q)$.

The Frobenius endomorphism $\sigma : \overline{\mathbb{F}}_q \to \overline{\mathbb{F}}_q, x \mapsto x^q$, extends naturally to points on C, where

$$\sigma((x, y)) = (x^q, y^q) \qquad \text{and} \qquad \sigma(\mathcal{O}) = \mathcal{O}.$$

For

$$D = \textstyle\sum_{i=1}^r P_i - r\mathcal{O} \in J_C, \qquad \text{define} \qquad \sigma(D) = \textstyle\sum_{i=1}^r \sigma(P_i) - r\mathcal{O}.$$

An element $D \in J_C$ as given in (3) is said to be defined over $\mathbb{F}_q$ if $\sigma(D)$ permutes the set $\{P_1, \ldots, P_r\}$. We use $J_C(\mathbb{F}_q)$ to denote the set of elements of J_C which are defined over $\mathbb{F}_q$.

The characteristic polynomial, $\chi_C(T)$ of the Frobenius endomorphism σ is a degree $2g$ polynomial with integer coefficients of the following form

$$\chi_C(T) = T^{2g} + s_1 T^{2g-1} + \cdots + s_g T^g + \cdots + s_1 q^{g-1} T + q^g, s_i \in \mathbb{Z}. \tag{5}$$

It follows from the Hasse-Weil Theorem [22, Theorem 5.1.15 and 5.2.1], that the complex roots τ_i of χ_C have absolute value $|\tau_i| = q^{1/2}, i = 1, \ldots, 2g$. For any extension degree n, the cardinality of $J_C(\mathbb{F}_{q^n})$ is given by

$$|J_C(\mathbb{F}_{q^n})| = \prod_{i=1}^{2g} (1 - \tau_i^n). \tag{6}$$

In particular, we have

$$(q^{n/2} - 1)^{2g} \leq |J_C(\mathbb{F}_{q^n})| \leq (q^{n/2} + 1)^{2g}, \; n \geq 1. \tag{7}$$

2.3. Mumford representation

A compact representation of elements of the Jacobian J_C is given by the *Mumford representation* [18] using a pair of polynomials $[u, v] \in \mathbb{F}_q[X] \times \mathbb{F}_q[X]$. For a reduced divisor $D = \sum_{i=1}^{r} P_i - r\mathcal{O}$ with $P_i = (x_i, y_i)$ the Mumford representation is given by $u = \prod_{i=1}^{r}(X - x_i)$ and v such that v interpolates the points P_i respecting multiplicities. In particular,

(a) u is monic,

(b) u divides $f - v^2$,

(c) $\deg(v) < \deg(u) \le g$.

For genus $g = 2$, a generic element $D = P_1 + P_2 - 2\mathcal{O}$ is represented by the polynomials

$$u = x^2 + u_1 x + u_0,\ v = v_1 x + v_0,\ u_i, v_i \in \mathbb{F}_{q^n}, i \in \{0, 1\} \text{ such that } D = [u, v]. \quad (8)$$

3. Koblitz curves and fast generation of elements in Jacobian

By a hyperelliptic *Koblitz curve*, we refer to a hyperelliptic curve that is defined over a small finite field and is considered over a large extension field. In this work, we avoid fields with characteristic 2 for technical reasons. For Koblitz curves, it is recommended to choose base fields $q \le 7$ for computational advantage, see [11]. However, we do not impose this restriction for our result.

For fast generation of elements in the Jacobian $J_C(\mathbb{F}_{q^n})$, Lange and Shparlinski in [12] introduced the following method using the Frobenius endomorphism. Here we restrict ourselves to the genus 2 case. Let

$$\mathcal{R} = \{0, \pm 1, \ldots, \pm (q^2 - 1)/2\}$$

represent the set $\mathbb{Z}/q^2\mathbb{Z}$. Let $D \in J_C(\mathbb{F}_{q^n})$ be an element of order ℓ. For fixed $k \le n$, consider the element of J_C defined as follows

$$D_{\boldsymbol{m}} = \sum_{j=0}^{k-1} m_j \sigma^j(D), \quad \boldsymbol{m} = (m_0, \ldots, m_{k-1}) \in \mathcal{R}^k. \quad (9)$$

It is natural to expect that the divisors $D_{\boldsymbol{m}}$ defined by (9) are sufficiently uniformly distributed. Lange and Shparlinski [12] showed that $D_{\boldsymbol{m}}$ do not take the same value too often (which would otherwise have catastrophic implications for their cryptographic applications).

In this paper we further investigate the randomness properties of $D_{\boldsymbol{m}}$. Namely, we show that different statistics of the divisors $D_{\boldsymbol{m}}$, like the Mumford coordinates u_i, v_i as in (8), possess large linear complexity if the divisors $D_{\boldsymbol{m}}$ are arranged in a natural way, say in lexicographic ordering. More precisely, let $f \in \mathbb{F}_{q^n}(J_C)$ be a rational function in the function field of the Jacobian. We arrange the elements of $\mathcal{R}^k$ with a lexicographic ordering and define the sequence $(w_{\boldsymbol{m}})_{\boldsymbol{m}\in\mathcal{R}^k}$ with

$$w_{\boldsymbol{m}} = \begin{cases} f(D_{\boldsymbol{m}}) & \text{if } D_{\boldsymbol{m}} \text{ is not a pole of } f, \\ 0, & \text{otherwise.} \end{cases} \tag{10}$$

Throughout the paper, $U \ll V$ is equivalent to the inequality $|U| \le cV$ with some constant $c > 0$. Our main result is the following bound on the linear complexity of $(w_{\boldsymbol{m}})_{\boldsymbol{m}\in\mathcal{R}^k}$.

Theorem 3.1. *Let C be a hyperelliptic curve of genus 2, defined over the base field $\mathbb{F}_q$ and let $J_C(\mathbb{F}_{q^n})$ be its Jacobian over the extension field $\mathbb{F}_{q^n}$. Let the characteristic polynomial of the Frobenius endomorphism χ_C be irreducible. Let $f \in \mathbb{F}_{q^n}(J_C)$ be a rational function with pole divisor of the form $\alpha\Theta$, $\alpha \in \mathbb{Z}, \alpha \ge 1$. If $D \in J_C(\mathbb{F}_{q^n})$ is of prime order $\ell, \ell \nmid q^2$, then for any k, where $1 \le k \le n$ with $(w_{\boldsymbol{m}})_{\boldsymbol{m}\in\mathcal{R}^k}$ as defined in (10), we have*

$$L(w_{\boldsymbol{m}}) \gg \frac{\min\{q^{3k/2}, \ell/q^8\}}{q^n \deg f}. \tag{11}$$

The result is non-trivial if $k \ge 2n/3$ and $\ell \ge q^{n+8}$. In the ideal case, $k = n$, $\deg f = 1$ and $\ell \sim q^{2n}$, we obtain $L(w_{\boldsymbol{m}}) > cq^{n/2}$ for some constant which may depend on $\deg f$. Examples for rational functions with $\deg f = 1$ are the Mumford coordinates (8).

We assume the characteristic polynomial of Frobenius endomorphism χ_C to be irreducible, in particular, χ_C is irreducible over $\mathbb{Z}$. Practically, this is the most interesting case, since, by (6) any non-trivial factor of χ_C leads to a non-trivial factor of the group order, which we want to avoid.

We remark, that in (9), if we replace the Frobenius map σ with the multiplication map $[2] : D \mapsto 2D$, and if we use colexicographic ordering for arranging sequence elements $D_{\boldsymbol{m}}$, then we are in the linear congruential generator case, for which we proved a stronger bound in [1].

We also remark, that Lange and Shparlinski [12, 14] defined and investigated the randomness properties of similar, but not completely analogous point-set for the elliptic curve case. Later, Mérai [16] studied the randomness properties of a sequence of elements from this point set, by arranging elements in a sequence using lexicographic ordering.

The proof of Theorem 3.1 is based on the method of [16], the results of [12] and taking advantage of the explicit addition formulas for genus 2 provided by Grant [4].

4. Preparation

The aim of this section is to collect some technical results for the proof of the main theorem. We use the *Grant representation* of a hyperelliptic curve of genus 2 since it provides explicit addition formulas. This allows us to prove the degree estimate in Proposition 4.4.

4.1. Arithmetic for genus 2 using Grant representation

In order to implement the group law $(Q, R) \mapsto Q + R$ on the Jacobian, one can use Cantor's algorithm which uses the Mumford representation. However, this algorithm is implicit. In this work, we use the explicit addition formulas provided by Grant [4, Theorem 3.3].

Let C be the hyperelliptic curve of genus $g = 2$ defined by (1) with

$$h(X) = X^5 + b_1X^4 + b_2X^3 + b_3X^2 + b_4X + b_5 \in \mathbb{F}_q[X],$$

for the finite field $\mathbb{F}_q$ with characteristic $p \geq 3$. In [4], Grant provides an embedding of J_C into the projective space $\mathbb{P}^8$.

Let

$$\mathbb{F}_q[\mathbf{Z}] = \mathbb{F}_q[Z_{11}, Z_{12}, Z_{22}, Z_{111}, Z_{112}, Z_{122}, Z_{222}, Z] \tag{12}$$

be a polynomial ring over $\mathbb{F}_q$ in 8 variables. The following proposition gives us a set of defining equations for the Jacobian, see [4, Corollary 2.15].

Proposition 4.1. *There are polynomials $f_1, \ldots, f_{13} \in \mathbb{F}_q[\mathbf{Z}]$ such that*

$$J_C \cong V\big(f_1^h, \ldots, f_{13}^h\big) = \big\{z \in \mathbb{P}^8 : f_i^h(z) = 0, 1 \leq i \leq 13\big\},$$

where f_i^h denotes the homogenized polynomial with respect to the variable Z_0.

Moreover, an embedding $\iota : J_C \to \mathbb{P}^8$ is given by

$$\iota(D) = \begin{cases} (1 : z_{11} : z_{12} : z_{22} : z_{111} : z_{112} : z_{122} : z_{222} : z) & \text{if } D \in J_C \setminus \Theta, \\ (0:0:0:0:1:0:0:0:0) & \text{if } D = \mathcal{O}, \\ (0:0:0:0:-x^3:-x^2:-x:1:-y) & \text{if } D = P - \mathcal{O} \in \Theta \setminus \mathcal{O}, \end{cases} \tag{13}$$

where $P = (x, y)$.

See Appendix A.1 for the polynomial expressions of $f_1, \dots, f_{13}$ in the same notation as used in this work. For $D = (x_1, y_1) + (x_2, y_2) - 2\mathcal{O} \in J_C(\mathbb{F}_q) \setminus \Theta(\mathbb{F}_q)$, the components z_{jk}, z_{jkl} of $\iota(D)$ can be expressed as rational functions in the coordinates (x_1, y_1) and (x_2, y_2).

We denote the affine part of J_C with respect to variable Z_0 under ι by U. Then $U = J_C \setminus \Theta$. Moreover, by [4, Theorem 2.5], we have

$$U \cong V(f_1, \dots, f_6). \tag{14}$$

Since J_C is irreducible and has dimension 2, it follows that U is irreducible, dense, and has dimension 2, see [6, Example 1.1.3]. As a result, $\mathbb{F}_q(U) = \mathbb{F}_q(J_C)$, see [6, Theorem 3.4].

For a rational function $h \in \mathbb{F}_q(U)$, we define its degree by choosing a representative element $\frac{h_1}{h_2}$ of the equivalence class h, such that $\deg h_1$ is minimal and set

$$\deg h = \max\{\deg h_1, \deg h_2\}.$$

We summarize the algebraic properties of the group law in the Grant representation. For explicit expressions, see Appendix A.2.

Lemma 4.2. *Assume that $Q, R, Q+R, Q-R \in U$. Let*

$$\mathfrak{q}(Q,R) = z_{11}(Q) - z_{11}(R) + z_{12}(Q)z_{22}(R) - z_{12}(R)z_{22}(Q). \tag{15}$$

Then there are explicit formulas for

$$z_{jk}(Q+R), \quad z_{jkl}(Q+R)$$

which are rational functions in

$$z_{jk}(Q), \quad z_{jk}(R), \quad z_{jkl}(Q), \quad z_{jkl}(R) \quad \text{and} \quad \mathfrak{q}(Q,R) \quad \text{for } 1 \le j \le k \le l \le 2.$$

We recall [1, Lemma 2.3] which will be used in Proposition 4.4.

Lemma 4.3. *Assume that $Q, R, Q+R, Q-R \in U$. Let $\mathfrak{q}(Q,R)$ be defined by (15) and set $\mathfrak{q}_R(Q) = \mathfrak{q}(Q,R)$. Then for any fixed $R \in U$, the zero set $\{\mathfrak{q}_R(Q) = \mathfrak{q}(Q,R) = 0\}$ has dimension one and $\Theta \pm R \subset \{\mathfrak{q}_R = 0\}$. Moreover if $R' \in U$ with $R \neq \pm R'$, then*

$$|\{\mathfrak{q}_R = 0\} \cap \{\mathfrak{q}_{R'} = 0\} \cap U| \le 20. \tag{16}$$

One can show that for $D \in U(\mathbb{F}_{q^m})$, where $m \in \mathbb{Z}, m \ge 1$, we have

$$|\{\Theta(\mathbb{F}_{q^m}) + D\} \cap \Theta(\mathbb{F}_{q^m})| \le 2.$$

See [1, Lemma 2.4]. Thus

$$|\{\Theta(\mathbb{F}_{q^m}) + D\} \cap U| \ge |\Theta(\mathbb{F}_{q^m})| - 2. \tag{17}$$

Proposition 4.4. *Let $f \in \mathbb{F}_{q^n}(U)$ be a rational function with a pole divisor of the form $\alpha\Theta, \alpha \in \mathbb{Z}, \alpha \geq 1$. Let L be a positive integer and let $R_0, \ldots, R_L \in J_C(\mathbb{F}_{q^n})$ such that $R_i \notin \Theta(\mathbb{F}_{q^n})$ and $R_L \neq \pm R_j$ for $0 \leq i \leq L$ and $0 \leq j \leq L-1$. Let $c_0 \ldots, c_L \in \mathbb{F}_{q^n}$ with $c_L \neq 0$. Then the rational function $F \in \mathbb{F}_{q^n}(U)$, with*

$$F(Q) = \sum_{i=0}^{L} c_i f(Q + R_i)$$

is non-constant and has degree

$$\deg F \leq 6(L+1) \deg f. \tag{18}$$

P r o o f. Defining the function $f_{R_i} : Q \mapsto f(Q + R_i)$ yields

$$F(Q) = \sum_{i=0}^{L-1} c_i f_{R_i}(Q) + c_L f_{R_L}(Q).$$

To prove that F is non-constant, we show that there exists $Q \in U$ such that it is a pole of f_{R_L}, but not a pole of any other terms f_{R_i} for $i < L$.

Observe that f_{R_L} has a pole at Q when $Q \in \Theta - R_L$, in particular, when $Q \in \Theta(\mathbb{F}_{q^m}) - R_L$, for $m \geq 1$ independent of n. Define $\mathfrak{q}_{R_i} = \mathfrak{q}(Q, R_i)$. From Lemma 4.3, we know that $\Theta(\mathbb{F}_{q^m}) - R_i \subseteq \{\mathfrak{q}_{R_i} = 0\}$. Hence, by (16) we obtain

$$\left| \Big((\Theta(\mathbb{F}_{q^m}) - R_L) \cap U \Big) \cap \{\mathfrak{q}_{R_i} = 0\} \right| \leq |\{\mathfrak{q}_{R_L} = 0\} \cap \{\mathfrak{q}_{R_i} = 0\} \cap U| \leq 20.$$

Thus, by (17), we obtain

$$\begin{aligned} &\left| \Big((\Theta(\mathbb{F}_{q^m}) - R_L) \cap U \Big) \setminus \left(\bigcup_{i=0}^{L-1} \{\mathfrak{q}_{R_i} = 0\} \right) \right| = \\ &\left| \bigcap_{i=0}^{L-1} \left(\Big((\Theta(\mathbb{F}_{q^m}) - R_L) \cap U \Big) \setminus \{\mathfrak{q}_{R_i} = 0\} \right) \right| \geq |\Theta(\mathbb{F}_{q^m})| - 2 - 20L. \end{aligned} \tag{19}$$

We pick m such that $|\Theta(\mathbb{F}_{q^m})| - 2 - 20L > 0$. Hence, there exists a point Q which is a pole of f_{R_L} but not a pole of any other term of F. Hence, F is non-constant.

To estimate the degree of F, we first estimate the degree of f_{R_i}. For arbitrary i, define $R = R_i$. We define

$$z_{jk}^R(Q) = z_{jk}(Q + R), \quad z_{jkl}^R(Q) = z_{jkl}(Q + R), \quad z^R = z(Q + R).$$

Then we can write $f_R(Q)$ as

$$f_R(Q) = f(Q + R) = f\left(z_{11}^R(Q), \ldots, z_{222}^R(Q), z^R(Q)\right).$$

We can consider $z_{jk}^R(Q), z_{jkl}^R(Q)$ to be rational functions in the variables $z_{jk}(Q)$, $z_{jkl}(Q)$ and $z(Q)$, see Appendix A.2. Then it follows from the explicit formulas of these functions that

$$\deg z_{jk}^R \leq 3, \quad \deg z_{jkl}^R \leq 4 \quad \text{and} \quad \deg z^R \leq 6.$$

Hence we obtain

$$\deg f_R \leq (\deg f)\Big(\max\big\{\deg z_{jk}^R,\ \deg z_{jkl}^R, \deg z^R\big\}\Big) = 6 \deg f,$$

and thus

$$\deg F \leq \deg\left(\sum_{i=0}^{L} c_i f_R\right) \leq 6(L+1)(\deg f).$$

□

4.2. Bounds on the number of zeros of a system of polynomial equations over a finite field.

Let $f_1, \ldots, f_k \in \mathbb{F}_{q^n}[X_1, \ldots, X_m]$. We denote the vanishing set of $f_1, \ldots, f_k$ over $\mathbb{F}_{q^n}$ by

$$V_{\mathbb{F}_{q^n}}(f_1, \ldots, f_k) = \left\{\mathbf{x} \in \mathbb{F}_{q^n}^m : f_1(\mathbf{x}) = \cdots = f_k(\mathbf{x}) = 0\right\},$$

and the vanishing set over the algebraic closure $\overline{\mathbb{F}}_q$ by

$$V(f_1, \ldots, f_k) = V_{\overline{\mathbb{F}}_q}(f_1, \ldots, f_k).$$

For each $m \in \mathbb{Z}, m \geq 1$, we define affine m-space over $\overline{\mathbb{F}}_q$ to be

$$\mathbb{A}^m(\overline{\mathbb{F}}_q) = \left\{(x_1, \ldots, x_m) : x_i \in \overline{\mathbb{F}}_q, 1 \leq i \leq m\right\}. \tag{20}$$

The following result gives us bounds for the cardinality of algebraic sets over finite fields, [10, Corollary 2.2].

Lemma 4.5. *Let $f_1, \ldots, f_k \in \mathbb{F}_{q^n}[X_1, \ldots, X_m]$ such that $V(f_1, \ldots, f_k)$ has dimension d in $\mathbb{A}^m(\overline{\mathbb{F}}_q)$. Then*

$$\left|V_{\mathbb{F}_{q^n}}(f_1, \ldots, f_k)\right| = \left|V(f_1, \ldots, f_k) \cap \mathbb{F}_{q^n}^m\right| \leq (q^n)^d \prod_{i=1}^{k} \deg f_i.$$

Lemma 4.6. *Let $f_1, \ldots, f_6$ be the defining equations of U as in (14), let $F \in \mathbb{F}_{q^n}(U)$ be a non-constant rational function and let G_1/G_2 be a representation of $F \in \mathbb{F}_{q^n}(\mathbf{Z})$ as a rational function. Then*

$$\left|V_{\mathbb{F}_{q^n}}(f_1, \ldots, f_6, G_1)\right| \leq 216 q^n \deg F. \tag{21}$$

P r o o f. Since U has dimension 2 and F is non-constant on U, $V(f_1, \ldots, f_6, G_1)$ has dimension 1 in $\mathbb{A}^8$. Applying Lemma 4.5, we obtain

$$\left|V_{\mathbb{F}_{q^n}}(f_1, \ldots, f_6, G_1)\right| \leq q^n \deg G_1 \prod_{i=1}^{6} \deg f_i \leq 216 q^n \deg F.$$

□

4.3. Linear complexity

We recall the following result on the linear complexity, see [13, Lemma 6].

Lemma 4.7. *Let (s_n) be a linear recurrent sequence of order L over $\mathbb{F}_q$ defined by a linear recursion*

$$s_{n+L} = c_0 s_n + \cdots + c_{L-1} s_{n+L-1}, \quad n \geq 0.$$

Then for any $T \geq L+1$ and pairwise distinct positive integers $j_1, \ldots, j_T$, there exist $\lambda_1, \ldots, \lambda_T \in \mathbb{F}_q$, not all equal to zero, such that

$$\sum_{i=1}^{T} \lambda_i s_{n+j_i} = 0, \quad n \geq 0.$$

4.4. Number of torsion elements

We need the following result on the number of torsion elements in the Jacobian of hyperelliptic curves over finite fields.

Lemma 4.8. *Let m be an integer coprime to the characteristic of $\mathbb{F}_q$. Then,*

$$\left|\left\{D \in J_C(\overline{\mathbb{F}}_q) : mD = \mathcal{O}\right\}\right| = m^{2g}.$$

For a proof, we refer to [7, Theorem A.7.2.7].

4.5. Collisions

We now turn our attention to the collisions which can occur in (9). Let $T_k(Q)$ be the number of k-tuples $\boldsymbol{m} = (m_0, \ldots, m_{k-1}) \in \mathcal{R}^k$ such that $D_{\boldsymbol{m}} = Q$. We recall the following result from [12, Theorem 2], which gives an upper bound for $T_k(Q)$. This upper bound implies that the elements generated by (9) do not take the same value too often and are sufficiently uniformly distributed.

Proposition 4.9. *Let C be a hyperelliptic curve of genus 2 defined over $\mathbb{F}_q$ such that the characteristic polynomial of the Frobenius endomorphism χ_C is irreducible. Let $D \in J_C(\mathbb{F}_{q^n})$ of prime order ℓ. Then for any integers k and e with $1 \leq e \leq k$ and $q^{2e} \leq (q^{1/2}-1)^4 q^{-8} \ell$, and for every element $Q \in J_C(\mathbb{F}_{q^n})$, the bound $T_k(Q) \leq q^{2(k-e)}$ holds.*

The bound of Proposition 4.9 shows that if k is small and

$$q^{2k} \le (q^{1/2}-1)^4 q^{-8}\ell,$$

then all the elements $D_{\boldsymbol{m}}$ are distinct. We observe that if $q^{2e} \ll \ell/q^8$, then $q^{2e} \ll (q^{1/2}-1)^4 q^{-8}\ell$. For larger k, choosing e maximal such that $q^{2e} \ll \ell/q^8$ yields

$$T_k(Q) \le \max\{1, q^{2k-2e}\} \ll \max\left\{1, \frac{q^{2k+8}}{\ell}\right\}. \tag{22}$$

5. Proof of the main theorem

Let $\chi_C(T) = T^4 + s_1T^3 + s_2T^2 + s_1qT + q^2$ be the characteristic polynomial of the Frobenius endomorphism for genus 2. The following result is a crucial step in the proof of the main theorem.

Lemma 5.1. *If $D \in J_C(\mathbb{F}_{q^n})$ has prime order ℓ, and ℓ does not divide the constant term of χ_C, then $\sigma(D) \neq \mathcal{O}$.*

Proof. If $\sigma(D) = \mathcal{O}$, then by definition of χ_C, we have that

$$q^2 D = -\sigma(D)^4 - s_1\sigma(D)^3 - s_2\sigma(D)^2 - s_1q\sigma(D) = \mathcal{O}.$$

Thus, the order ℓ of D divides q^2, which is the constant term of χ_C. □

Proof. (Theorem 3.1) We fix $r = \max\{\lfloor \frac{k}{4} \rfloor, 1\}$. Let $\boldsymbol{m} \in \mathcal{R}^k$, we can write

$$\boldsymbol{m} = (\boldsymbol{\mu}, \boldsymbol{\nu}), \boldsymbol{\mu} \in \mathcal{R}^r, \boldsymbol{\nu} \in \mathcal{R}^{k-r}.$$

Let N_r and N_{k-r} be the number of distinct elements $D_{\boldsymbol{\nu}}, \boldsymbol{\nu} \in \mathcal{R}^r$ and $\boldsymbol{\nu} \in \mathcal{R}^{k-r}$, respectively. We can assume that $\ell \gg q^{\frac{3}{4}n+8}$, since otherwise (11) holds trivially. Therefore, $\max\{q^{2r}, q^{2k-2r}\} \ll \ell/q^8$. Hence, by (22), we obtain

$$N_{k-r} \ge \frac{|\mathcal{R}^{k-r}|}{\max_Q T_{k-r}(Q)} \gg \frac{q^{2(k-r)}}{\max\{1, q^{2(k-r)+8}/\ell\}} = \min\left\{q^{2(k-r)}, \frac{\ell}{q^8}\right\}. \tag{23}$$

Let L be the linear complexity of the sequence $(w_{\boldsymbol{m}})_{\boldsymbol{m}\in\mathcal{R}^k}$ as defined in (10). We can assume that

$$L < \min\left\{N_r, \frac{|J_C(\mathbb{F}_{q^n})| - |\Theta(\mathbb{F}_{q^n})|}{|\Theta(\mathbb{F}_{q^n})| + 16}\right\}, \tag{24}$$

since otherwise the theorem holds trivially.

Since by (24), we assume that $L < N_r$, there exist $L+1$ vectors $\boldsymbol{d_0}, \dots, \boldsymbol{d_L} \in \mathcal{R}^r$ such that $D_{\boldsymbol{d_0}}, \dots, D_{\boldsymbol{d_L}}$ are distinct.

We fix these vectors and for each $j = 0, \dots, L$ define the sequence

$$a_j(\boldsymbol{s}) = w_{(\boldsymbol{d_j}, \boldsymbol{s})}, \quad \boldsymbol{s} \in \mathcal{R}^{k-r},$$

where again the elements $a_j(\boldsymbol{s})$ are arranged in a sequence by using lexicographic ordering for vectors $\boldsymbol{s}$. The sequences $(a_j(\boldsymbol{s}))_{\boldsymbol{s} \in \mathcal{R}^{k-r}}$ are parts of $(w_{\boldsymbol{m}})_{\boldsymbol{m} \in \mathcal{R}^k}$, that is, they are consecutive elements in $(w_{\boldsymbol{m}})_{\boldsymbol{m} \in \mathcal{R}^k}$, as $\boldsymbol{s}$ runs through $\mathcal{R}^{k-r}$. By Lemma 4.7, these sequences are linearly dependent, i.e. there exist constants $c_0, \dots . c_L \in \mathbb{F}_{q^n}$, not all zero, such that

$$c_0 w_{(\boldsymbol{d_0}, \boldsymbol{s})} + \cdots + c_L w_{(\boldsymbol{d_L}, \boldsymbol{s})} = 0, \quad \boldsymbol{s} \in \mathcal{R}^{k-r}. \tag{25}$$

Note that for

$$\boldsymbol{m} = (\boldsymbol{d_j}, \boldsymbol{s}), \quad D_{\boldsymbol{m}} = D_{(\boldsymbol{d_j}, \boldsymbol{s})} = D_{\boldsymbol{d_j}} + \sigma^r(D_{\boldsymbol{s}}) \qquad \text{by (9)}.$$

We would like to avoid collision of elements $D_{\boldsymbol{d_j}}, j \in \{0, \dots, L\}$ with $\Theta(\mathbb{F}_{q^n})$. We claim that there exists an element $R \in J_C(\mathbb{F}_{q^n})$ such that

$$D_{\boldsymbol{d_i}} + R \notin \Theta(\mathbb{F}_{q^n}), \quad \text{for } \ 0 \le i \le L, \tag{26}$$

$$D_{\boldsymbol{d_L}} + R \neq -(D_{\boldsymbol{d_j}} + R), \quad \text{for } \ 0 \le j \le L - 1. \tag{27}$$

We count the number of elements $R \in J_C(\mathbb{F}_{q^n})$ such that R does not satisfy (26) or (27). There are at most $(L+1)|\Theta(\mathbb{F}_{q^n})|$ choices for R such that $D_{\boldsymbol{d_i}} + R \in \Theta(\mathbb{F}_{q^n})$ for some $0 \le i \le L$.

Furthermore, if (27) was not satisfied, then we obtain that

$$-(D_{\boldsymbol{d_L}} + D_{\boldsymbol{d_j}}) = 2R, \quad \text{for some } \ 0 \le j \le L - 1.$$

By Lemma 4.8, we obtain that there are at most 16 elements $R \in J_C(\overline{\mathbb{F}}_q)$ such that $2R = \mathcal{O}$. Therefore, there are at most $16L$ choices for R such that $2R = -(D_{\boldsymbol{d_L}} + D_{\boldsymbol{d_j}})$ for some $j \in \{0, \dots, L-1\}$. By (24), we know that

$$|J_C(\mathbb{F}_{q^n})| - (L+1)\,|\Theta(\mathbb{F}_{q^n})| - 16L > 0,$$

hence there exists $R \in J_C(\mathbb{F}_{q^n})$ such that (26) and (27) are satisfied.

Let $R_i = D_{\boldsymbol{d_i}} + R$. Consider the function

$$F(Q) = \sum_{i=0}^{L} c_i f(Q + R_i). \tag{28}$$

By Proposition 4.4 we know that F is non-constant and has degree at most $6(L+1)(\deg f)$.

We observe that if F has a pole at Q, then Q must have a form

$$Q = \sigma^r(D_{\boldsymbol{s}}) - R, \quad \boldsymbol{s} \in \mathcal{R}^{k-r},$$

with

$$Q \in \Theta(\mathbb{F}_{q^n}) \quad \text{or} \quad Q \in \Theta(\mathbb{F}_{q^n}) \pm R_i \quad \text{for } \ 0 \leq i \leq L.$$

Hence, defining set $\mathcal{S}$ as follows ensures that for $Q \in \mathcal{S}$, the sum in (28) does not contain any poles. Define

$$\mathcal{S} = \{Q \in J_C(\mathbb{F}_{q^n}) : \ Q = \sigma^r(D_{\boldsymbol{s}}) - R, \quad \boldsymbol{s} \in \mathcal{R}^{k-r},$$

with

$$Q \notin \Theta(\mathbb{F}_{q^n}) \quad \text{and} \quad Q \pm R_i \notin \Theta(\mathbb{F}_{q^n}) \quad \text{for} \quad 0 \leq i \leq L\}.$$

Hence by (10) and (25), $F(Q) = 0$ for $Q \in \mathcal{S}$.

Now we give a lower bound for $|\mathcal{S}|$. We observe that if D has prime order ℓ, then $\sigma^j(D)$ also has order ℓ, since σ is an endomorphism and hence additive. Combining this with (9), we see that if $\ell D_{\boldsymbol{m}} = \mathcal{O}$, then either $D_{\boldsymbol{m}} = \mathcal{O}$ or it has order ℓ, since ℓ is prime. Hence, by Lemma 5.1, we obtain that if $D_{\boldsymbol{m}} \neq D_{\boldsymbol{n}}$, then

$$\sigma^j(D_{\boldsymbol{m}}) \neq \sigma^j(D_{\boldsymbol{n}}), \boldsymbol{m}, \boldsymbol{n} \in \mathcal{R}^k, j \in \mathbb{Z}, j \geq 1.$$

Therefore, the number of distinct elements

$$\sigma^r(D_{\boldsymbol{s}}) - R, \quad \boldsymbol{s} \in \mathcal{R}^{k-r} \quad \text{is} \quad N_{k-r}.$$

We observe that for

$$Q = \sigma^r(D_{\boldsymbol{s}}) - R, \boldsymbol{s} \in \mathcal{R}^{k-r},$$

$$|\{Q \in J_C(\mathbb{F}_{q^n}) : Q \in \Theta(\mathbb{F}_{q^n})\}| \leq |\Theta(\mathbb{F}_{q^n})| \tag{29}$$

and

$$|\{Q \in J_C(\mathbb{F}_{q^n}) : Q \pm R_i \in \Theta(\mathbb{F}_{q^n})\}| \leq 2(L+1) \left|\Theta(\mathbb{F}_{q^n})\right|. \tag{30}$$

Hence, by (29) and (30) we obtain,

$$|\mathcal{S}| \geq N_{k-r} - 2(L+1)|\Theta(\mathbb{F}_{q^n})| - \left|\Theta(\mathbb{F}_{q^n})\right|. \tag{31}$$

To give an upper bound for $|\mathcal{S}|$, we use Lemma 4.6 and (18) to obtain

$$|\mathcal{S}| \leq 216 q^n \deg F \leq 1296(L+1) q^n \deg f. \tag{32}$$

Combining equations (31) and (32) gives us

$$L \geq \frac{N_{k-r} - 3|\Theta(\mathbb{F}_{q^n})| - 1296 q^n \deg f}{1296 q^n \deg f + 2|\Theta(\mathbb{F}_{q^n})|}. \tag{33}$$

By (2), we can estimate the size of $|\Theta(\mathbb{F}_{q^n})|$. Substituting the lower bound on N_{k-r} as given in (23) into (33), we obtain

$$L(w_{\boldsymbol{m}}) \gg \frac{\min\{q^{3k/2}, \ell/q^8\}}{q^n \deg f}. \qquad \square$$

Acknowledgement. The author was supported by the Austrian Science Fund FWF Project P31762. I am very grateful to László Mérai for valuable discussions and comments.

Appendix A.

Let C be the hyperelliptic curve defined by (1) with

$$f(X) = X^5 + b_1X^4 + b_2X^3 + b_3X^2 + b_4X + b_5 \in \mathbb{F}_q[X],$$

for the finite field $\mathbb{F}_q$ with characteristic $p \geq 3$.

A.1. Defining equations of the Jacobian

Let

$$S = \mathbb{F}_q[Z_0, Z_{11}, Z_{12}, Z_{22}, Z_{111}, Z_{112}, Z_{122}, Z_{222}, Z]$$

be a polynomial ring over field $\mathbb{F}_q$, with characteristic $p \geq 3$. Following [4], in particular Theorem 2.5, Theorem 2.11 and Corollary 2.15, we define f_i as follows:

$$\begin{aligned} f_0 &= Z^2 + Z_{11}^2Z_{12} + b_1Z_{11}^2Z_{22} + b_2Z_{11}^2Z_{12}Z_{22} - b_3Z_{11}Z_{22}^2 + b_4Z_{12}Z_{22}^2 \\ &\quad - b_5Z_{22}^3 + 2b_1ZZ_{11} - 2b_2ZZ_{12} + 2b_3ZZ_{22} + (b_3 - b_1b_2)Z_{11}Z_{12} \\ &\quad + (b_2^2 - b_1b_3)Z_{11}Z_{22} + (b_1b_4 - b_2b_3 - b_5)Z_{12}Z_{22} - b_1b_5Z_{22}^2 \\ &\quad + 2(b_1b_3 - b_2^2)Z + (b_1b_4 - b_5)Z_{11} + b_2(b_2^2 - b_1b_3)Z_{12} \\ &\quad + (b_3b_4 - b_2b_5)Z_{22} + b_1b_3b_4 - b_2^2b_4 - b_3b_5, \\ f_1 &= 2Z - Z_{11}Z_{22} + Z_{12}^2 - b_2Z_{12} + b_4, \\ f_2 &= Z_{112} - Z_{222}Z_{12} + Z_{122}Z_{22}, \\ f_3 &= Z_{111} + Z_{222}Z_{11} + Z_{122}Z_{12} - 2Z_{112}Z_{22} - 2b_1Z_{112} + b_2Z_{122}, \end{aligned}$$

$$
\begin{aligned}
f_4 &= Z_{122}^2 - Z_{11}Z_{22}^2 + 2ZZ_{22} + Z_{11}Z_{12} - b_1Z_{11}Z_{22} - b_2Z_{12}Z_{22} \\
&\quad + 2b_1Z - b_1b_2Z_{12} + b_4Z_{22} + b_1b_4 - b_5, \\
f_5 &= Z_{222}^2 - Z_{22}^3 - Z_{12}Z_{22} - b_1Z_{22}^2 - Z_{11} - b_2Z_{22} - b_3, \\
f_6 &= Z_{122}Z_{222} - Z_{12}Z_{22}^2 + Z - b_2Z_{12} - b_1Z_{12}Z_{22}, \\
f_7 &= Z_{111}^2 - Z_{11}^3 - b_3Z_{11}^2 - b_4Z_{11}Z_{12} + 3b_5Z_{11}Z_{22} + 2b_5Z \\
&\quad + (4b_1b_5 - b_2b_4)Z_{11} - 3b_2b_5Z_{12} + (4b_3b_5 - b_4^2)Z_{22} \\
&\quad + 4b_1b_3b_5 + b_4b_5 - b_1b_4^2 - b_2^2b_5, \\
f_8 &= -Z_{111}Z_{112} + b_1Z_{111}Z_{122} - b_2Z_{112}Z_{122} + b_3Z_{112}Z_{222} \\
&\quad - b_4Z_{122}Z_{222} + b_5Z_{222}^2 - Z^2 - b_1ZZ_{11} + b_2ZZ_{12} - b_3ZZ_{22} \\
&\quad - b_3Z_{11}Z_{12} + b_1b_3Z_{11}Z_{22} - (b_5 + b_1b_4)Z_{12}Z_{22} + 2b_1b_5Z_{22}^2 \\
&\quad - 2(b_1b_3 + b_4)Z + (2b_2b_4 + b_1b_2b_3 + b_1b_5 - b_3^2 - b_1^2b_4)Z_{12} \\
&\quad - 2b_5Z_{11} + 2b_5(b_1^2 - b_2)Z_{22} + b_1b_2b_5 - b_1b_3b_4 - 2b_3b_5, \\
f_9 &= Z_{122}^2 - Z_{111}Z_{122} + Z_{11}Z - b_3Z_{11}Z_{22} + 2b_4Z_{12}Z_{22} - 3b_5Z_{22}^2 \\
&\quad + 2b_3Z + (b_1b_4 - b_2b_3 - b_5)Z_{12} - 2b_1b_5Z_{22} + b_3b_4 - b_2b_5, \\
f_{10} &= Z_{111}Z_{222} - Z_{112}Z_{122} - 2ZZ_{12} + Z_{11}^2 - 2b_1Z_{11}Z_{12} \\
&\quad + 3b_2Z_{11}Z_{22} - 2b_3Z_{12}Z_{22} + b_4Z_{22}^2 - 5b_2Z + b_3Z_{11} \\
&\quad + (3b_2^2 - 2b_1b_3)Z_{12} + (b_1b_4 - b_5)Z_{22} - 2b_2b_4, \\
f_{11} &= Z_{122}^2 - Z_{112}Z_{222} + Z_{22}Z + 2Z_{11}Z_{12} - b_1Z_{11}Z_{22} + 2b_1Z \\
&\quad + (b_3 - b_1b_2)Z_{12} + b_1b_4 - b_5, \\
f_{12} &= Z_{111}Z_{12} - Z_{112}Z_{11} - b_4Z_{122} + 2b_5Z_{222}, \\
f_{13} &= 2Z_{122}Z_{11} - Z_{112}Z_{12} - Z_{111}Z_{22} - b_2Z_{112} + 2b_3Z_{122} - b_4Z_{222}.
\end{aligned}
$$

One can show that $f_0 \in \langle f_4, f_5, f_6 \rangle$ and the vanishing locus of these polynomials homogenized with respect to the variable Z_0 forms a set of defining equations for the Jacobian J_C, i.e.,

$$J_C = V(f_1^h, \ldots, f_{13}^h) = \{z \in \mathbb{P}^8(\overline{\mathbb{F}}_q) : f_i^h(z) = 0, 1 \leq i \leq 13\}$$

A.2. Addition formulas

For $D = (x_1, y_1) + (x_2, y_2) - 2\mathcal{O} \in J_C(\mathbb{F}_q) \setminus \Theta(\mathbb{F}_q)$, (13) gives us $\iota(D)$, where the components z_{jk}, z_{jkl} of $\iota(D)$ can be expressed as rational functions in the coordinates (x_1, y_1) and (x_2, y_2). For the sake of completeness, we collect the addition formulas as given in [4, Theorem 3.3] and as explicitly computed in [1, Appendix A.3].

$$
\begin{aligned}
z_{ij}(Q+R) &= -z_{ij}(Q) - z_{ij}(R) + \frac{1}{4}\left(\frac{q_i(Q,R)}{q(Q,R)}\right)\left(\frac{q_j(Q,R)}{q(Q,R)}\right) - \frac{1}{4}\left(\frac{q_{ij}(Q,R)}{q(Q,R)}\right),\\
z_{111}(Q+R) &= -\frac{1}{2}z_{111}(Q) - \frac{1}{2}z_{111}(R) + \frac{3}{16}\frac{q_1(Q,R)q_{11}(Q,R)}{q(Q,R)^2} - \frac{1}{16}\frac{q_{111}(Q,R)}{q(Q,R)}\\
&\quad - \frac{1}{8}\left(\frac{q_1(Q,R)}{q(Q,R)}\right)^3 + \frac{3}{4}\big(z_{11}(Q) + z_{11}(R)\big)\frac{q_1(Q,R)}{q(Q,R)},\\
z_{112}(Q+R) &= -\frac{1}{2}z_{112}(Q) - \frac{1}{2}z_{112}(R) + \frac{1}{16}\frac{q_2(Q,R)q_{11}(Q,R)}{q(Q,R)^2}\\
&\quad + \frac{1}{8}\frac{q_1(Q,R)q_{12}(Q,R)}{q(Q,R)^2} - \frac{1}{16}\frac{q_{112}(Q,R)}{q(Q,R)} - \frac{1}{8}\frac{q_2(Q,R)(q_1(Q,R))^2}{q(Q,R)^3}\\
&\quad + \frac{3}{8}\big(z_{11}(Q) + z_{11}(R)\big)\frac{q_2(Q,R)}{q(Q,R)} + \frac{3}{8}\big(z_{12}(Q) + z_{12}(R)\big)\frac{q_1(Q,R)}{q(Q,R)},\\
z_{122}(Q+R) &= -\frac{1}{2}z_{122}(Q) - \frac{1}{2}z_{122}(R) + \frac{1}{16}\frac{q_1(Q,R)q_{22}(Q,R)}{q(Q,R)^2}\\
&\quad + \frac{1}{8}\frac{q_2(Q,R)q_{12}(Q,R)}{q(Q,R)^2} - \frac{1}{16}\frac{q_{122}(Q,R)}{q(Q,R)}\\
&\quad - \frac{1}{8}\frac{q_1(Q,R)(q_2(Q,R))^2}{q(Q,R)^3} + \frac{3}{4}\big(z_{12}(Q) + z_{12}(R)\big)\frac{q_2(Q,R)}{q(Q,R)},\\
z_{222}(Q+R) &= -\frac{1}{2}z_{222}(Q) - \frac{1}{2}z_{222}(R) + \frac{3}{16}\frac{q_2(Q,R)q_{22}(Q,R)}{q(Q,R)^2} - \frac{1}{16}\frac{q_{222}(Q,R)}{q(Q,R)}\\
&\quad - \frac{1}{8}\left(\frac{q_2(Q,R)}{q(Q,R)}\right)^3 + \frac{3}{4}\big(z_{22}(Q) + z_{22}(R)\big)\frac{q_2(Q,R)}{q(Q,R)},\\
z(Q+R) &= \frac{1}{2}\big(z_{11}(Q+R)z_{22}(Q+R) - z_{11}^2(Q+R) + b_2 z_{12}(Q+R) - b_4\big).
\end{aligned}
$$

To evaluate the addition formulas above, we need the following rational functions:

$$
\begin{aligned}
q(Q,R) &= z_{11}(Q) - z_{11}(R) + z_{12}(Q)z_{22}(R) - z_{12}(R)z_{22}(Q),\\
q_1(Q,R) &= 2z_{111}(Q) - 2z_{111}(R) + 2z_{112}(Q)z_{22}(R) - 2z_{112}(R)z_{22}(Q)\\
&\quad + 2z_{122}(R)z_{12}(Q) - 2z_{122}(Q)z_{12}(R),\\
q_2(Q,R) &= 2z_{112}(Q) - 2z_{112}(R) + 2z_{122}(Q)z_{22}(R) - 2z_{122}(R)z_{22}(Q)\\
&\quad + 2z_{222}(R)z_{12}(Q) - 2z_{222}(Q)z_{12}(R),\\
q_{11}(Q,R) &= 4b_3q(Q,R) + 4b_4\big(z_{12}(Q) - z_{12}(R)\big) + 4\big((2z - b_2z_{12} + b_4)(Q)z_{12}(R)\big)\\
&\quad - 4\big((2z - b_2z_{12} + b_4)(R)z_{12}(Q)\big) - 8b_5\big(z_{22}(Q) - z_{22}(R)\big)\\
&\quad + 2\big(2z_{112}(Q)2z_{122}(R) - 2z_{112}(R)2z_{122}(Q)\big),\\
q_{12}(Q,R) &= 4b_3\big(z_{12}(Q) - z_{12}(R)\big) + 2b_2\big(z_{12}(Q)z_{22}(R)\big)\\
&\quad - 2b_2\big(z_{12}(R)z_{22}(Q)\big) - 4\big(z_{11}(Q)z_{12}(R) - z_{11}(R)z_{12}(Q)\big)\\
&\quad + 2\big((2z - b_2z_{12} + b_4)(Q)z_{22}(R) - (2z - b_2z_{12} + b_4)(R)z_{22}(Q)\big)\\
&\quad - 2b_4\big(z_{22}(Q) - z_{22}(R)\big) + 2z_{222}(R)2z_{112}(Q) - 2z_{222}(Q)2z_{112}(R),\\
q_{22}(Q,R) &= 8b_1\big(z_{12}(Q)z_{22}(R) - z_{12}(R)z_{22}(Q)\big) + 4b_2z_{12}(Q)\\
&\quad - 4b_2z_{12}(R) - 8\big(z_{11}(Q)z_{22}(R) - z_{11}(R)z_{22}(Q)\big)\\
&\quad - 4\big((2z - b_2z_{12} + b_4)(Q) - (2z - b_2z_{12} + b_4)(R)\big)\\
&\quad + 2\big(2z_{122}(Q)2z_{222}(R) - 2z_{122}(R)2z_{222}(Q)\big),\\
q_{111}(Q,R) &= 4b_3q_1(Q,R) + 4\big(2z_{111}(Q)z_{22}(Q)z_{12}(R) - 2z_{111}(R)z_{22}(R)z_{12}(Q)\big)\\
&\quad + 2z_{122}(R)\Big(2z_{12}(Q)\big(6z_{11}(Q) - 2z_{11}(R) + 4b_3\big) - 4b_4z_{22}(Q)\Big)\\
&\quad - 2z_{122}(Q)\Big(2z_{12}(R)\big(6z_{11}(R) - 2z_{11}(Q) + 4b_3\big) - 4b_4z_{22}(R)\Big)\\
&\quad + 2z_{112}(Q)\Big(z_{12}(R)\big(12z_{12}(R) - 8z_{12}(Q) + 4b_2\big) + 4b_4\Big)\\
&\quad - 2z_{112}(R)\Big(z_{12}(Q)\big(12z_{12}(Q) - 8z_{12}(R) + 4b_2\big) + 4b_4\Big),
\end{aligned}
$$

$$
\begin{aligned}
q_{112}(Q,R) = {} & 2z_{222}(Q)\big(4z_{11}(Q)z_{12}(R) - 4z_{12}(R)b_3 - 8b_5\big) \\
& + 2z_{112}(Q)\Big(-4z_{11}(R) + 4z_{12}(R)z_{22}(Q) + z_{12}(R)\big(12z_{22}(R) + 8b_1\big)\Big) \\
& + 2z_{112}(R)\Big(4z_{11}(Q) + z_{12}(Q)\big(-12z_{22}(Q) - 4z_{22}(R) - 8b_1\big) - 4b_3\Big) \\
& + 2z_{122}(Q)\big(-8z_{11}(R)z_{22}(R) - 8z_{12}(Q)z_{12}(R) - 4z_{12}(R)^2 \\
& + 4z_{22}(R)b_3 + 4b_4 - 4z_{12}(R)b_2\big) \\
& + 2z_{122}(R)\Big(8z_{11}(Q)z_{22}(Q) + 4z_{12}(Q)^2 + z_{12}(Q)\big(8z_{12}(R) + 4b_2\big) \\
& - 4z_{22}(Q)b_3 - 4b_4\Big) + 2z_{112}(Q)4b_3 \\
& + 2z_{222}(R)\Big(z_{12}(Q)\big(-4z_{11}(R) + 4b_3\big) + 8b_5\Big), \\
q_{122}(Q,R) = {} & 2z_{112}(R)\Big(-6z_{22}(Q)^2 + z_{22}(Q)\big(-2z_{22}(R) - 4b_1\big) - 2b_2\Big) \\
& + 2z_{122}(R)\Big(-4z_{11}(Q) + z_{22}(Q)\big(4z_{12}(R) - 2b_2\big) - 4b_3\Big) \\
& + 2z_{222}(Q)\big(2z_{11}(Q)z_{22}(R) - 4z_{11}(R)z_{22}(R) - 2z_{12}(R)^2\big) \\
& + 2z_{112}(Q)\big(2z_{22}(Q)z_{22}(R) + 6z_{22}(R)^2 + 4z_{22}(R)b_1 + 2b_2\big) \\
& + 2z_{222}(R)\big(4z_{11}(Q)z_{22}(Q) - 2z_{11}(R)z_{22}(Q) + 2z_{12}(Q)^2\big) \\
& + 2z_{122}(Q)\big(4z_{11}(R) - 4z_{12}(Q)z_{22}(R) + 2z_{22}(R)b_2 + 4b_3\big) \\
& - 2z_{222}(Q)\big(2b_4 + 4z_{12}(R)b_2\big) \\
& + 2z_{222}(R)\big(2b_4 + 4z_{12}(Q)b_2\big), \\
q_{222}(Q,R) = {} & 2z_{222}(R)\Big(-12z_{11}(Q) + 4z_{11}(R) + z_{12}(Q)\big(12z_{22}(Q) + 16b_1\big)\Big) \\
& + 2z_{122}(R)\big(-8z_{12}(Q) - 8z_{12}(R) - 12z_{22}(Q)^2 - 16z_{22}(Q)b_1 - 8b_2\big) \\
& + 2z_{112}(Q)\big(-4z_{22}(Q) - 8z_{22}(R)\big) \\
& + 2z_{222}(Q)\Big(-4z_{11}(Q) + 12z_{11}(R) + z_{12}(R)\big(-12z_{22}(R) - 16b_1\big)\Big) \\
& + 2z_{112}(R)\big(8z_{22}(Q) + 4z_{22}(R)\big) \\
& + 2z_{122}(Q)\big(8z_{12}(Q) + 8z_{12}(R) + 12z_{22}(R)^2 + 16z_{22}(R)b_1 + 8b_2\big).
\end{aligned}
$$

REFERENCES

[1] ANUPINDI, V.—MÉRAI, L.: *Linear complexity of some sequences derived from hyperelliptic curves of genus 2*, Cryptogr. Commun. **14** (2022), 117–134.

[2] *Handbook of Elliptic and Hyperelliptic Curve Cryptography.* (H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, F. Vercauteren, eds.). Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2006.

[3] GALBRAITH, S. D.: *Mathematics of Public Key Cryptography*. Cambridge University Press, Cambridge, 2012.

[4] GRANT, D.: *Formal groups in genus two*, J. Reine Angew. Math. **411** (1990), 96–121.

[5] GÜNTHER, C.—LANGE, T.—STEIN, A.: *Speeding up the arithmetic on Koblitz curves of genus two.* In: *Selected Areas in Cryptography (Waterloo, ON, 2000)*, In: *Lecture Notes in Comput. Sci. Vol. 2012*, Springer, Berlin, 2001, pp. 106–117.

[6] HARTSHORNE, R.: *Algebraic Geometry*. In: *Graduate Texts in Mathematics, No. 52.* Springer-Verlag, New York-Heidelberg, 1977.

[7] HINDRY, M.—SILVERMAN, J. H.: *Diophantine Geometry* (An introduction). In: *Graduate Texts in Math. Vol. 201*, Springer-Verlag, New York, 2000.

[8] KOBLITZ, N.: *CM-curves with good cryptographic properties.* In:*Advances in Cryptology—CRYPTO '91 (Santa Barbara, CA, 1991)*, In:*Lecture Notes in Comput. Sci. Vol. 576,* Springer-Verlag, Berlin, 1992. pp. 279–287.

[9] KOBLITZ, N.: *Algebraic Aspects of Cryptography*. (With an appendix by Alfred J. Menezes, Yi-Hong Wu and Robert J. Zuccherato). In: *Algorithms and Computation in Mathematics Vol. 3*, Springer-Verlag, Berlin, 1998.

[10] LACHAUD, G.—ROLLAND, R.: *On the number of points of algebraic sets over finite fields*, J. Pure Appl. Algebra **219** (2015), 5117–5136.

[11] LANGE, T.: *Koblitz curve cryptosystems*, Finite Fields Appl. **11** (2005), 200–229.

[12] LANGE, T.—SHPARLINSKI, I.: *Collisions in fast generation of ideal classes and points on hyperelliptic and elliptic curves*, Appl. Algebra Engrg. Comm. Comput. **15** (2005), 329–337.

[13] LANGE, T.—SHPARLINSKI, I. E.: *Certain exponential sums and random walks on elliptic curves*, Canad. J. Math. **57** (2005), 338–350.

[14] LANGE, T.—SHPARLINSKI, I. E.: *Distribution of some sequences of points on elliptic curves*, J. Math. Cryptol. **1** (2007), 1–11.

[15] MEIDL, W.—WINTERHOF, A.: *Linear Complexity of Sequences and Multisequences*. In: *Handbook of Finite Fields*. CRC Press, Boca Raton, 2013.

[16] MÉRAI, L.: *On pseudorandom properties of certain sequences of points on elliptic curve.* In: *Arithmetic of Finite Fields*, In: *Lecture Notes in Comput. Sci. Vol. 10064*, Springer, Cham, 2016. pp. 54–63.

[17] MÜLLER, V.: *Fast multiplication on elliptic curves over small fields of characteristic two*, J. Cryptology **11** (1998), 219–234.

[18] MUMFORD, D.: *Tata Lectures on Theta. II.* Jacobian theta functions and differential equations, With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura, Modern Birkhäuser Classics. Birkhäuser Boston, Inc., Boston, MA, 2007. (Reprint of the 1984 original).

[19] NIEDERREITER, H.: *Linear complexity and related complexity measures for sequences.* In: *Progress in Cryptology—INDOCRYPT 2003*, *Lecture Notes in Comput. Sci. Vol. 2904*, Springer-Verlag, Berlin, 2003, pp. 1–17.

[20] SMART, N. P.: *Elliptic curve cryptosystems over small fields of odd characteristic*, J.Cryptology **12** (1999), 141–151.

[21] SOLINAS, J. A.: *Efficient arithmetic on Koblitz curves.* Towards a quarter-century of public key cryptography. vol. 19, 2000, pp. 195–249.

[22] STICHTENOTH, H.: *Algebraic function fields and codes* (2nd edition) In: *Graduate Texts in Mathematics Vol. 254*, Springer-Verlag, Berlin, 2009.

[23] WINTERHOF, A.: *Linear complexity and related complexity measures.* In:*Selected Topics in Information and Coding Theory*, *Ser. Coding Theory Crypto. Vol. 7* World Sci. Publ. Hackensack, NJ, 2010, pp. 3–40.

Received March 4, 2022
Accepted March 25, 2022

Vishnupriya Anupindi
Johann Radon Institute
for Computational
and Applied Mathematics,
Austrian Academy of Sciences,
Altenberger Straße 69,
A-4040 Linz,
AUSTRIA
E-mail: vishnupriya.anupindi@oeaw.ac.at