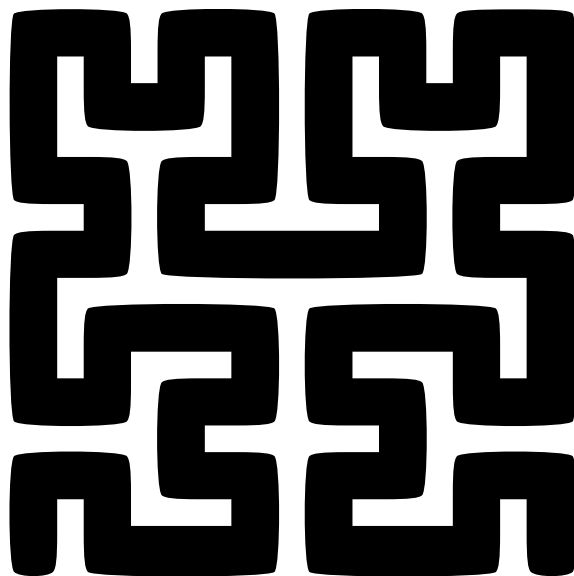




Polynesian Journal of Mathematics

Volume 4, Issue 10

Special volume AĴAX in honor of René Schoof

**Factorization pattern and fields of definition
of ℓ -torsion points on the Jacobians
of genus-3 hyperelliptic curves**

Amalia Pizarro-Madariaga

Edgardo Riquelme Faúndez

Received 26 Feb 2026

Revised 29 Jun 2026

Accepted 20 Aug 2026

Published 28 Sep 2026

Communicated by Elisa Lorenzo García

DOI: 10.69763/polyjmath.4.10

Factorization patterns and fields of definition of ℓ -torsion points on the Jacobians of genus-3 hyperelliptic curves

Amalia Pizarro-Madariaga¹ Edgardo Riquelme Faúndez²

¹Instituto de Matemáticas, Universidad del Valparaíso, Chile

²Departamento de Ciencias Básicas, Universidad del Bío-Bío, Chile

Dedicated to René Schoof, who generously helped shape the CIMPA school on Serre's open image theorem in Valparaíso and who, through his warmth toward the students and his evident delight in the city's hills and sea, made his visit especially memorable for all of us.

—Amalia Pizarro-Madariaga

Dedicated to René Schoof, whose point-counting algorithm profoundly shaped my mathematical career and has accompanied my journey from elliptic curves to higher-genus Jacobians, with gratitude and fond memories of the René 25 conference.

—Edgardo Riquelme Faúndez

Abstract

Motivated by Schoof–Pila-type point-counting algorithms, we study the fields of definition and factorization patterns of Galois orbits of ℓ -torsion points on the Jacobians of genus-3 hyperelliptic curves over finite fields. We show that the degree of the field of definition of the ℓ -torsion points can be bounded by $O(\ell^4)$, improving the previously expected $O(\ell^6)$ bound (which reflects the size of the ℓ -torsion subgroup, of order ℓ^6 for a genus-3 Jacobian). Moreover, we establish a precise correspondence between the rank of the ℓ -torsion subgroup and the Galois orbits of ℓ -torsion divisors. Our approach relies on a detailed analysis of the Jordan decomposition of the Frobenius action on J and its nilpotent part.

Keywords: Hyperelliptic curve cryptosystems, hyperelliptic curves, Jacobians, ℓ -adic point counting algorithms, torsion points.

This work was partially supported by STICAmSud project 24-STIC-04. The second author was also supported in part by grants 2020433 IF/R and GI2610409 of Universidad del Bío-Bío, Chile.

1 Introduction

The discovery of Schoof's elliptic curve point-counting algorithm [18] generated significant interest in the efficient computation of zeta functions of curves defined over finite fields, due to applications in cryptographic curve construction.

Gaudry et al. showed in [8, 9, 10] that Schoof's algorithm can be effectively adapted to hyperelliptic curves of genus two defined over a prime field, up to cryptographic sizes. (The first adaptation to the very general case of an abelian variety is the work of Pila [14] in 1990.) This makes it possible to compute the order of the group associated with the hyperelliptic curve and thereby to select curves suitable for cryptographic use.

The idea behind Schoof-type algorithms is to study the action of the Frobenius endomorphism on the ℓ -torsion subgroup $J[\ell]$ of the Jacobian of a hyperelliptic curve in order to determine the characteristic polynomial modulo ℓ . Repeating this process for several primes ℓ and combining the resulting congruences via the Chinese remainder theorem allows one to recover the full characteristic polynomial.

In Schoof's algorithm for elliptic curves, division polynomials vanish precisely on the abscissa of ℓ -torsion points. In genus two, generalized division polynomials [3] do not provide such a description; moreover, no equally simple representation of the ℓ -torsion subgroup is known, and constructing such a representation becomes the main computational bottleneck. This phenomenon also appears to persist for curves of genus $g > 2$; see [2].

To accelerate Schoof-type algorithms, Gaudry and Schost exploited ℓ^k -torsion elements. Since the cost of computing ℓ -torsion grows rapidly with ℓ , it is often more efficient to work with ℓ^k -torsion for small primes (such as $\ell = 2, 3, 5, 7$) rather than using larger primes ℓ .

To compute the ℓ^k -torsion subgroup, one recursively computes successive ℓ -divisions starting from the ℓ -torsion subgroup itself. An ℓ -division consists of algebraically inverting the multiplication-by- ℓ map on the Jacobian variety of C , $[\ell] : J \rightarrow J$. More precisely, given a divisor D_ℓ , the goal is to describe algebraically all divisors D satisfying $[\ell]D \sim D_\ell$; see [10, 13, 15, 16].

1.1 Motivation

Work of Abelard, Gaudry and Spaenlehauer [1] on genus-3 point-counting algorithms has continued this line of research. Furthermore, recent improvements to ℓ -division algorithms [13] have impacted Schoof–Pila-type algorithms, raising the question of how much the complexity of general algorithms (i.e. without efficiently computable real multiplication) decreases in genus three, and making it important to revisit the possibility of the generic case (i.e. without assuming real multiplication). In Schoof–Pila-type algorithms, it is essential to construct the ℓ -torsion subgroup. The analogue of the division polynomials for hyperelliptic curves is given by Cantor [3]. Other approaches have been suggested by Eid [6] using p -adic differential equations. In the specific case $g = 3$, Lupoian in [12] gives a practical method for computing the 3-torsion subgroup of the Jacobian of a hyperelliptic curve.

The importance of determining the field of definition of the ℓ -torsion subgroup appears in the following two situations. Since torsion points are usually obtained through the factorization of auxiliary polynomials over finite fields, the complexity of these algorithms strongly depends on the corresponding extension degree. As noted by Matsuo [11], the distinct-degree factorization (DDF) step in the Cantor–Zassenhaus-type algorithm (see [4]) dominates the complexity, so knowledge of the field of definition can significantly improve the efficiency of these algorithms. Another application arises in the construction of towers of field extensions required in Schoof-type algorithms to compute ℓ -division points [10, 13]. Such explicit algorithms highlight the importance of understanding the arithmetic structure of the ℓ -torsion subgroups. In general, the possible factorization types of the Galois orbits of the ℓ -torsion divisors are determined by the characteristic polynomial $P(x)$ of the reduced Frobenius endomorphism π modulo ℓ .

1.2 Literature overview and main result

For elliptic curves (genus one), this was studied by Verdure [20]. For hyperelliptic curves of genus two, the number of distinct cases to consider increases significantly. An upper bound analysis for irreducible factors can be found in Matsuo [11], and an application to the factorization types of ℓ -modular polynomials can be found in Gaudry and Schost [7]. Furthermore, Riquelme [15] has established the relationship between the factorization type of the Galois orbits of the ℓ -torsion divisors and the field of definition of the ℓ -divisions. To our knowledge, a genus-3 version of polynomial factorization patterns has not yet been developed. On the other hand, bounds for genus three could be interesting considering applicability (concrete algorithms for computing the order of cryptographically secure genus-3 curves). This work generalizes Gaudry’s approach in genus two by providing a classification of the possible Frobenius action matrices on the ℓ -torsion of Jacobians of genus-3 hyperelliptic curves. As the genus increases, genuinely new configurations appear, and several arguments valid in lower genus no longer apply directly. This classification constitutes a first step toward establishing effective bounds for the fields of definition of ℓ -torsion points.

We derive explicit upper bounds for the degree of the field of definition of the ℓ -torsion, proving in particular that this degree is bounded by $O(\ell^4)$. More precisely,

Theorem 1.1 (Theorem 4.2 in Section 4). *If $\ell > 2$, there exists a positive integer $d \leq \ell^4 - \ell^3 + \ell - 1$ such that*

$$J[\ell] \subset J(\mathbb{F}_{q^d}).$$

Additionally, we provide an example showing that the bound of Theorem 4.2 is attained for $\ell = 3$.

1.3 Methodology

We begin by classifying the characteristic polynomials of Frobenius endomorphisms in genus three, determining which cases are compatible with the Hasse–Weil theorem and the Weil pairing. Next, using the elementary divisor version of the rational canonical form theorem, we derive a general framework that generalizes factorization patterns

to genus three. Rather than presenting an exhaustive list of all possible factorizations, we adopt a more abstract and conceptual approach; nevertheless, we include detailed analyses of the case $\ell = 2$. Finally, in contrast to Matsuo's approach, which relies on an exhaustive case-by-case analysis, we focus on the worst-case contribution of the nilpotent part in the Jordan decomposition, resulting in uniform upper bounds.

The paper is organized as follows. In Section 2, we recall the necessary background on Jacobians of genus-3 hyperelliptic curves over finite fields, the action of Frobenius on the ℓ -torsion subgroup, and the relation between the characteristic polynomial modulo ℓ and Galois orbits. In Section 3, we analyze the possible factorization patterns of the ℓ -torsion in genus three, based on the Jordan decomposition of the Frobenius endomorphism, and relate these patterns to fields of definition of ℓ -torsion points. In Section 4, we derive explicit upper bounds for the degree of the field of definition of the ℓ -torsion, and prove the main result showing that this degree is bounded by $O(\ell^4)$.

1.4 Acknowledgments

The authors wish to thank the anonymous referees for their valuable comments and suggestions, which significantly improved the quality and presentation of the manuscript.

2 Background

Let $\mathbb{F}_q$ be a finite field where $q = p^k$ with $p > 2$ prime and $\overline{\mathbb{F}}_q$ be an algebraic closure of $\mathbb{F}_q$. A hyperelliptic curve of genus three over $\mathbb{F}_q$ is given by an equation $C: y^2 = f(x)$, where $f(x) \in \mathbb{F}_q[x]$ is a monic polynomial of degree seven with distinct roots.

We denote by $J = \text{Jac}(C)$ the Jacobian variety of C . For any field extension K of $\mathbb{F}_q$, we denote by $J(K)$ the abelian group of K -rational points of J .

For a prime number ℓ , the ℓ -torsion subgroup of the Jacobian is defined by

$$J[\ell] = \{D \in J(\overline{\mathbb{F}}_q) : [\ell]D = 0\},$$

where 0 denotes the neutral element of $J(\overline{\mathbb{F}}_q)$ and $[\ell]$ is the multiplication-by- ℓ map.

It is known that if $\ell \neq p$, then $J[\ell] \simeq (\mathbb{Z}/\ell\mathbb{Z})^6$. Let $\pi(x, y) = (x^q, y^q)$ be the Frobenius endomorphism acting on C . This induces an endomorphism of the Jacobian, which we also call the Frobenius endomorphism and denote by π . This endomorphism induces a linear action on $J[\ell]$, which we represent by a matrix $T \in M_{6 \times 6}(\mathbb{F}_\ell)$.

If $T_\ell(J)$ is the Tate module of J and ρ is an endomorphism of J , we denote by $T_\ell(\rho)$ the corresponding element in $\text{End}_{\mathbb{Z}_\ell}(J)$.

Definition 2.1. We define the characteristic polynomial of the Frobenius as the characteristic polynomial of $T_\ell(\pi)$, that is,

$$P(X) := \det(XI_d - T_\ell(\pi))$$

The polynomial $P(X)$ has degree six, has integer coefficients, and is independent of ℓ by [5, Theorem 4.83]. As a consequence of the Weil conjectures, it can be written as

$$P(X) = X^6 - s_1 X^5 + s_2 X^4 - s_3 X^3 + s_2 q X^2 - s_1 q^2 X + q^3.$$

For details, see [5, Proposition 8.4]. We denote by

$$\tilde{P}(X) = X^6 - \tilde{s}_1 X^5 + \tilde{s}_2 X^4 - \tilde{s}_3 X^3 + \tilde{s}_2 q X^2 - \tilde{s}_1 \tilde{q}^2 X + \tilde{q}^3$$

the reduction of $P(X)$ modulo ℓ . The roots of $P(X)$ satisfy the following relations

Theorem 2.2 ([5, Theorem 5.76]). *Let $\alpha_1, \dots, \alpha_6$ be the roots of P .*

- (i) *Each α_i is an algebraic integer of degree ≤ 6 .*
- (ii) *We can numerate the roots such that, for $1 \leq i \leq 3$, we have*

$$\alpha_i \alpha_{i+3} = q.$$

- (iii) *For $1 \leq i \leq 6$, take any embedding of α_i into $\mathbb{C}$. Then the complex absolute value $|\alpha_i|$ is equal to $\sqrt{q}$.*

Proof. See [19, Theorem 5.1.15]. □

We will use the following notation:

- $[n_1]^{c_1} \dots [n_k]^{c_k}$ denotes a squarefree polynomial having c_i irreducible factors of degree n_i in $\mathbb{F}_\ell[X]$.
- $(n_1)^{c_1} \dots (n_k)^{c_k}$ describes the factorization pattern of the Galois orbit of ℓ -torsion points. Each n_i represents the degree of an irreducible factor, which corresponds to the size of a Galois orbit, and the exponent c_i denotes the number of distinct orbits of size n_i .

The factorization of $P(X)$ into irreducible factors $[n_1]^{c_1} \dots [n_k]^{c_k}$ over $\mathbb{F}_\ell$ determines the structure of $J[\ell]$. In fact, the decomposition of $J[\ell]$ into disjoint Galois orbits is determined by the factorization pattern of the characteristic polynomial $\tilde{P}(X)$. Each irreducible factor of degree n implies the existence of a Galois orbit with points defined over an extension of degree n .

The degrees n_i correspond to the degree of the extensions $\mathbb{F}_{\ell^n}$ which contain the eigenvalues of the matrix T . More precisely, if $\mathbb{F}_{\ell^n}$ is the minimal extension of $\mathbb{F}_\ell$ that contains all eigenvalues of T , it can be decomposed as

$$T = PAP^{-1},$$

where $A \in \text{GL}_6(\mathbb{F}_{\ell^n})$ is in Jordan canonical form and $P \in \text{GL}_6(\mathbb{F}_{\ell^n})$. For the details, see [17, Theorem 8.6].

Definition 2.3. *A square matrix A is called nilpotent if there exists a positive integer k such that $A^k = 0$. The smallest such integer k is called the index of nilpotence of A .*

Remark 2.4. It is easy to see that if $A \in M_{n \times n}$ is strictly upper triangular, then $A^n = 0$. In fact, the characteristic polynomial of A is $p(x) = x^n$ and, by the Cayley–Hamilton theorem, $p(A) = A^n = 0$.

3 ℓ -torsion pattern factorization

For hyperelliptic curves of genus three, the possible factorization types of the characteristic polynomial of Frobenius over $\mathbb{Z}$ are very restricted. Up to isogeny, the genuinely new cases are the irreducible type [6] and the completely split type [2][2][2]; all other factorization types correspond to Jacobians that are isogenous to products of Jacobians of genus-1 or genus-2 curves.

Theorem 3.1 ([21, Theorem 1]). *The possible characteristic polynomials of abelian varieties of dimension three over $\mathbb{F}_q$ (where $q = p^k$) are all $f(t) \in \mathbb{Z}[t]$ of degree six satisfying one of the following conditions:*

- (i) $f(t) = t^6 + a_1t^5 + a_2t^4 + a_3t^3 + a_2qt^2 + a_1q^2t + q^3$ whose roots are Weil numbers, $v_p(d(0))/k \in \mathbb{Z}$ for any irreducible factor $d(t)$ of $f(t)$ in $\mathbb{Q}_p[t]$, and the polynomial $t^3 + a_1t^2 + (a_2 - 3q)t + a_3 - 2qa_1$ is irreducible over $\mathbb{Q}$.
- (ii) $f(t) = (t^2 + \beta t + q)^3$, where β is equal to either
 - (a) $\beta = aq^{1/3}$ with $3 \mid k$, $p \nmid a$, and $|a| < 2q^{1/6}$.
 - (b) $\beta = \pm q^{2/3}$ with $q = 8$ or 27 .
- (iii) $f(t) = f_1(t)f_2(t)$, where $f_1(t)$ and $f_2(t)$ are the characteristic polynomials of abelian varieties of dimensions one and two, respectively.

The abelian varieties in case (i) and case (ii) are simple, and not simple in case (iii). The abelian varieties in case (ii) are supersingular.

When reducing modulo ℓ , however, these types may give rise to additional phenomena, such as repeated factors and nontrivial nilpotent parts in the Frobenius action. For this reason, the case [2][2][2] plays a central role in genus three and accounts for the most significant new situations in our analysis.

3.1 Classification of the characteristic polynomial of the Frobenius endomorphism

We analyse all possible reductions of the Frobenius endomorphism matrix and derive the corresponding ℓ -factorization patterns. This classification is based on the possible factorizations of the minimal and characteristic polynomials of the Frobenius endomorphism π .

Lemma 3.2. *If the characteristic polynomial of the Frobenius endomorphism has a quintuple root modulo ℓ , then the multiplicity is actually six.*

Proof. Let $\tilde{P}(X) = (X - A)^5(X - B)$ be the characteristic polynomial of π modulo ℓ . By Weil's theorem, if λ is a root of the characteristic polynomial of π , then q/λ is also a root of it. Therefore we have $A^2 \equiv q \pmod{\ell}$ and $AB \equiv q \pmod{\ell}$. But q is nonzero modulo ℓ , so that $A \equiv B \pmod{\ell}$. $\square$

Lemma 3.3. *Suppose that $\tilde{P}(X) \in \mathbb{F}_\ell[X]$ has an irreducible factor of degree three. Then its factorization pattern is necessarily $[3][3]$.*

Proof. Let $\alpha, \beta, \gamma \in \mathbb{F}_{\ell^3} \setminus \mathbb{F}_\ell$ be the roots of the irreducible cubic factor of $\tilde{P}(X)$. By Theorem 2.2 there exists a root, say γ , such that $\gamma = \tilde{q}/\gamma'$ where γ' is a root of the remaining factors. If γ' were a root of a quadratic or linear polynomial, it would imply that γ also belongs to $\mathbb{F}_{\ell^2}$, which is a contradiction. Therefore, $\gamma' \in \mathbb{F}_{\ell^3} \setminus \mathbb{F}_\ell$ and the remaining factor must be an irreducible cubic polynomial. $\square$

Lemma 3.4. *Suppose that $\tilde{P}(X) \in \mathbb{F}_\ell[X]$ has linear irreducible factors of the form $(X - \alpha)^3(X - \beta)^2$, for some nonzero $\alpha, \beta \in \mathbb{F}_\ell$. Then its factorization pattern is necessarily $[1]^4[1]^2$ or $[1]^3[1]^3$.*

Proof. It is enough to observe that if $(X - \gamma)$ is the remaining linear factor, then q/γ is equal to α or β . $\square$

The Jordan form of the Frobenius endomorphism on $J[\ell]$ is strongly constrained by the arithmetic and symplectic structure of the Jacobian. In particular, when π has a unique eigenvalue in $\mathbb{F}_\ell$, not every non-semisimple Jordan configuration can occur. The following lemma excludes several highly non-diagonalizable cases in genus three.

Lemma 3.5. *Let C be a hyperelliptic curve of genus three defined over a finite field $\mathbb{F}_q$, and let π be the Frobenius endomorphism acting on $J[\ell]$, where $\ell \nmid q$. Suppose that π has a unique eigenvalue $A \in \mathbb{F}_\ell$. Then the Jordan form of π cannot be $[1]^5[1]$, $[1]^3[1]^2[1]$ or $[1]^3[1][1][1]$.*

Proof. Suppose that the Jordan form of π is $[1]^5[1]$. Let $V \subset \mathbb{F}_\ell^6$ be a π -stable subspace of dimension 5. If A is the only eigenvalue of π in $\mathbb{F}_\ell$, then there exists a basis $\{D_1, D_2, D_3, D_4, D_5\}$ of V such that the action of π on a basis $\{D_1, D_2, D_3, D_4, D_5, D_6\}$ of $\mathbb{F}_\ell^6$ is given by the matrix

$$\begin{pmatrix} A & 1 & 0 & 0 & 0 & 0 \\ 0 & A & 1 & 0 & 0 & 0 \\ 0 & 0 & A & 1 & 0 & 0 \\ 0 & 0 & 0 & A & 1 & 0 \\ 0 & 0 & 0 & 0 & A & 0 \\ 0 & 0 & 0 & 0 & 0 & A \end{pmatrix}.$$

Following the idea in [7], we can use the Weil pairing on $J[C]$. For any points $R, S \in J[\ell]$, the Weil pairing satisfies $e_\ell(R, S)^q = e_\ell(\pi(R), \pi(S))$. Considering that $\pi(D_1) = AD_1$, $\pi(D_i) = AD_i + D_{i-1}$ for $i \in \{2, 3, 4, 5\}$ and $\pi(D_6) = AD_6$, then $e_\ell(D_1, D_i) = 1$ for all $i \in \{2, 3, 4, 5\}$. In fact, we have that

$$e_\ell(D_1, D_i)^q = e_\ell(AD_1, AD_i + D_{i-1}) = e_\ell(D_1, D_i)^{A^2} e_\ell(D_1, D_{i-1})^A.$$

We know that $q \equiv A^2 \pmod{\ell}$ and $e_\ell(\cdot, \cdot)$ takes values in the ℓ^{th} roots of unity in $\overline{\mathbb{F}}_q$, so

$$1 = e_\ell(D_1, D_{i-1})^A.$$

Type	Factorization patterns of the characteristic polynomial
I	[6]
II	[3][3]
III	[4][2]
IV	[4][1][1], [4][1] ²
V	[2][2][2], [2] ² [2], [2] ³
VI	[2][2][1][1], [2][2][1] ² , [2] ² [1][1], [2] ² [1] ²
VII	[2][1] ⁴ , [2][1] ² [1] ² , [2][1] ² [1][1], [2][1][1][1][1]
VIII	[1] ² [1] ⁴ , [1] ² [1] ² [1] ² , [1] ² [1] ² [1][1], [1] ² [1][1][1][1], [1] ³ [1] ³ , [1][1][1][1][1][1], [1] ⁶

Table 1: Factorization types of the characteristic polynomial of the Frobenius endomorphism for genus-3 curves.

Since $A \in \mathbb{F}_\ell^\times$, this implies $e_\ell(D_1, D_{i-1}) = 1$. Applying the same argument to $e_\ell(D_2, D_4)$ and $e_\ell(D_3, D_4)$, we successively obtain $e_\ell(D_2, D_3) = e_\ell(D_2, D_4) = 1$. Finally, substituting these relations into the identity for $e_\ell(D_2, D_5)$, we deduce $e_\ell(D_1, D_5) = 1$.

Finally, from

$$\begin{aligned} e_\ell(D_2, D_6)^q &= e_\ell(AD_2 + D_1, AD_6) \\ &= e_\ell(D_2, D_6)^{A^2} e_\ell(D_1, D_6)^A \end{aligned}$$

we obtain $e_\ell(D_1, D_6) = 1$, which contradicts the non-degeneracy of the Weil pairing.

For the remaining patterns, the same principle applies. In fact, in both cases there is a Jordan block of dimension 3. Let $\{D_1, D_2, D_3\}$ be a basis of the invariant subspace such that the action of π is the following: $\pi(D_1) = AD_1$, $\pi(D_2) = AD_2 + D_1$ and $\pi(D_3) = AD_3 + D_2$. As in the previous cases, it is possible to prove that $e_\ell(D_1, D_2) = e_\ell(D_1, D_3) = 1$. If the Jordan form is $[1]^3[1][1][1]$, then there is a basis $\{D_1, D_2, D_3, F_4, F_5, F_6\}$ such that $\pi(F_i) = AF_i$, for $i = 4, 5, 6$. It follows that $e_\ell(D_1, F_i) = 1$. Finally, if we are in the case $[1]^3[1]^2[1]$, the block of dimension two has a basis $\{E_1, E_2\}$ such that $\pi(E_1) = AE_1$, $\pi(E_2) = AE_2 + E_1$ and $e_\ell(D_1, E_1) = e_\ell(D_1, E_2) = 1$. $\square$

Corollary 3.6. *The factorization types of the characteristic polynomial are listed in Table 1.*

3.2 Factorization pattern

Having classified the possible matrices, we can now show how to obtain factorization patterns from them. Following the approach of Gaudry and Schost [7], we provide the details for the case with $P(x) = p(x)^3$ where $p(x)$ is an irreducible polynomial of degree two. The remaining cases follow by analogy.

We will use the following result.

Lemma 3.7 ([15, Lemma 1]). *Let D be a point in $J[\ell]$ and let*

$$V_D := \text{Span}_{\mathbb{F}_\ell} \{ \pi^n(D), n \in \mathbb{N} \}.$$

Let P be the minimal polynomial of π restricted to V_D . Then the degree of extension of $\mathbb{F}_q$ where D is defined is

$$o(P) := \min \{ k \in \mathbb{N}^* : x^k - 1 = 0 \bmod P \}.$$

We first provide a counting lemma valid for a general companion block, from which the individual cases can be deduced by combining such blocks.

Lemma 3.8. *Let A_d be the block associated with an irreducible polynomial $p(x)$ of degree d , and let n be its length. For each $1 \leq k \leq n$, the number of elements annihilated by $p(x)^k$ but not by $p(x)^{k-1}$ is*

$$\ell^{d(k-1)} (\ell^d - 1).$$

Proof. The subspace annihilated by $p(x)^k$ has dimension kd and hence contains $\ell^{kd} - 1$ nonzero elements. Similarly, the subspace annihilated by $p(x)^{k-1}$ has dimension $(k-1)d$ and contains $\ell^{(k-1)d} - 1$ nonzero elements. Therefore the number of elements annihilated by $p(x)^k$ but not by $p(x)^{k-1}$ is

$$(\ell^{kd} - 1) - (\ell^{(k-1)d} - 1) = \ell^{(k-1)d} (\ell^d - 1). \quad \square$$

Definition 3.9. *The companion matrix of the monic polynomial $p(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1} + x^n$ is*

$$C[p] = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 1 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 1 \\ -a_0 & -a_1 & \cdots & -a_{n-3} & -a_{n-2} & -a_{n-1} \end{pmatrix}.$$

Having established the degree of the field of definition for a divisor (Lemma 3.7) and the count of elements at a specific level within a single companion block (Lemma 3.8), we now extend this analysis to the entire vector space. Since the Frobenius matrix M decomposes as a direct sum of companion blocks, the choices of components in each block are independent. The following proposition provides the systematic method to compute the exact number of ℓ -torsion elements defined over a specific extension by combining these independent blocks.

Proposition 3.10. *Let $p_1(x), \dots, p_n(x)$ be distinct irreducible polynomials of degrees $d_1, \dots, d_n$, respectively, and consider the matrix*

$$M = \text{diag} \left(C[p_1^{e_{1,1}}], \dots, C[p_1^{e_{1,m_1}}], \dots, C[p_n^{e_{n,1}}], \dots, C[p_n^{e_{n,m_n}}] \right).$$

For elements with nonzero components in blocks $C[p_{i_1}^{e_{i_1,j_1}}], \dots, C[p_{i_r}^{e_{i_r,j_r}}]$ at levels $k_1, \dots, k_r$ (i.e., with minimal polynomials exactly $p_{i_s}^{k_s}(x)$, respectively), the following statements hold:

- (i) Their minimal polynomial is $\text{lcm} \left(p_{i_1}^{k_1}(x), \dots, p_{i_r}^{k_r}(x) \right)$.
- (ii) They are defined over an extension of degree $o \left(\text{lcm} \left(p_{i_1}^{k_1}(x), \dots, p_{i_r}^{k_r}(x) \right) \right)$.
- (iii) The total number of such elements is $\prod_{s=1}^r \ell^{d_{i_s}(k_s-1)} (\ell^{d_{i_s}} - 1)$.

Proof. For each block $C[p_i^{e_{i,j}}]$, Lemma 3.8 gives $\ell^{d_i(k-1)} (\ell^{d_i} - 1)$ elements at level k . Since the matrix M decomposes as a direct sum, a vector with nonzero component at level k_s in block $C[p_{i_s}^{e_{i_s,j_s}}]$ for $s = 1, \dots, r$ has minimal polynomial

$$\text{lcm} \left(p_{i_1}^{k_1}(x), \dots, p_{i_r}^{k_r}(x) \right).$$

The choices in each block are independent, so the number of such elements is

$$\prod_{s=1}^r \ell^{d_{i_s}(k_s-1)} (\ell^{d_{i_s}} - 1),$$

and the corresponding orbit degree is $o \left(\text{lcm} \left(p_{i_1}^{k_1}(x), \dots, p_{i_r}^{k_r}(x) \right) \right)$ by Lemma 3.7. $\square$

The fact that the minimal polynomial of a vector in a direct sum of invariant subspaces is the least common multiple of the minimal polynomials of its components follows from the order properties of modules over a principal ideal domain (for more details, see [17, Theorems 6.2 and 7.14]).

The matrix representing the Frobenius endomorphism with characteristic polynomial $P(x)$ admits three possible Jordan forms:

$$(i) \begin{pmatrix} A_2 & 0 & 0 \\ 0 & A_2 & 0 \\ 0 & 0 & A_2 \end{pmatrix}, \quad (ii) \begin{pmatrix} A_2 & I_2 & 0 \\ 0 & A_2 & I_2 \\ 0 & 0 & A_2 \end{pmatrix}, \quad (iii) \begin{pmatrix} A_2 & 0 & 0 \\ 0 & A_2 & I_2 \\ 0 & 0 & A_2 \end{pmatrix}.$$

We now describe the factorization of the Galois orbits for case (iii), as the remaining cases are similar.

We have that $M = \text{diag}(C[p^2], C[p])$.

- In the first level ($k = 1$) of the block $C[p^2]$, the elements have minimal polynomial $p(x)$. By Lemma 3.8, there are $\ell^{2(1-1)} (\ell^2 - 1) = \ell^2 - 1$ such elements, all defined over an extension of degree $o(p(x))$.
- In the second level ($k = 2$) of the block $C[p(x)^2]$, the elements have minimal polynomial $p(x)^2$. By Lemma 3.8, there are $\ell^{2(2-1)} (\ell^2 - 1) = \ell^2 (\ell^2 - 1)$ such elements, all defined over an extension of degree $o(p(x)^2)$.
- In the block $C[p]$, the elements have minimal polynomial $p(x)$. By Lemma 3.8, there are $\ell^{2(1-1)} (\ell^2 - 1) = \ell^2 - 1$ such elements, all defined over an extension of degree $o(p(x))$.

- Consider elements with nonzero components in both the first level of $C[p^2]$ and the block $C[p]$. Since $\text{lcm}(p(x), p(x)) = p(x)$, their minimal polynomial is $p(x)$. Hence there are $(\ell^2 - 1)^2$ such elements, all defined over an extension of degree $o(p(x))$.
- Consider elements with nonzero components in both the second level of $C[p^2]$ and the block $C[p]$. Since $\text{lcm}(p(x)^2, p(x)) = p(x)^2$, their minimal polynomial is $p(x)^2$. Hence there are $\ell^2(\ell^2 - 1)^2$ such elements, all defined over an extension of degree $o(p(x)^2)$.

The corresponding elements are grouped according to orbit size: $(\ell^2 - 1) + (\ell^2 - 1) + (\ell^2 - 1)^2 = \ell^4 - 1$ of degree $o(p(x))$ and $\ell^2(\ell^2 - 1) + \ell^2(\ell^2 - 1)^2 = \ell^4(\ell^2 - 1)$ of degree $o(p(x)^2)$.

Therefore the ℓ -torsion Galois orbits decomposition is

$$\left(o(p(x))\right)^{\frac{\ell^4-1}{o(p(x))}} \left(o(p(x)^2)\right)^{\frac{\ell^4(\ell^2-1)}{o(p(x)^2)}}.$$

Example 3.11. Consider the field $\mathbb{F}_5$ and the curve

$$C: y^2 = x^7 + 4x^3 + 3x$$

over $\mathbb{F}_5$. The characteristic polynomial of Frobenius acting on $T_\ell(\pi)$ is $(x^2 + 2x + 2)^3$.

Over $\mathbb{F}_3$, the polynomial $p(x) = x^2 + 2x + 2$ is irreducible. The elements contained in the subspace corresponding to the first blocks in rational form are defined over an extension of degree $o(p(x)) = 8$, while the remaining elements, which are in the next layer, are defined over an extension of degree $o(p(x)^2) = 24$. Then, its factorization of the 3-torsion Galois orbits is of the form $(8)^{10}(24)^{27}$. There are $10 = \frac{3^4-1}{8}$ Galois orbits of length 8 and $27 = \frac{3^4(3^2-1)}{24}$ Galois orbits of length 24. Therefore, the number of nonzero 3-torsion points accounted for is

$$10 \cdot 8 + 27 \cdot 24 = 80 + 648 = 728 = 3^6 - 1.$$

This agrees with the fact that $J[3]$ is a 6-dimensional $\mathbb{F}_3$ -vector space. Consequently, the 3-torsion has rank 4 over $\mathbb{F}_{p^8}$ and full rank 6 over $\mathbb{F}_{p^{24}}$. Hence $J[3](\mathbb{F}_{p^8}) \simeq (\mathbb{Z}/3\mathbb{Z})^4$ and $J[3](\mathbb{F}_{p^{24}}) \simeq (\mathbb{Z}/3\mathbb{Z})^6$.

4 Upper bounds for extension degrees in genus three

Following Matsuo's approach, we analyze the upper bound for the extension degree of the field of definition of $J[\ell]$ for each type. Throughout this section we assume that $\ell \neq 2$, unless the case $\ell = 2$ is treated separately. For each factorization type of the characteristic polynomial modulo ℓ , we proceed as follows. First, we determine a finite extension of $\mathbb{F}_\ell$ over which the matrix representing the Frobenius endomorphism

Type	Char. polynomial	Max. extension degree	Worst case
I	[6]	$e(\ell^3 + 1)$	$\ell^4 - \ell^3 + \ell - 1$
II	[3][3]	$(\ell - 1)(\ell^2 + \ell + 1)$	$\ell^3 - 1$
III	[4][2]	$\text{lcm}(e(\ell^2 + 1), e(\ell + 1))$	$(\ell^4 - 1)/2$
IV	[4][1][1]	$e\ell(\ell^2 + 1)$	$\ell^4 - \ell^3 + \ell^2 - \ell$
V	[2][2][2]	$e\ell(\ell + 1)$	$\ell^3 - \ell$
VI	[2][2][1][1]	$(\ell - 1)\ell(\ell + 1)$	$\ell^3 - \ell$
VII	[2][1][1][1][1]	$\text{lcm}(e_r\ell^2, e(\ell + 1))$	$(\ell - 1)\ell^2(\ell + 1)/2$
VIII	[1][1][1][1][1][1]	$e_r\ell^2$	$(\ell - 1)\ell^2$

Table 2: Upper bounds of extension degrees.

becomes upper triangular, and identify the semisimple part of its action on $J[\ell]$. We then bound the exponent needed to annihilate the nilpotent contribution, which depends on the maximal size of the Jordan blocks. Combining these two ingredients yields an explicit upper bound for the degree of the field of definition of $J[\ell]$. We denote by

$$e = \#\langle \tilde{q} \rangle, \quad e_n = \#\langle -\tilde{q} \rangle,$$

the multiplicative orders of $\tilde{q}$ and $-\tilde{q}$ in $\mathbb{F}_\ell^\times$. If $\tilde{q}$ is a quadratic residue modulo ℓ , we denote by $e_r = \#\langle \sqrt{\tilde{q}} \rangle$ the multiplicative order of a fixed square root $\sqrt{\tilde{q}} \in \mathbb{F}_\ell^\times$. By Fermat's little theorem, all these orders divide $\ell - 1$. In order to obtain uniform bounds, we assume $e = e_n = e_r = \ell - 1$.

Type I

In this type, $\tilde{P}$ has six roots $\tilde{\alpha}, \tilde{\alpha}^\ell, \tilde{\alpha}^{\ell^2}, \tilde{\alpha}^{\ell^3}, \tilde{\alpha}^{\ell^4}, \tilde{\alpha}^{\ell^5} \in \mathbb{F}_{\ell^6} \setminus \mathbb{F}_{\ell^2}$ and $\mathbb{F}_{\ell^6} \setminus \mathbb{F}_{\ell^3}$, which are all distinct. Therefore, A can be defined over $\mathbb{F}_{\ell^6}$ as

$$A = \begin{pmatrix} \tilde{\alpha} & 0 & 0 & 0 & 0 & 0 \\ 0 & \tilde{\alpha}^\ell & 0 & 0 & 0 & 0 \\ 0 & 0 & \tilde{\alpha}^{\ell^2} & 0 & 0 & 0 \\ 0 & 0 & 0 & \tilde{\alpha}^{\ell^3} & 0 & 0 \\ 0 & 0 & 0 & 0 & \tilde{\alpha}^{\ell^4} & 0 \\ 0 & 0 & 0 & 0 & 0 & \tilde{\alpha}^{\ell^5} \end{pmatrix}.$$

From Theorem 2.2, we can see that

$$\tilde{\alpha}^{\ell^3+1} = \tilde{q} \in \mathbb{F}_\ell,$$

so that

$$A^{\ell^3+1} = \begin{pmatrix} \widetilde{q} & 0 & 0 & 0 & 0 & 0 \\ 0 & \widetilde{q} & 0 & 0 & 0 & 0 \\ 0 & 0 & \widetilde{q} & 0 & 0 & 0 \\ 0 & 0 & 0 & \widetilde{q} & 0 & 0 \\ 0 & 0 & 0 & 0 & \widetilde{q} & 0 \\ 0 & 0 & 0 & 0 & 0 & \widetilde{q} \end{pmatrix}.$$

For $D \in J[\ell]$, since $T^{e(\ell^3+1)} = PA^{e(\ell^3+1)}P^{-1} = I_6$, we have

$$D^{q^{e(\ell^3+1)}} - D = 0.$$

Therefore, we obtain

$$J[\ell] \subset J(\mathbb{F}_{q^{e(\ell^3+1)}}) \subset J(\mathbb{F}_{q^{\ell^4-\ell^3+\ell-1}}).$$

Type II

In this type, $\widetilde{P}$ has four roots $\widetilde{\alpha}_1, \widetilde{\alpha}_1^\ell, \widetilde{\alpha}_1^{\ell^2}, \widetilde{\alpha}_2, \widetilde{\alpha}_2^\ell \in \mathbb{F}_{\ell^2}, \widetilde{\alpha}_1^{\ell^3} \in \mathbb{F}_{\ell^3} \setminus \mathbb{F}_\ell$, which are all distinct. Therefore, A can be defined over $\mathbb{F}_{\ell^2}$ as

$$A = \begin{pmatrix} \widetilde{\alpha}_1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \widetilde{\alpha}_1^\ell & 0 & 0 & 0 & 0 \\ 0 & 0 & \widetilde{\alpha}_1^{\ell^2} & 0 & 0 & 0 \\ 0 & 0 & 0 & \widetilde{\alpha}_2 & 0 & 0 \\ 0 & 0 & 0 & 0 & \widetilde{\alpha}_2^\ell & 0 \\ 0 & 0 & 0 & 0 & 0 & \widetilde{\alpha}_2^{\ell^2} \end{pmatrix}.$$

Moreover,

$$N_{\mathbb{F}_{\ell^3}/\mathbb{F}_\ell}(\widetilde{\alpha}_i) = \widetilde{\alpha}_i^{\ell^2+\ell+1} \in \mathbb{F}_\ell \quad (i = 1, 2).$$

It follows that $A^{(\ell-1)(\ell^2+\ell+1)} = I_6$, and therefore

$$J[\ell] \subset J(\mathbb{F}_{q^{\ell^3-1}}).$$

Type III

In this type, $\widetilde{P}$ has four roots $\widetilde{\alpha}_1, \widetilde{\alpha}_1^\ell, \widetilde{\alpha}_1^{\ell^2} \in \mathbb{F}_{\ell^4} \setminus \mathbb{F}_{\ell^2}$, and $\widetilde{\alpha}_2, \widetilde{\alpha}_2^\ell \in \mathbb{F}_{\ell^2} \setminus \mathbb{F}_\ell$ which are all distinct. Therefore, A can be defined over $\mathbb{F}_{\ell^4}$ as

$$A = \begin{pmatrix} \widetilde{\alpha}_1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \widetilde{\alpha}_1^\ell & 0 & 0 & 0 & 0 \\ 0 & 0 & \widetilde{\alpha}_1^{\ell^2} & 0 & 0 & 0 \\ 0 & 0 & 0 & \widetilde{\alpha}_1^{\ell^3} & 0 & 0 \\ 0 & 0 & 0 & 0 & \widetilde{\alpha}_2 & 0 \\ 0 & 0 & 0 & 0 & 0 & \widetilde{\alpha}_2^\ell \end{pmatrix}.$$

Let A_4 (respectively, A_2) denote the companion matrix of the irreducible factor of degree four (respectively, two) of $\tilde{P}$. It follows that $A_4^{(\ell-1)(\ell^2+1)} = I_4$ and $A_2^{(\ell-1)(\ell+1)} = I_2$, therefore taking the least common multiple of these two orders yields

$$J[\ell] \subset J(\mathbb{F}_{q^{\text{lcm}(\ell^2+1, \ell+1)}}) \subset J(\mathbb{F}_{q^{(\ell^4-1)/2}}).$$

Type IV

In this type, $\tilde{P}$ has four roots $\tilde{\alpha}_1, \tilde{\alpha}_1^\ell, \tilde{\alpha}_1^{\ell^2}, \tilde{\alpha}_1^{\ell^3} \in \mathbb{F}_{\ell^4} \setminus \mathbb{F}_{\ell^2}$, and two roots $\tilde{\alpha}_2, \tilde{\alpha}_2^\ell \in \mathbb{F}_{\ell^2} \setminus \mathbb{F}_\ell$ which are all distinct. Therefore, A can be defined over $\mathbb{F}_{\ell^4}$ as

$$(i) \quad A = \begin{pmatrix} \tilde{\alpha}_1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \tilde{\alpha}_1^\ell & 0 & 0 & 0 & 0 \\ 0 & 0 & \tilde{\alpha}_1^{\ell^2} & 0 & 0 & 0 \\ 0 & 0 & 0 & \tilde{\alpha}_1^{\ell^3} & 0 & 0 \\ 0 & 0 & 0 & 0 & \tilde{\alpha}_2 & 0 \\ 0 & 0 & 0 & 0 & 0 & \tilde{\alpha}_2 \end{pmatrix}, \quad (ii) \quad A = \begin{pmatrix} \tilde{\alpha}_1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \tilde{\alpha}_1^\ell & 0 & 0 & 0 & 0 \\ 0 & 0 & \tilde{\alpha}_1^{\ell^2} & 0 & 0 & 0 \\ 0 & 0 & 0 & \tilde{\alpha}_1^{\ell^3} & 0 & 0 \\ 0 & 0 & 0 & 0 & \tilde{\alpha}_2 & 1 \\ 0 & 0 & 0 & 0 & 0 & \tilde{\alpha}_2 \end{pmatrix},$$

$$(iii) \quad A = \begin{pmatrix} \tilde{\alpha}_1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \tilde{\alpha}_1^\ell & 0 & 0 & 0 & 0 \\ 0 & 0 & \tilde{\alpha}_1^{\ell^2} & 0 & 0 & 0 \\ 0 & 0 & 0 & \tilde{\alpha}_1^{\ell^3} & 0 & 0 \\ 0 & 0 & 0 & 0 & \tilde{\alpha}_2 & 0 \\ 0 & 0 & 0 & 0 & 0 & \tilde{\alpha}_3 \end{pmatrix}.$$

As in Type III, taking the least common multiple of these two orders yields

$$J[\ell] \subset J(\mathbb{F}_{q^{\text{lcm}(\ell^2+1, \ell+1)}}) \subset J(\mathbb{F}_{q^{(\ell^4-1)/2}}).$$

Type V

In this type, $\tilde{P}$ has six roots in $\mathbb{F}_{\ell^2} \setminus \mathbb{F}_\ell$. The cases $[2]^3$, $[2]^2[2]$ and $[2][2][2]$ are possible. Because the cases $[2]^3$ and $[2]^2[2]$ have roots with multiplicity greater than one, the corresponding matrices may admit a non-trivial nilpotent part, which can increase the extension degree. We therefore analyze the worst cases. Here $\tilde{\alpha}$ and $\tilde{\alpha}_1$ denote elements of $\mathbb{F}_{\ell^2} \setminus \mathbb{F}_\ell$, and $\tilde{\alpha}^\ell$ and $\tilde{\alpha}_1^\ell$ their Galois conjugates. Among all configurations compatible with this factorization pattern, cases (i) and (ii) yield the largest possible nilpotent blocks and therefore lead to the largest extension degree. We

have

$$(i) \quad A = \begin{pmatrix} \tilde{\alpha} & 1 & 0 & 0 & 0 & 0 \\ 0 & \tilde{\alpha} & 0 & 0 & 0 & 0 \\ 0 & 0 & \tilde{\alpha}^\ell & 1 & 0 & 0 \\ 0 & 0 & 0 & \tilde{\alpha}^\ell & 0 & 0 \\ 0 & 0 & 0 & 0 & \tilde{\alpha}_1 & 0 \\ 0 & 0 & 0 & 0 & 0 & \tilde{\alpha}_1^\ell \end{pmatrix}, \quad (ii) \quad A = \begin{pmatrix} \tilde{\alpha} & 1 & 0 & 0 & 0 & 0 \\ 0 & \tilde{\alpha} & 1 & 0 & 0 & 0 \\ 0 & 0 & \tilde{\alpha} & 0 & 0 & 0 \\ 0 & 0 & 0 & \tilde{\alpha}^\ell & 1 & 0 \\ 0 & 0 & 0 & 0 & \tilde{\alpha}^\ell & 1 \\ 0 & 0 & 0 & 0 & 0 & \tilde{\alpha}^\ell \end{pmatrix}.$$

- In case (i), we obtain

$$A^k = \begin{pmatrix} \tilde{\alpha}^k & k\tilde{\alpha}^{k-1} & 0 & 0 & 0 & 0 \\ 0 & \tilde{\alpha}^k & 0 & 0 & 0 & 0 \\ 0 & 0 & \tilde{\alpha}^{\ell k} & k\tilde{\alpha}^{\ell(k-1)} & 0 & 0 \\ 0 & 0 & 0 & \tilde{\alpha}^{\ell k} & 0 & 0 \\ 0 & 0 & 0 & 0 & \tilde{\alpha}_1^k & 0 \\ 0 & 0 & 0 & 0 & 0 & \tilde{\alpha}_1^{\ell k} \end{pmatrix}.$$

$A^{e^\ell(\ell+1)} = I_6$ or $A^{e_n\ell(\ell+1)} = I_6$. Therefore we have

$$J[\ell] \subset J(\mathbb{F}_{q^{e^\ell(\ell+1)}}) \subset J(\mathbb{F}_{q^{\ell^3-\ell}}).$$

or

$$J[\ell] \subset J(\mathbb{F}_{q^{e_n\ell(\ell+1)}}) \subset J(\mathbb{F}_{q^{\ell^3-\ell}}).$$

- In case (ii), we deduce

$$A^k = \begin{pmatrix} \tilde{\alpha}^k & \binom{k}{1}\tilde{\alpha}^{k-1} & \binom{k}{2}\tilde{\alpha}^{k-2} & 0 & 0 & 0 \\ 0 & \tilde{\alpha}^k & \binom{k}{1}\tilde{\alpha}^{k-1} & 0 & 0 & 0 \\ 0 & 0 & \tilde{\alpha}^k & 0 & 0 & 0 \\ 0 & 0 & 0 & \tilde{\alpha}^{\ell k} & \binom{k}{1}\tilde{\alpha}^{\ell(k-1)} & \binom{k}{2}\tilde{\alpha}^{\ell(k-2)} \\ 0 & 0 & 0 & 0 & \tilde{\alpha}^{\ell k} & \binom{k}{1}\tilde{\alpha}^{\ell(k-1)} \\ 0 & 0 & 0 & 0 & 0 & \tilde{\alpha}^{\ell k} \end{pmatrix}.$$

Therefore,

$$J[\ell] \subset J(\mathbb{F}_{q^{e^\ell(\ell+1)}}) \subset J(\mathbb{F}_{q^{\ell^3-\ell}}).$$

Remark 4.1. If $\ell = 2$, then

$$J[\ell] \subset J(\mathbb{F}_{q^{e^\ell(\ell+1)}}) \subset J(\mathbb{F}_{q^{\ell^4-\ell^2}}).$$

Type VI

In this type, $\tilde{P}$ has four roots in $\mathbb{F}_{\ell^2} \setminus \mathbb{F}_\ell$ and two roots in $\mathbb{F}_\ell$. The cases $[2]^2[1]^2$, $[2]^2[1][1]$, and $[2][2][1]^2$, $[2][2][1][1]$ are possible. Because the cases $[2]^2[1]^2$, $[2]^2[1][1]$, and $[2][2][1]^2$ have roots with multiplicity greater than one, the possible matrices could have a nilpotent part that increases the bound, so we will analyze the worst cases. For some $\tilde{\alpha}, \tilde{\alpha}^\ell, \tilde{\alpha}, \tilde{\alpha}^\ell, \tilde{\alpha}_1, \tilde{\alpha}_1 \in \mathbb{F}_\ell$ we have

$$A = \begin{pmatrix} \tilde{\alpha} & 1 & 0 & 0 & 0 & 0 \\ 0 & \tilde{\alpha} & 0 & 0 & 0 & 0 \\ 0 & 0 & \tilde{\alpha}^\ell & 1 & 0 & 0 \\ 0 & 0 & 0 & \tilde{\alpha}^\ell & 0 & 0 \\ 0 & 0 & 0 & 0 & \tilde{\alpha}_1 & 1 \\ 0 & 0 & 0 & 0 & 0 & \tilde{\alpha}_1 \end{pmatrix},$$

$$A^k = \begin{pmatrix} \tilde{\alpha}^k & k\tilde{\alpha}^{k-1} & 0 & 0 & 0 & 0 \\ 0 & \tilde{\alpha}^k & 0 & 0 & 0 & 0 \\ 0 & 0 & \tilde{\alpha}^{\ell k} & k\tilde{\alpha}^{\ell(k-1)} & 0 & 0 \\ 0 & 0 & 0 & \tilde{\alpha}^{\ell k} & 0 & 0 \\ 0 & 0 & 0 & 0 & \tilde{\alpha}_1^k & k\tilde{\alpha}_1^{k-1} \\ 0 & 0 & 0 & 0 & 0 & \tilde{\alpha}_1^k \end{pmatrix}.$$

Therefore

$$J[\ell] \subset J(\mathbb{F}_{q^{\ell(\ell+1)}}) \subset J(\mathbb{F}_{q^{\ell^3-\ell}}).$$

Type VII

In this type, $\tilde{P}$ has two roots $\tilde{\alpha}_1, \tilde{\alpha}_1^\ell \in \mathbb{F}_{\ell^2} \setminus \mathbb{F}_\ell$ and a quadruple root $\tilde{\alpha} \in \mathbb{F}_\ell$. Therefore A can be given over $\mathbb{F}_{\ell^2}$ in the worst case as

$$A = \begin{pmatrix} \tilde{\alpha} & 1 & 0 & 0 & 0 & 0 \\ 0 & \tilde{\alpha} & 1 & 0 & 0 & 0 \\ 0 & 0 & \tilde{\alpha} & 1 & 0 & 0 \\ 0 & 0 & 0 & \tilde{\alpha} & 0 & 0 \\ 0 & 0 & 0 & 0 & \tilde{\alpha}_1 & 0 \\ 0 & 0 & 0 & 0 & 0 & \tilde{\alpha}_1^\ell \end{pmatrix}.$$

Thus,

$$A^k = \begin{pmatrix} \tilde{\alpha}^k & \binom{k}{1}\tilde{\alpha}^{k-1} & \binom{k}{2}\tilde{\alpha}^{k-2} & \binom{k}{3}\tilde{\alpha}^{k-3} & 0 & 0 \\ 0 & \tilde{\alpha}^k & \binom{k}{1}\tilde{\alpha}^{k-1} & \binom{k}{2}\tilde{\alpha}^{k-2} & 0 & 0 \\ 0 & 0 & \tilde{\alpha}^k & \binom{k}{1}\tilde{\alpha}^{k-1} & 0 & 0 \\ 0 & 0 & 0 & \tilde{\alpha}^k & 0 & 0 \\ 0 & 0 & 0 & 0 & \tilde{\alpha}_1^k & 0 \\ 0 & 0 & 0 & 0 & 0 & \tilde{\alpha}_1^{\ell k} \end{pmatrix}$$

holds for any $k \in \mathbb{N}$. Therefore, for $\ell \notin \{2, 3\}$, we have

$$J[\ell] \subset J(\mathbb{F}_{q^{\text{lcm}(e_r, \ell, e(\ell+1))}}),$$

and, for $\ell \in \{2, 3\}$, we have

$$J[\ell] \subset J(\mathbb{F}_{q^{\text{lcm}(e_r, \ell^2, e(\ell+1))}}).$$

Type VIII

In this type, $\tilde{P}$ has a sixfold root $\tilde{\alpha} = \sqrt[6]{q} \in \mathbb{F}_\ell$. In the worst nilpotent case, A can be given over $\mathbb{F}_\ell$ as

$$A = \begin{pmatrix} \tilde{\alpha} & 1 & 0 & 0 & 0 & 0 \\ 0 & \tilde{\alpha} & 1 & 0 & 0 & 0 \\ 0 & 0 & \tilde{\alpha} & 1 & 0 & 0 \\ 0 & 0 & 0 & \tilde{\alpha} & 1 & 0 \\ 0 & 0 & 0 & 0 & \tilde{\alpha} & 1 \\ 0 & 0 & 0 & 0 & 0 & \tilde{\alpha} \end{pmatrix},$$

and

$$A^k = \begin{pmatrix} \tilde{\alpha}^k & \binom{k}{1}\tilde{\alpha}^{k-1} & \binom{k}{2}\tilde{\alpha}^{k-2} & \binom{k}{3}\tilde{\alpha}^{k-3} & \binom{k}{4}\tilde{\alpha}^{k-4} & \binom{k}{5}\tilde{\alpha}^{k-5} \\ 0 & \tilde{\alpha}^k & \binom{k}{1}\tilde{\alpha}^{k-1} & \binom{k}{2}\tilde{\alpha}^{k-2} & \binom{k}{3}\tilde{\alpha}^{k-3} & \binom{k}{4}\tilde{\alpha}^{k-4} \\ 0 & 0 & \tilde{\alpha}^k & \binom{k}{1}\tilde{\alpha}^{k-1} & \binom{k}{2}\tilde{\alpha}^{k-2} & \binom{k}{3}\tilde{\alpha}^{k-3} \\ 0 & 0 & 0 & \tilde{\alpha}^k & \binom{k}{1}\tilde{\alpha}^{k-1} & \binom{k}{2}\tilde{\alpha}^{k-2} \\ 0 & 0 & 0 & 0 & \tilde{\alpha}^k & \binom{k}{1}\tilde{\alpha}^{k-1} \\ 0 & 0 & 0 & 0 & 0 & \tilde{\alpha}^k \end{pmatrix}.$$

holds for any $k \in \mathbb{N}$. Then, for $\ell \notin \{2, 3, 5\}$, we have

$$J[\ell] \subset J(\mathbb{F}_{q^{e_r \ell}}) \subset J(\mathbb{F}_{q^{\ell^2 - \ell}})$$

from $A^{e_r \ell} = I_4$ and, for $\ell \in \{3, 5\}$, we have

$$J[\ell] \subset J(\mathbb{F}_{q^{e_r \ell^2}}) \subset J(\mathbb{F}_{q^{\ell^3 - \ell^2}})$$

Finally, for $\ell = 2$, we have

$$J[\ell] \subset J(\mathbb{F}_{q^{e\ell^3}}) \subset J(\mathbb{F}_{q^{\ell^4-\ell^3}}).$$

Theorem 4.2. *If $\ell > 2$, there exists a positive integer $d \leq \ell^4 - \ell^3 + \ell - 1$ such that*

$$J[\ell] \subset J(\mathbb{F}_{q^d}).$$

Proof. The bounds obtained for Types I–VIII are summarized in Table 2 on page 12. The maximal value is attained in Type I and equals $e(\ell^3 + 1)$. Since $e \mid (\ell - 1)$,

$$e(\ell^3 + 1) \leq (\ell - 1)(\ell^3 + 1) = \ell^4 - \ell^3 + \ell - 1.$$

This proves the theorem. $\square$

The following example shows that the bound of Theorem 4.2 is attained for $\ell = 3$.

Example 4.3. Consider $p = 5$ and the curve

$$C: y^2 = x^7 + x^2 + 3x + 1$$

over $\mathbb{F}_p$. The characteristic polynomial of Frobenius acting on $T_\ell(\pi)$ is $x^6 + 2x^4 + 2x^3 + x^2 + 2$. Then, its factorization of the 3-torsion Galois orbits is of the form $(56)^{13}$. Consequently, the full 3-torsion is defined over $\mathbb{F}_{p^{56}}$. Hence

$$J[3](\mathbb{F}_{p^{56}}) \simeq (\mathbb{Z}/3\mathbb{Z})^6.$$

In particular, the bound $56 = 3^4 - 3^3 + 3 - 1$ is attained.

Remark 4.4. The bounds obtained in genus two and three suggest a common underlying pattern. Let J be an abelian variety of dimension g defined over a finite field, and let $\ell \neq p$ be a prime. The Frobenius action on $J[\ell]$ is represented by a $2g \times 2g$ matrix, whose largest possible Jordan block has size at most $2g$. We observed for hyperelliptic curves of genus two and three that, for sufficiently large ℓ , the worst case arises in two situations: when $p(x)$ is irreducible of degree $2g$, or when $g = g_1 + \cdots + g_r$ (corresponding to the case where the Jacobian is isogenous to a product of Jacobians of lower-genus curves). In these cases, the bounds are respectively $(\ell - 1)(\ell^g + 1)$ and $(\ell - 1) \prod_{i=1}^r (\ell^{g_i} + 1)$, both of order $O(\ell^{g+1})$. On the other hand, the nilpotent part is annihilated by an ℓ -power ℓ^r . In particular, for $\ell > g$, a power of order $\ell^2 > 2g$ suffices to annihilate the nilpotent contribution. As a consequence, the nilpotent part cannot dominate the growth coming from the largest semisimple block.

This provides a heuristic explanation for the appearance of bounds of order $O(\ell^{g+1})$ in genus two and three.

5 Supplementary data

Tables 3 and 4 enumerate factorization patterns of the characteristic polynomial of the Frobenius endomorphism and, for each, lists the corresponding possible Jordan decompositions of the Frobenius endomorphism on $J[\ell]$. Tables 5 and 6 enumerate characteristic polynomials over $\mathbb{F}_2$ and corresponding Frobenius action on $J[2]$ and, for each, give the factorization type of the 2-torsion Galois orbits.

Type	Factorization	Decompositions	
I	[6]	(A_6)	
II	[3][3]	$\begin{pmatrix} A_3 & 0 \\ 0 & B_3 \end{pmatrix}$	
III	[4][2]	$\begin{pmatrix} A_4 & 0 \\ 0 & B_2 \end{pmatrix}$	
IV	[4][1][1]	$\begin{pmatrix} A_4 & 0 \\ 0 & b & 0 \\ & 0 & c \end{pmatrix}$	
	[4][1] ²	$\begin{pmatrix} A_4 & 0 \\ 0 & b & 0 \\ & 0 & b \end{pmatrix}$	$\begin{pmatrix} A_4 & 0 \\ 0 & b & 1 \\ & 0 & b \end{pmatrix}$
V	[2][2][2]	$\begin{pmatrix} A_2 & 0 & 0 \\ 0 & B_2 & 0 \\ 0 & 0 & C_2 \end{pmatrix}$	
	[2] ² [2]	$\begin{pmatrix} A_2 & 0 & 0 \\ 0 & A_2 & 0 \\ 0 & 0 & B_2 \end{pmatrix}$	$\begin{pmatrix} A_2 & * & 0 \\ 0 & A_2 & 0 \\ 0 & 0 & B_2 \end{pmatrix}$
	[2] ³	$\begin{pmatrix} A_2 & 0 & 0 \\ 0 & A_2 & 0 \\ 0 & 0 & A_2 \end{pmatrix}$	$\begin{pmatrix} A_2 & * & * \\ 0 & A_2 & * \\ 0 & 0 & A_2 \end{pmatrix} \quad \begin{pmatrix} A_2 & 0 & 0 \\ 0 & A_2 & * \\ 0 & 0 & A_2 \end{pmatrix}$
VI	[2][2][1][1]	$\begin{pmatrix} A_2 & 0 & 0 \\ 0 & B_2 & 0 \\ 0 & 0 & c & 0 \\ & 0 & 0 & d \end{pmatrix}$	
	[2][2][1] ²	$\begin{pmatrix} A_2 & 0 & 0 \\ 0 & B_2 & 0 \\ 0 & 0 & c & 0 \\ & 0 & 0 & c \end{pmatrix}$	$\begin{pmatrix} A_2 & 0 & 0 \\ 0 & B_2 & 0 \\ 0 & 0 & c & 1 \\ & 0 & 0 & c \end{pmatrix}$
	[2] ² [1][1]	$\begin{pmatrix} A_2 & 0 & 0 \\ 0 & A_2 & 0 \\ 0 & 0 & b & 0 \\ & 0 & 0 & c \end{pmatrix}$	$\begin{pmatrix} A_2 & * & 0 \\ 0 & A_2 & 0 \\ 0 & 0 & b & 0 \\ & 0 & 0 & b \end{pmatrix}$
	[2] ² [1] ²	$\begin{pmatrix} A_2 & 0 & 0 \\ 0 & A_2 & 0 \\ 0 & 0 & b & 0 \\ & 0 & 0 & b \end{pmatrix}$	$\begin{pmatrix} A_2 & 0 & 0 \\ 0 & A_2 & 0 \\ 0 & 0 & b & 1 \\ & 0 & 0 & b \end{pmatrix} \quad \begin{pmatrix} A_2 & * & 0 \\ 0 & A_2 & 0 \\ 0 & 0 & b & 0 \\ & 0 & 0 & b \end{pmatrix} \quad \begin{pmatrix} A_2 & * & 0 \\ 0 & A_2 & 0 \\ 0 & 0 & b & 1 \\ & 0 & 0 & b \end{pmatrix}$
VII	[2][1] ⁴	$\begin{pmatrix} A_2 & 0 \\ 0 & b & 0 & 0 & 0 \\ & 0 & b & 0 & 0 \\ & 0 & 0 & b & 0 \\ & 0 & 0 & 0 & b \end{pmatrix}$	$\begin{pmatrix} A_2 & 0 \\ 0 & b & 1 & 0 & 0 \\ & 0 & b & 0 & 0 \\ & 0 & 0 & b & 0 \\ & 0 & 0 & 0 & b \end{pmatrix} \quad \begin{pmatrix} A_2 & 0 \\ 0 & b & 1 & 0 & 0 \\ & 0 & b & 0 & 0 \\ & 0 & 0 & b & 1 \\ & 0 & 0 & 0 & b \end{pmatrix} \quad \begin{pmatrix} A_2 & 0 \\ 0 & b & 1 & 0 & 0 \\ & 0 & b & 0 & 1 \\ & 0 & 0 & b & 1 \\ & 0 & 0 & 0 & b \end{pmatrix}$
	[2][1] ² [1] ²	$\begin{pmatrix} A_2 & 0 \\ 0 & b & 0 & 0 & 0 \\ & 0 & b & 0 & 0 \\ & 0 & 0 & c & 0 \\ & 0 & 0 & 0 & c \end{pmatrix}$	$\begin{pmatrix} A_2 & 0 \\ 0 & b & 1 & 0 & 0 \\ & 0 & b & 0 & 0 \\ & 0 & 0 & c & 0 \\ & 0 & 0 & 0 & c \end{pmatrix} \quad \begin{pmatrix} A_2 & 0 \\ 0 & b & 1 & 0 & 0 \\ & 0 & b & 0 & 0 \\ & 0 & 0 & c & 1 \\ & 0 & 0 & 0 & c \end{pmatrix}$
	[2][1] ² [1][1]	$\begin{pmatrix} A_2 & 0 \\ 0 & b & 0 & 0 & 0 \\ & 0 & b & 0 & 0 \\ & 0 & 0 & c & 0 \\ & 0 & 0 & 0 & d \end{pmatrix}$	$\begin{pmatrix} A_2 & 0 \\ 0 & b & 1 & 0 & 0 \\ & 0 & b & 0 & 0 \\ & 0 & 0 & c & 0 \\ & 0 & 0 & 0 & d \end{pmatrix}$
	[2][1][1][1][1]	$\begin{pmatrix} A_2 & 0 \\ 0 & b & 0 & 0 & 0 \\ & 0 & c & 0 & 0 \\ & 0 & 0 & d & 0 \\ & 0 & 0 & 0 & e \end{pmatrix}$	

Table 3: Factorization patterns of the Frobenius characteristic polynomial and corresponding possible decompositions of the Frobenius endomorphism on $J[\ell]$; Types I–VII.

Type	Characteristic Polynomial	Matrix	Orbits
I	$x^6 + x^3 + 1$	$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$	$(9)^7$
II	$(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1)$	$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$	$(3)(5)^3(15)^3$
III	$(x^4 + x^3 + x^2 + x + 1)(x + 1)^2$	$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$	$(1)^3(5)^{12}$
		$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$	$(1)(2)(5)^6(10)^3$
IV	$(x^3 + x^2 + 1)(x^3 + x + 1)$	$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}$	$(7)^9$
V	$(x^2 + x + 1)^3$	$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$	$(3)^{21}$
		$\begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$	$(3)^1(6)^2(12)^4$
		$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$	$(3)^5 6^8$
VI	$(x^2 + x + 1)^2(x + 1)^2$	$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$	$(1)^3(3)^{20}$
		$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$	$(1)(2)(3)^{10}(6)^5$
		$\begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$	$(1)^3(3)^4(6)^8$
		$\begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$	$(1)(2)(3)^2(6)^9$

Table 5: Characteristic polynomials over $\mathbb{F}_2$, corresponding Frobenius action on $J[2]$ and factorization type of the 2-torsion Galois orbits; Types I–VI.

Type	Characteristic Polynomial	Matrix	Orbits
VII	$(x^2 + x + 1)(x + 1)^4$	$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$	$(1)^{15}(3)^{16}$
		$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$	$(1)^7(2)^4(3)^8(6)^4$
		$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$	$(1)^3(2)^6(3)^4(6)^6$
		$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$	$(1)(2)(3)^2(4)^3(6)$
VIII	$(x + 1)^6$	$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$	$(1)(2)(4)^3(8)^6$
		$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$	$(1)^3(2)^6(4)^{12}$
		$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$	$(1)^7(2)^4(4)^{12}$
		$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$	$(1)^3(2)^6(4)^{12}$
		$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$	$(1)^7(2)^{28}$
		$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$	$(1)^{15}(2)^{24}$
		$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$	$(1)^{31}(2)^{16}$
		$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$	$(1)^{63}$

Table 6: Characteristic polynomials over $\mathbb{F}_2$, corresponding Frobenius action on $J[2]$ and factorization type of the 2-torsion Galois orbits; Types VII and VIII.

References

- [1] Simon Abeldard, Pierrick Gaudry, and Pierre-Jean Spaenlehauer. Counting points on genus-3 hyperelliptic curves with explicit real multiplication. In *Proceedings of the Thirteenth Algorithmic Number Theory Symposium*, volume 2 of *The Open Book Series*, pages 1–19. Mathematical Sciences Publishers, 2019. DOI: 10.2140/obs.2019.2.1.
- [2] Simon Abeldard, Pierrick Gaudry, and Pierre-Jean Spaenlehauer. Improved complexity bounds for counting points on hyperelliptic curves. *Foundations of Computational Mathematics*, 19(3):591–621, 2019. DOI: 10.1007/s10208-018-9392-1.
- [3] David G. Cantor. On the analogue of the division polynomials for hyperelliptic curves. *Journal für die reine und angewandte Mathematik*, 447:91–145, 1994. DOI: 10.1515/crll.1994.447.91.
- [4] David G. Cantor and Hans Zassenhaus. A new algorithm for factoring polynomials over finite fields. *Mathematics of Computation*, 36:587–592, 1981. DOI: 10.1090/S0025-5718-1981-0606517-5.
- [5] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren. *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. Chapman & Hall, 2005. DOI: 10.1201/9781420034981.
- [6] Elie Eid. Efficient computation of Cantor’s division polynomials of hyperelliptic curves over finite fields. *Journal of Symbolic Computation*, 117:68–100, 2023. DOI: 10.1016/j.jsc.2022.10.006.
- [7] Pierrick Gaudry and Éric Schost. Modular equations for hyperelliptic curves. *Mathematics of Computation*, 74(249):429–454, 2005. DOI: 10.1090/S0025-5718-04-01682-5.
- [8] Pierrick Gaudry and Robert Harley. Counting points on hyperelliptic curves over finite fields. In *Algorithmic Number Theory*, volume 1838 of *Lecture Notes in Computer Science*, pages 313–332. Springer, 2000. DOI: 10.1007/10722028.18.
- [9] Pierrick Gaudry and Éric Schost. Construction of secure random curves of genus 2 over prime fields. In *Advances in Cryptology*, volume 3027 of *Lecture Notes in Computer Science*, pages 239–256. Springer, 2004. DOI: 10.1007/978-3-540-24676-3.15.
- [10] Pierrick Gaudry and Éric Schost. Genus 2 point counting over prime fields. *Journal of Symbolic Computation*, 47(4):368–400, 2012. DOI: 10.1016/j.jsc.2011.09.003.
- [11] Tsukasa Ishiguro and Kazuto Matsuo. Fields of definition of torsion points on the Jacobians of genus 2 hyperelliptic curves over finite fields. In *The 6th Symposium on Cryptography and Information Security*, paper 2D4-6. The Institute of Electronics, Information and Communication Engineers, 2010.

- [12] Elvira Lupoian. Three-torsion subgroups and wild conductors of genus 3 hyperelliptic curves. *Journal of Number Theory*, 278:267–284, 2026. DOI: 10.1016/j.jnt.2025.04.015.
- [13] Josep M. Miret, Jordi Pujolàs, and Nicolas Thériault. On ℓ -th roots and division by ℓ . Preprint, 2004. DOI: 10.48550/arXiv.2403.06619.
- [14] Jonathan Pila. Frobenius maps of abelian varieties and finding roots of unity in finite fields. *Mathematics of Computation*, 55(192):745–763, 1990. DOI: 10.1090/S0025-5718-1990-1035941-X.
- [15] Edgardo Riquelme. Trisection for genus 2 curves in odd characteristic. *Applicable Algebra in Engineering, Communication and Computing*, 27(5):373–397, 2016. DOI: 10.1007/s00200-015-0282-3.
- [16] Edgardo Riquelme and Nicolas Thériault. Symbolic trisection polynomials for genus 2 curves in odd characteristic. *SIAM Journal on Discrete Mathematics*, 32(4):2421–2440, 2018. DOI: 10.1137/18M1167292.
- [17] Steven Roman. *Advanced Linear Algebra*. Volume 135 of *Graduate Texts in Mathematics*. Springer, 2008. DOI: 10.1007/978-0-387-72831-5.
- [18] René Schoof. Elliptic curves over finite fields and the computation of square roots mod p . *Mathematics of Computation*, 44(170):483–494, 1985. DOI: 10.1090/S0025-5718-1985-0777280-6.
- [19] Henning Stichtenoth. *Algebraic Function Fields and Codes*. Volume of *Universitext*. Springer, 1993. ISBN: 9783540564898.
- [20] Hugues Verduré. Factorisation patterns of division polynomials. *Proceedings of the Japan Academy, Series A*, 80(5):79–82, 2004. DOI: 10.3792/pjaa.80.79.
- [21] Chao-Ping Xing. The characteristic polynomials of abelian varieties of dimensions three and four over finite fields. *Science in China, Series A*, 37(2):147–150, 1994. DOI: 10.1360/ya1994-37-2-147.