MATIMYÁS MATEMATIKA
ISSN 0115-6926

Journal of the Mathematical Society of the Philippines
Vol. 49 No. 1 (2026) pp. 1-12

Generalized Parametric Families of Algebraic Points on the Hyperelliptic Curve Γ

Mohamadou M.D. Diallo
Mathematics and Applications Laboratory
Assane Seck University of Ziguinchor
Ziguinchor, Senegal
m.diallo1836@zig.univ.sn

Abstract

We provide a complete description of algebraic points of a given degree on the hyperelliptic curve Γ defined by the affine equation

$$y^2 = xf(x)g(x).$$

Our approach is based on the assumption that the Mordell–Weil group of the Jacobian of Γ over $\mathbb{Q}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Under this hypothesis, we classify all rational divisors and construct explicit bases of the Riemann–Roch spaces $\mathcal{L}(m\infty)$. We then define rational functions parametrized by $\sigma \in \{0, 1\}$, which allow the systematic construction of families of algebraic points of arbitrary degree. These results provide a clear and effective framework for understanding the arithmetic of the curve.

Keywords: Jacobians, divisors and linear systems, rational points

2020 MSC: 14H40, 14C20, 14G05

1 Introduction

Let $\mathcal{C}$ be a smooth, projective, and geometrically integral curve defined over a number field $\mathbb{K}$. A fundamental problem in arithmetic geometry is the determination of the set $\mathcal{C}(\mathbb{K})$ of $\mathbb{K}$-rational points on $\mathcal{C}$, or equivalently, the description of the solutions over $\mathbb{K}$ to systems of polynomial equations in several variables. Despite substantial progress over the past centuries, no general method for resolving this problem is currently known.

Even when $\mathcal{C}$ is a curve, the problem of determining its rational points remains highly nontrivial. In particular, there is no general algorithm that determines $\mathcal{C}(\mathbb{K})$ for an arbitrary smooth projective curve over a number field. In this work, we restrict our attention to the case where $\mathbb{K} = \mathbb{Q}$ or a finite extension thereof.

Major advances in Diophantine geometry during the twentieth century have led to a qualitative understanding of the structure of $\mathcal{C}(\mathbb{Q})$ for curves of genus $g \geq 2$. A landmark result in this direction is Faltings' proof of the Mordell Conjecture [6], which establishes the

finiteness of $\mathcal{C}(\mathbb{Q})$ when $g \geq 2$. An alternative proof was later given by Vojta [10]. However, both approaches are ineffective in nature: for a given explicit curve, they do not provide a practical method for computing $\mathcal{C}(\mathbb{Q})$, but only yield upper bounds on $|\mathcal{C}(\mathbb{Q})|$, which are typically far from optimal and difficult to determine explicitly.

For a finite extension $\mathbb{K}/\mathbb{Q}$ of degree ℓ, the study of $\mathcal{C}(\mathbb{K})$ amounts to understanding the set of algebraic points of degree ℓ on $\mathcal{C}$, that is, points defined over number fields of degree ℓ. Recall that the degree of an algebraic point is defined as the degree of its field of definition over $\mathbb{Q}$.

In certain favorable situations, particularly when the Mordell–Weil rank of the Jacobian variety $\mathrm{Jac}(\mathcal{C})$ is zero, more explicit techniques can be employed to determine the rational points on $\mathcal{C}$. In such cases, the Abel–Jacobi map, together with descent methods and Chabauty-type techniques, plays a central role in the analysis.

A particularly interesting example arises from an infinite family of hyperelliptic curves of genus 2 defined over $\mathbb{Q}$ by the affine model

$$\Gamma : y^2 = xf(x)g(x), \tag{1}$$

where $f(x), g(x) \in \mathbb{Z}[x]$ are irreducible polynomials over $\mathbb{Q}$ of degree 2, and where the Jacobian of Γ has Mordell–Weil group over $\mathbb{Q}$ isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

This family therefore provides a rich source of explicit examples in which the finiteness of rational points can be studied effectively, and for which descent-theoretic methods may be applied to determine all rational solutions explicitly.

This paper is organized as follows. In Section 2, we collect the technical results that form the foundation of our main theorem. In Section 3, we prove our principal result concerning the structure of algebraic points of degree ℓ on curves in this family. We conclude with a final section in which we present explicit examples of curves to which our results apply, together with perspectives for future research.

Our main result, stated in Theorem 1.1, provides an explicit description of the algebraic points of degree $\ell \geq 5$ over $\mathbb{Q}$, denoted $\Gamma^{(\ell)}(\mathbb{Q})$, on the curves Γ. This description relies on rational parametrizations involving auxiliary polynomials and highlights key algebraic relations arising from the defining equation of the curve.

The following result provides an explicit description of all algebraic points on the curve Γ of degree at most ℓ. More precisely, it shows that these points can be partitioned into two families, each defined by rational parametrizations subject to certain symmetric algebraic relations.

Theorem 1.1. *Let $\ell \geq 5$ be an integer. Then the set of algebraic points of degree at most ℓ over $\mathbb{Q}$ on the curve Γ, whose Jacobian $\mathcal{J}(\mathbb{Q})$ has Mordell–Weil group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, is given by*

$$\Gamma^{(\ell)}(\mathbb{Q}) = \bigcup_{\sigma=0}^{1} \left(\mathcal{M}_\sigma \cup \mathcal{D}_\sigma\right),$$

where $\mathcal{M}_\sigma$ and $\mathcal{D}_\sigma$ are defined as follows:

$$\mathcal{M}_\sigma = \left\{ \left(x, -\sum_{\kappa=\sigma}^{\lfloor\frac{\ell+\sigma}{2}\rfloor} a_\kappa x^\kappa \Big/ \sum_{\epsilon=0}^{\lfloor\frac{\ell+\sigma-5}{2}\rfloor} b_\epsilon x^\epsilon \right) \;\middle|\; \begin{array}{l} a_{\lfloor\frac{\ell+\sigma}{2}\rfloor} \neq 0 \text{ if } \ell \text{ is even, } b_{\lfloor\frac{\ell+\sigma-5}{2}\rfloor} \neq 0 \\ \text{if } \ell \text{ is odd, and } x \text{ is a root of} \\ \left(\sum_{\kappa=\sigma}^{\lfloor\frac{\ell+\sigma}{2}\rfloor} a_\kappa x^{\kappa-\frac{\sigma}{2}} \right)^2 = x^{1-\sigma} \left(\sum_{\epsilon=0}^{\lfloor\frac{\ell+\sigma-5}{2}\rfloor} b_\epsilon x^\epsilon \right)^2 \prod_{\nu=1}^{2}(x+\xi_\nu) \prod_{\mu=3}^{4}(x+\lambda_\mu) \end{array} \right\},$$

$$\mathcal{D}_\sigma = \left\{ \left(x, -\sum_{\kappa=1}^{\lfloor\frac{\ell+2}{2}\rfloor} a_\kappa \left(x^\kappa + \psi_\sigma^\kappa\right) \Big/ \sum_{\epsilon=0}^{\lfloor\frac{\ell-3}{2}\rfloor} b_\epsilon x^\epsilon \right) \;\middle|\; \begin{array}{l} \psi_0^\kappa = -\frac{1}{2}(\xi_1^\kappa + \xi_2^\kappa),\ \psi_1^\kappa = -\frac{1}{2}(\lambda_3^\kappa + \lambda_4^\kappa), \\ a_{\lfloor\frac{\ell+2}{2}\rfloor} \neq 0 \text{ if } \ell \text{ is even, } b_{\lfloor\frac{\ell-3}{2}\rfloor} \neq 0 \text{ if } \ell \\ \text{is odd, and } x \text{ is a root of} \\ \left(\sum_{\kappa=1}^{\lfloor\frac{\ell+2}{2}\rfloor} a_\kappa \Big(\frac{x^\kappa + \psi_\sigma^\kappa}{x} \Big) \right)^2 = \left(\sum_{\epsilon=0}^{\lfloor\frac{\ell-3}{2}\rfloor} b_\epsilon x^{\epsilon-\frac{1}{2}} \right)^2 \prod_{\nu=1}^{2}(x+\xi_\nu) \prod_{\mu=3}^{4}(x+\lambda_\mu) \end{array} \right\}.$$

2 Auxiliary results

Let $\mathbb{K}$ be a number field and let $\mathcal{C}$ be a smooth projective curve defined over $\mathbb{K}$. For any divisor $\varpi \in \mathrm{Div}(\mathcal{C})$, the associated Riemann–Roch space is the $\mathbb{K}$-vector space defined by

$$\mathcal{L}(\varpi) := \{ f \in \mathbb{K}(\mathcal{C}) \setminus \{0\} \mid \mathrm{div}(f) \geq -\varpi \} \cup \{0\}.$$

Moreover, for any two divisors $\varpi, \varpi' \in \mathrm{Div}(\mathcal{C})$, if ϖ is linearly equivalent to ϖ' (denoted $\varpi \equiv \varpi'$), then their Riemann–Roch spaces are isomorphic:

$$\mathcal{L}(\varpi) \simeq \mathcal{L}(\varpi'), \quad \text{and in particular} \quad \dim \mathcal{L}(\varpi) = \dim \mathcal{L}(\varpi').$$

Definition 2.1. *Let Γ be a smooth projective curve of genus $g \geq 1$, and let $S \in \Gamma(\mathbb{K})$. The Abel–Jacobi map associated to S is the embedding*

$$j : \Gamma \hookrightarrow \mathcal{J}(\mathbb{K}), \quad P \longmapsto [P - S], \tag{2}$$

where $\mathcal{J}$ denotes the Jacobian variety of Γ.

Theorem 2.1 (Abel–Jacobi)**.** *[7] A divisor $\varpi \in \mathrm{Div}^0(\Gamma)$ is principal if and only if its image in the Jacobian is trivial. Equivalently, ϖ is the divisor of a rational function if and only if $[\varpi] = 0$ in $\mathcal{J}(\mathbb{K})$.*

The affine model (1) of the curve Γ can be written as

$$y^2 = x \prod_{\nu=1}^{2}(x-\xi_\nu) \prod_{\mu=3}^{4}(x-\lambda_\mu), \tag{3}$$

where ξ_ν and λ_μ are respectively the roots of the polynomials $f(x)$ and $g(x)$, satisfying $\xi_2 = \overline{\xi_1}$ and $\lambda_4 = \overline{\lambda_3}$.

By homogenizing (3) via $x = X/Z$ and $y = Y/Z$, we obtain the projective model of Γ:

$$Z^3Y^2 = X\prod_{\nu=1}^{2}(X - \xi_\nu Z)\prod_{\mu=3}^{4}(X - \lambda_\mu Z). \tag{4}$$

From (4), we define the affine points S_0, S_ν, S_μ and the point at infinity ∞ by

$$S_0 = (0,0), \quad S_\nu = (\xi_\nu, 0), \quad S_\mu = (\lambda_\mu, 0), \quad \infty = [0:1:0].$$

Lemma 2.1. *The rational divisors associated with the curve Γ are:*

(*i*) $\operatorname{div}(x - \sigma_k) = 2S_k - 2\infty$, *where* $\sigma_k \in \{0, \xi_\nu, \lambda_\mu\}$,

(*ii*) $\operatorname{div}(y) = \sum_{k=0}^{4} S_k - 5\infty$.

Proof. These results follow from intersection theory, using the formula

$$\operatorname{div}(\omega - \sigma) = (\Omega - \sigma Z = 0)\cdot\Gamma - (Z = 0)\cdot\Gamma,$$

where $\omega \in \{x, y\}$ are affine coordinates and $\Omega \in \{X, Y\}$ their projective lifts. A detailed proof can be found in [5, Lemma 4]. □

Corollary 2.1. *We have:*

- $\circledast$ $\displaystyle\sum_{k=0}^{4} j(S_k) = 0$,
- $\circledast$ $2j(S_k) = 0$ *for all* $k \in \{0, \nu, \mu\}$.

Hence, the images $j(S_k)$ generate the same subgroup of $\mathcal{J}(\mathbb{Q})$.

Remark 2.1. *The torsion subgroup of the Jacobian $\mathcal{J}(\mathbb{Q})_{\mathrm{tor}}$ is generated by*

$$\mathcal{J}(\mathbb{Q})_{\mathrm{tor}} \simeq \left\langle [S_0 - \infty],\ \left[\sum_{k=1}^{2} S_k - 2\infty\right]\right\rangle.$$

Since $\mathcal{J}(\mathbb{Q})$ is finite (as recalled in Section 1), it coincides with its torsion subgroup. Hence, we obtain the following consequence.

Lemma 2.2. *The Mordell–Weil group of the Jacobian is generated by the divisor classes*

$$[S_0 - \infty], \qquad \left[\sum_{k=1}^{2} S_k - 2\infty\right],$$

and every element of $\mathcal{J}(\mathbb{Q})$ can be written as a $\mathbb{Z}$-linear combination of these classes. In particular,

$$\mathcal{J}(\mathbb{Q}) = \left\{ \alpha\, j(S_0) + \beta \sum_{k=1}^{2} j(S_k) \;\middle|\; \alpha, \beta \in \{0,1\} \right\}. \tag{5}$$

Proof. Since $\mathcal{J}(\mathbb{Q})$ is finite, it coincides with its torsion subgroup:

$$\mathcal{J}(\mathbb{Q}) = \mathcal{J}(\mathbb{Q})_{\mathrm{tor}}.$$

The generators of the torsion subgroup are given in Remark 2.1, which implies that $\mathcal{J}(\mathbb{Q})$ is generated by the classes $[S_0 - \infty]$ and $\left[\sum_{k=1}^{2} S_k - 2\infty\right]$.

The explicit description (5) follows immediately from this generating set. □

Remark 2.2. *From Lemma 2.2, any element $t \in \mathcal{J}(\mathbb{Q})$ can be written as*

$$t = \left[(\alpha + 2\beta)\infty - \alpha S_0 - \beta \sum_{k=1}^{2} S_k \right],$$

for some $\alpha, \beta \in \{0,1\}$.

Lemma 2.3. *Let ℓ be a positive integer. A $\mathbb{Q}$-basis of the Riemann–Roch space $\mathcal{L}(\ell\infty)$ is*

$$\mathcal{B}_\ell = \left\{ x^\kappa \;:\; 0 \le \kappa \le \left\lfloor \tfrac{\ell}{2} \right\rfloor \right\} \cup \left\{ yx^\epsilon \;:\; 0 \le \epsilon \le \left\lfloor \tfrac{\ell-5}{2} \right\rfloor \right\}.$$

Proof. The result follows from Lemma 2.1, Clifford's theorem (see [2]) for $\ell \le 2g-2$, and the Riemann-Roch theorem (see [9]) for $\ell \ge 2g-2$. For full details, see [3, Lemma 3]. □

3 Proof of main results

Proof. Let $G \in \Gamma\left(\bar{\mathbb{Q}}\right)$ be a point of degree $\ell \ge 5$ over $\mathbb{Q}$, *i.e.*,

$$[\mathbb{Q}(G) : \mathbb{Q}] = \ell,$$

and assume that $G \notin \{S_k \mid 0 \le k \le 4\} \cup \{\infty\}$. Let $G_1, \ldots, G_\ell$ denote the Galois conjugates of G over $\mathbb{Q}$. Consider the point

$$\lambda = \left[\sum_{n=1}^{\ell} G_n - \ell\infty \right] \in \mathcal{J}_{p,i,j}(\mathbb{Q}).$$

From Remark 2.2, we have the equality

$$\left[\sum_{n=1}^{\ell} G_n - \ell\infty \right] = \left[(\alpha + 2\beta)\infty - \alpha S_0 - \beta \sum_{k=1}^{2} S_k \right], \tag{6}$$

for some $\alpha, \beta \in \{0,1\}$. Transposing the right-hand side of equation (6) to the left-hand side, we obtain:

$$\Big[\sum_{n=1}^{\ell} G_n + \alpha S_0 + \beta \sum_{k=1}^{2} S_k - (\ell + \alpha + 2\beta)\infty\Big] = 0. \tag{7}$$

From Theorem 2.1, equation (7) implies the existence of a rational function $f_{\alpha,\beta}(x,y) \in \mathbb{Q}(\Gamma)$ such that:

$$\operatorname{div}(f_{\alpha,\beta}) = \sum_{n=0}^{\ell} G_n + \alpha S_0 + \beta \sum_{k=1}^{2} S_k - (\ell + \alpha + 2\beta)\infty. \tag{8}$$

From expression (8), it follows that $f_{\alpha,\beta} \in \mathcal{L}\left((\ell + \alpha + 2\beta)\infty\right)$. Then, by Lemma 2.3, the function $f_{\alpha,\beta}(x,y)$ admits the following explicit form:

$$f_{\alpha,\beta}(x,y) = \sum_{\kappa=0}^{\lfloor \frac{\ell+\alpha+2\beta}{2} \rfloor} a_\kappa x^\kappa + \sum_{\epsilon=0}^{\lfloor \frac{\ell+\alpha+2\beta-5}{2} \rfloor} b_\epsilon y x^\epsilon \tag{9}$$

for some coefficients $a_\kappa, b_\epsilon \in \mathbb{Q}$.

Depending on the values of α and β, the pair (α, β) ranges over the set

$$\big\{(0,0),(1,0),(0,1),(1,1)\big\}.$$

- First, consider the case where the parameters (α, β) belong to the subset $\{(0,0),(1,0)\}$. In this case, equation (9) becomes:

$$f_{\alpha,\beta}(x,y) = \sum_{\kappa=0}^{\lfloor \frac{\ell+\alpha}{2} \rfloor} a_\kappa x^\kappa + \sum_{\epsilon=0}^{\lfloor \frac{\ell+\alpha-5}{2} \rfloor} b_\epsilon y x^\epsilon. \tag{10}$$

  – If $(\alpha, \beta) = (0,0)$, then the expression (10) of $f_{\alpha,\beta}(x,y)$ simplifies to:

$$f_{\alpha,\beta}(x,y) = \sum_{\kappa=0}^{\lfloor \frac{\ell}{2} \rfloor} a_\kappa x^\kappa + \sum_{\epsilon=0}^{\lfloor \frac{\ell-5}{2} \rfloor} b_\epsilon y x^\epsilon \tag{11}$$

  where the coefficients $a_\kappa, b_\varepsilon \in \mathbb{Q}$ are all nonzero (otherwise one of the points G_n would coincide with S_0, which is impossible). In particular, we require $a_{\lfloor \frac{\ell}{2} \rfloor} \neq 0$ and $b_{\lfloor \frac{\ell-5}{2} \rfloor} \neq 0$, depending on whether ℓ is even or odd (to ensure none of the G_n's equals ∞).

  – If $(\alpha, \beta) = (1,0)$, we have $\operatorname{ord}_{S_0} f_{\alpha,\beta} = 1$, which implies $a_0 = 0$. Thus, the expression (10) of $f_{\alpha,\beta}(x,y)$ becomes:

$$f_{\alpha,\beta}(x,y) = \sum_{\kappa=1}^{\lfloor \frac{\ell+1}{2} \rfloor} a_\kappa x^\kappa + \sum_{\epsilon=0}^{\lfloor \frac{\ell-4}{2} \rfloor} b_\epsilon y x^\epsilon \tag{12}$$

  with $b_0 \neq 0$ (otherwise one of the G_n's would coincide with S_0, which is again

impossible), and both $a_{\lfloor \frac{\ell+1}{2} \rfloor} \neq 0$ and $b_{\lfloor \frac{\ell-4}{2} \rfloor} \neq 0$, depending on whether ℓ is even or odd (to ensure none of the G_n's equals ∞).

Thus, for any pair of parameters (α, β), belonging to the set $\{(0,0),(1,0)\}$, we may encode the expressions (11) and (12), uniformly using the parameter σ with $\sigma \in \{0,1\}$ leading to the following general form:

$$f_\sigma(x,y) = \sum_{\kappa=\sigma}^{\lfloor \frac{\ell+\sigma}{2} \rfloor} a_\kappa x^\kappa + \sum_{\epsilon=0}^{\lfloor \frac{\ell+\sigma-5}{2} \rfloor} b_\epsilon y x^\epsilon. \tag{13}$$

At each point G_n vanishes, we have $f_\sigma(x,y) = 0$, which yields an explicit expression for y in terms of x:

$$y = -\sum_{\kappa=\sigma}^{\lfloor \frac{\ell+\sigma}{2} \rfloor} a_\kappa x^\kappa \Big/ \sum_{\epsilon=0}^{\lfloor \frac{\ell+\sigma-5}{2} \rfloor} b_\epsilon x^\epsilon. \tag{14}$$

Substituting this expression for y into the equation (14) into the expression (3) defining the hyperelliptic curve Γ, we obtain:

$$\Big(\sum_{\kappa=\sigma}^{\lfloor \frac{\ell+\sigma}{2} \rfloor} a_\kappa x^\kappa \Big)^2 = \Big(\sum_{\epsilon=0}^{\lfloor \frac{\ell+\sigma-5}{2} \rfloor} b_\epsilon x^\epsilon \Big)^2 x \prod_{\nu=1}^{2} (x+\xi_\nu) \prod_{\mu=3}^{4} (x+\lambda_\mu). \tag{15}$$

As equation (15) is not yet of degree ℓ, we reparametrize it to the equivalent equation:

$$\Big(\sum_{\kappa=\sigma}^{\lfloor \frac{\ell+\sigma}{2} \rfloor} a_\kappa x^{\kappa-\frac{\sigma}{2}} \Big)^2 = x^{1-\sigma} \Big(\sum_{\epsilon=0}^{\lfloor \frac{\ell+\sigma-5}{2} \rfloor} b_\epsilon x^\epsilon \Big)^2 \prod_{\nu=1}^{2} (x+\xi_\nu) \prod_{\mu=3}^{4} (x+\lambda_\mu). \tag{16}$$

Equation (16) is now of degree ℓ. Indeed, the left hand side has degree

$$2 \times \Big(\frac{\ell+\sigma}{2} + \frac{\sigma}{2} \Big) = \ell$$

and the right hand side also has degree

$$2 \times \Big(\frac{\ell+\sigma-5}{2} \Big) + 5 - \sigma = \ell.$$

Hence, equation (16) defines a degree ℓ algebraic equation whose roots correspond to x coordinates of degree ℓ points on Γ. This gives us the first family of points of degree ℓ, which we denoted by $\mathcal{M}_\sigma$ in Theorem 1.1.

- We now consider the case where the parameters (α, β) belong to the set $\{(0,1),(1,1)\}$.

In this case, the general expression (9) becomes:

$$f_{\alpha,\beta}(x,y) = \sum_{\kappa=0}^{\lfloor\frac{\ell+\alpha+2}{2}\rfloor} a_\kappa x^\kappa + \sum_{\epsilon=0}^{\lfloor\frac{\ell+\alpha-3}{2}\rfloor} b_\epsilon y x^\epsilon. \tag{17}$$

– If $(\alpha,\beta) = (0,1)$, the condition $\mathrm{ord}_{S_\nu} f_{\alpha,\beta} = 1$ for each $\nu \in \{0,1\}$, implies that:

$$a_0 = \sum_{\kappa=1}^{\lfloor\frac{\ell+2}{2}\rfloor} a_\kappa \psi_0^\kappa, \quad \text{where} \quad \psi_0^\kappa = -\frac{1}{2}(\xi_1^\kappa + \xi_2^\kappa).$$

Therefore, the function $f_{\alpha,\beta}(x,y)$ given in (17) takes the form:

$$f_{\alpha,\beta}(x,y) = \sum_{\kappa=1}^{\lfloor\frac{\ell+2}{2}\rfloor} a_\kappa \left(x^\kappa + \psi_0^\kappa\right) + \sum_{\epsilon=0}^{\lfloor\frac{\ell-3}{2}\rfloor} b_\epsilon y x^\epsilon \tag{18}$$

with $a_{\lfloor\frac{\ell+2}{2}\rfloor} \neq 0$ and $b_{\lfloor\frac{\ell-3}{2}\rfloor} \neq 0$, depending on whether ℓ is even or odd (otherwise, some of the points G_n would lie at ∞, which is not allowed).

– If $(\alpha,\beta) = (1,1)$, then by Corollary 2.1, the principal divisor associated with $f_{\alpha,\beta}$ as defined in (8) becomes:

$$\mathrm{div}(f_{\alpha,\beta}) = \sum_{n=0}^{\ell} G_n + \sum_{k=3}^{4} S_k - (\ell+2)\infty. \tag{19}$$

It follows from (19) that $f_{\alpha,\beta} \in \mathcal{L}\left((\ell+2)\infty\right)$. Then, by Lemma 2.3, we deduce that the function $f_{\alpha,\beta}(x,y)$ given in (17) admits the following explicit form:

$$f_{\alpha,\beta}(x,y) = \sum_{\kappa=0}^{\lfloor\frac{\ell+2}{2}\rfloor} a_\kappa \left(x^\kappa + \psi_1^\kappa\right) + \sum_{\epsilon=0}^{\lfloor\frac{\ell-3}{2}\rfloor} b_\epsilon y x^\epsilon \tag{20}$$

Since $\mathrm{ord}_{S_\mu} f_{\alpha,\beta} = 1$ for each $\mu \in \{0,1\}$, as seen in (19), this implies that:

$$a_0 = \sum_{\kappa=1}^{\lfloor\frac{\ell+2}{2}\rfloor} a_\kappa \psi_1^\kappa, \quad \text{where} \quad \psi_1^\kappa = -\frac{1}{2}(\lambda_3^\kappa + \lambda_4^\kappa).$$

Substituting this into (20), we obtain a simplified expression for $f_{\alpha,\beta}$:

$$f_{\alpha,\beta}(x,y) = \sum_{\kappa=1}^{\lfloor\frac{\ell+2}{2}\rfloor} a_\kappa \left(x^\kappa + \psi_1^\kappa\right) + \sum_{\epsilon=0}^{\lfloor\frac{\ell-3}{2}\rfloor} b_\epsilon y x^\epsilon \tag{21}$$

where $a_{\lfloor\frac{\ell+2}{2}\rfloor} \neq 0$ and $b_{\lfloor\frac{\ell-3}{2}\rfloor} \neq 0$ depending on whether ℓ is even or odd (otherwise, some G_n would lie at ∞, which is not permissible).

Thus, for any pair of parameters (α, β), belonging to the set $\{(0,1),(1,1)\}$, we may encode the expressions (19) and (21), uniformly using the parameter σ with $\sigma \in \{0,1\}$ leading to the following general form:

$$f_\sigma(x,y) = \sum_{\kappa=1}^{\lfloor \frac{\ell+2}{2} \rfloor} a_\kappa \left(x^\kappa + \psi_\sigma^\kappa\right) + \sum_{\epsilon=0}^{\lfloor \frac{\ell-3}{2} \rfloor} b_\epsilon y x^\epsilon$$

with

$$\psi_0^\kappa = -\frac{1}{2}(\xi_1^\kappa + \xi_2^\kappa) \qquad \text{and} \qquad \psi_1^\kappa = -\frac{1}{2}(\lambda_3^\kappa + \lambda_4^\kappa).$$

At each point G_n vanishes, we have $f_\sigma(x,y) = 0$, which yields an explicit expression for y in terms of x:

$$y = -\sum_{\kappa=1}^{\lfloor \frac{\ell+2}{2} \rfloor} a_\kappa \left(x^\kappa + \psi_\sigma^\kappa\right) \Big/ \sum_{\epsilon=0}^{\lfloor \frac{\ell-3}{2} \rfloor} b_\epsilon x^\epsilon. \tag{22}$$

Substituting this expression for y into the curve equation (3) defining Γ, we obtain:

$$\left(\sum_{\kappa=1}^{\lfloor \frac{\ell+2}{2} \rfloor} a_\kappa \left(x^\kappa + \psi_\sigma^\kappa\right)\right)^2 = \left(\sum_{\epsilon=0}^{\lfloor \frac{\ell-3}{2} \rfloor} b_\epsilon x^\epsilon\right)^2 x \prod_{\nu=1}^{2}(x+\xi_\nu) \prod_{\mu=3}^{4}(x+\lambda_\mu) \tag{23}$$

As equation (23) is not yet of degree ℓ, we reparametrize it to the equivalent equation:

$$\left(\sum_{\kappa=1}^{\lfloor \frac{\ell+2}{2} \rfloor} a_\kappa \Big(\frac{x^\kappa + \psi_\sigma^\kappa}{x}\Big)\right)^2 = \left(\sum_{\epsilon=0}^{\lfloor \frac{\ell-3}{2} \rfloor} b_\epsilon x^{\epsilon-\frac{1}{2}}\right)^2 \prod_{\nu=1}^{2}(x+\xi_\nu) \prod_{\mu=3}^{4}(x+\lambda_\mu) \tag{24}$$

Equation (24) is now of degree ℓ. Indeed, the left hand side has degree

$$2 \times \Big(\frac{\ell+2}{2} - 1\Big) = \ell,$$

and the right hand side also has degree

$$2 \times \Big(\frac{\ell-3}{2} - \frac{1}{2}\Big) + 4 = \ell.$$

Hence, equation (24) defines a degree ℓ algebraic equation whose roots correspond to x coordinates of degree ℓ points on Γ. This yields a second family $\mathcal{D}_\sigma$ of degree ℓ points. □

Conclusion

In this note, we have explicitly described sets of algebraic points of a given degree, applicable in particular to certain hyperelliptic curves, such as the one studied in [4], with affine equation $y^2 = x(x^2+x-4)(x^2-x+45)$. These results also extend to the study of algebraic

points of arbitrary degree on the family of curves $\mathcal{C}_{i,j,p}$ introduced in [8], defined by the affine equation $y^2 = x(x^2 + 2^i p^j)(x^2 + 2^{i+1} p^j)$ where $p \equiv 11, 16 \pmod{32}$. Several research directions emerge from this work. In particular, the explicit determination of algebraic points of fixed degree on such curves constitutes a natural and promising direction. Moreover, the study of embeddings of these curves over finite fields could open the way to new algorithmic approaches, especially in the context of cryptography based on algebraic curves.

Acknowledgment

I would like to express my sincere gratitude to the editor and the entire editorial team of *Matimyás Matematika* for accepting this article for publication, as well as to the reviewer for their thorough examination, which has significantly contributed to improving the quality of this manuscript.

References

[1] Bernard N., Leprévost F. and Pohst M., Jacobians of genus two curves with a rational point of order 11, *Experimental Mathematics*, **18**, no. 1, (2009), 65–70.

[2] Coppens M. and Martens G., Secant spaces and Clifford's theorem, *Compositio Mathematica*, **2**, no. 78, (1991), 193–212.

[3] Diallo M.M.D., Analytic Parametrization of the Algebraic Points of Given Degree on the Curve of Affine Equation $y^2 = 157(x^2 - 2)(x^2 + x)(x^2 + 1)$, *Transylvanian Journal of Mathematics & Mechanics*, **15**, (2023), 41–50.

[4] Diallo M.M.D., *Describing families of algebraic points of given degree on a hyperelliptic curve*, *Journal of Finsler Geometry and its Applications*, **6**, no. 1, (2025), 83–91.

[5] Diallo M.M.D., Explicit family of algebraic points of given degree of the curve family $\mathcal{C}_q$, *Journal of Advanced Mathematical Studies*, **17**, no. 4, (2024), 444–450.

[6] Faltings, G., *Finiteness theorems for abelian varieties over number fields*, Arithmetic geometry, (1986), 9–26.

[7] Griffiths, P. A., *Introduction to algebraic curves*, Translated from the Chinese by Kuniko Weltin. Translations of Mathematical Monographs, American Mathematical Society, **76**, (1989).

[8] Matsumura, H., *Infinitely many hyperelliptic curves with exactly two rational points: Part II*, arXiv, (2020).

[9] Mattuck A. and Mayer A., The Riemann-Roch theorem for algebraic curves, *Annali della Scuola Normale Superiore di Pisa-Scienze Fisiche e Matematiche*, **17**, no. 3, (1963), 223–237.

[10] Vojta P., *On algebraic points on curves*, Compositio Mathematica, **78** (1991), no. 1, 29–36.

This page is intentionally left blank.