DIVISION POLYNOMIALS IN MUMFORD COORDINATES

J BERNATSKA

Abstract. An effective method of computing division polynomials in terms of Mumford coordinates is presented. As an example, division polynomials for 3- and 4-torsion divisors on a genus two curve are obtained explicitly in terms of Mumford coordinates, and x-, y-coordinates of the support of torsion divisors. As a result, n-torsion divisors on a given curve can be computed directly from the division polynomials. Alternatively, these divisors are obtained by solving the Jacobi inversion problem at points of the Jacobian variety of order n.

1. Introduction

The research projects like Crypto-Math CREST [18], and the stream of publications in IACR Cryptology ePrint Archive show that the isogeny-based cryptography is considered as a part of the next-generation cryptography. And genus two curves have essential benefits in public-key cryptography, as proven, for example, in [6, 7]

Below, we focus on division polynomials, which arose in the elliptic case to define n-torsion points on the curve. Generalizations to higher genera are suggested in [14, 17, 20].

In [14], polynomials which define the reduced representation of divisors nD, $D = (x, y) - \infty$, are constructed, and called division polynomials. (By nD the sum $D + D + \cdots + D$ with n terms is denoted, and we adopt this notation.) On the contrary, computations show that n-torsion divisors on a hyperelliptic curve are non-special, except the case of 2-torsion divisors, and no divisors contain repeated points. Thus, divisors of the form $k \cdot (x, y)$ are not n-torsion for any n.

In [17], we find a division polynomial in the form $\phi_n(u) = \sigma(nu)/\sigma(u)^{n^2}$, $u \in \mathrm{Jac}(\mathcal{C})\backslash(\sigma)_0$, where $(\sigma)_0 = \{u \in \mathrm{Jac}(\mathcal{C}) \mid \sigma(u) = 0\}$ denotes the theta divisor. Polynomials ϕ_n are expressible in terms of fixed set of $\wp$-functions. A curve $\mathcal{C}$ of genus two is considered. The expression for ϕ_2 is adopted from [2, p. 100]. For $n \geqslant 3$ a recurrence relation is suggested, as well as a method of constructing ϕ_n. According to [17, Theorem 7], n-torion points on $\mathrm{Jac}(\mathcal{C})[n]\backslash((\sigma)_0 \cap \mathrm{Jac}(\mathcal{C})[n])$ are the common zeros of the equations of $\mathrm{Jac}(\mathcal{C})$, ϕ_n, $\partial_{u_1}\phi_n$, $\partial^2_{u_1}\phi_n$, where $\partial_u \equiv \partial/\partial u$.

In [20], Kanayama's division polynomials are generalized to the case of a general hyperelliptic Jacobian, though all examples do not exceed genus two, and only the case of $n = 2$ in genus two is considered in detail. A more general case is proven for special divisors composed from one point only, similar to the determinant formulas adopted from [19].

The method suggested in [17] and developed in [20] requires essential efforts, and the knowledge of identities for $\wp$-functions associated with the curve in question. Moreover, obtaining multiplication formulas of the form $\sigma(nu)/\sigma(u)^{n^2}$ is a

Date: February 28, 2025.

complicate problem itself. Below, a simpler method of obtaining division polynomials is suggested. Under division polynomials we will understand the polynomials which define n-torsion divisors on a curve $\mathcal{C}$. The method leads to purely algebraic computations, though it is based on the structure of the field of abelian $\wp$-functions associated with $\mathcal{C}$. As a result, x-, y-coordinates of the support of n-torsion divisors are obtained.

There is no problem to find n-torsion points on $\mathrm{Jac}(\mathcal{C})$ — these are points of order n. The problem arises when x-, y-coordinates of the Abel pre-images of such points are required. There exists a direct way to compute the non-special Abel pre-image from a given point of $\mathrm{Jac}(\mathcal{C})$, based on a solution of the Jacobi inversion problem. Such a solution is known in terms of $\wp$-functions, see [1, § 216] for hyperelliptic curves, and [4] for non-hyperelliptic curves. This way became feasible due to the progress in computing uniformization of plane algebraic curves, see [5]. In the computations presented below, we use this way for verification.

The proposed method of obtaining division polynomials is based on the addition and duplication laws, written in terms of the Mumford coordinates of n-torsion divisors. As will be shown, defining n-torsion divisors on a genus g curve requires not more than g polynomials. The number of polynomials decreases in the case of even n, say $n = 2k$, when kD is a special divisor. Note, that kD produced from an n-torsion divisor D is 2-torsion, if $n = 2k$.

For the sake of compact expressions, we work with a genus two curve $\mathcal{C}$. Addition on the Jacobian variety $\mathrm{Jac}(\mathcal{C})$ of such a curve is widely known, see [13, 16]. This approach arises from Cantor's algorithm, and uses Mumford's representation of divisors on a hyperelliptic curve $f(x, y) = 0$ by interpolation polynomials in x-coordinate.

Below, the addition law is adopted from [8]. It is based on the theory of polynomial functions on $\mathcal{C}$, which form a ring $\mathfrak{P}(\mathcal{C}) = \mathbb{C}[x, y]/f(x, y; \lambda)$. The structure of the ring is closely connected to the field of $\wp$-functions associated with $\mathcal{C}$. Polynomial functions are composed of monomials in x, y arranged by the Sato weight. The theory of polynomial functions on $\mathcal{C}$ contains an elegant technique which replaces the mentioned interpolation polynomials, and makes the addition law explicit, and easy to derive.

The paper is organized as follows. In Section 2 basic notions are recalled and notations are introduced. In Section 3 the ring $\mathfrak{P}(\mathcal{C})$ of polynomial functions on a hyperelliptic curve $\mathcal{C}$ is described in detail; these functions are used to define divisors, and implement addition and inversion on the curve. In Section 4 the addition and duplication laws are derived by means of polynomial functions from $\mathfrak{P}(\mathcal{C})$. The cases of special divisors are also addressed. Section 5 is devoted to n-torsion divisors, and derivation of division polynomials in the Mumford coordinates, and x-, y-coordinates.

The method is illustrated by obtaining the division polynomials for 3- and 4-torsion divisors. Computations of these division polynomials on a given curve, as well as the corresponding torsion divisors, are implemented in Wolfram Mathematica 12, see `https://community.wolfram.com/groups/-/m/t/3338527`.

The proposed method can be easily extended to a hyperelliptic curve of any genus, as well as to non-hyperelliptic curves.

2. Preliminaries

2.1. **Hyperelliptic curve of genus two.** Let a genus two curve $\mathcal{C}$ be defined by the equation

$$\begin{aligned} 0 = f(x,y;\lambda) &= -y^2 + \mathcal{P}(x) \\ &= -y^2 + x^5 + \lambda_2 x^4 + \lambda_4 x^3 + \lambda_6 x^2 + \lambda_8 x + \lambda_{10}, \end{aligned} \tag{1}$$

which we call the canonical form, unlike [15], but according to the theory of multivariable σ-functions [10].

The canonical form of a plane algebraic curve $\mathcal{C}$, also known as (n,s)-curve, $\gcd(n,s)=1$, see [11], is the Weierstass canonical form described in [1, §§60–63]. Every (n,s)-curve is equipped with a unique modular-invariant, entire σ-function, which has a representation as an analytic series in $u \in \mathrm{Jac}(\mathcal{C})$ and parameters λ of $\mathcal{C}$, see [10, Ch. 9]. The differential field of abelian functions generated from σ-function, which we call $\wp$-functions, gives rise to an algebraic model of $\mathrm{Jac}(\mathcal{C})$, see [10, Ch. 3], and the addition law on $\mathcal{C}$, see [8].

We work over the field $\mathbb{C}$ of complex numbers, $(x,y) \in \mathbb{C}^2$; and assume that the curve $\mathcal{C}$ defined by (1) is not degenerate, that is $\lambda \in \mathbb{C}^5 \setminus \mathrm{Dscr}$, where Dscr consists of such λ that the genus of $\mathcal{C}$ reduces to 1 or 0. In more detail strata of the space of parameters λ are described in [3].

The theory of σ- and $\wp$-functions associated with (n,s)-curves respects the Sato weight, which shows the order of zero at infinity[1]. Due to the leading terms $-y^2 + x^5$ with co-prime exponents, the curve (1) admits the following expansion about infinity in a local parameter ξ:

$$\begin{aligned} x = \xi^{-2}, \quad y = \xi^{-5}\big(1 &+ \tfrac{1}{2}\lambda_2\xi^2 + \tfrac{1}{2}(\lambda_4 - \tfrac{1}{4}\lambda_2^2)\xi^4 + \tfrac{1}{2}(\lambda_6 - \tfrac{1}{2}\lambda_2\lambda_4 + \tfrac{1}{8}\lambda_2^3)\xi^6 \\ &+ \tfrac{1}{2}(\lambda_8 - \tfrac{1}{2}\lambda_2\lambda_6 - \tfrac{1}{2}\lambda_4^2 + \tfrac{3}{8}\lambda_2^2\lambda_4 - \tfrac{5}{64}\lambda_2^4)\xi^8 \\ &+ \tfrac{1}{2}(\lambda_{10} - \tfrac{1}{2}\lambda_2\lambda_8 - \tfrac{1}{2}\lambda_4\lambda_6 + \tfrac{3}{8}\lambda_2^2\lambda_6 + \tfrac{3}{8}\lambda_2\lambda_4^2 \\ &- \tfrac{5}{16}\lambda_2^3\lambda_4 + \tfrac{7}{128}\lambda_2^5)\xi^{10} + O(\xi^{12})\big). \end{aligned} \tag{2}$$

The negative exponents of leading terms show the Sato weights: $\mathrm{wgt}\, x = 2$, $\mathrm{wgt}\, y = 5$. The weight introduces an order in the list of monomials in x and y:

$$\begin{array}{lccccccccc} \text{weights:} & 0 & 2 & 4 & 5 & 6 & 7 & 8 & 9 & \\ \mathfrak{M} = \{ & 1, & x, & x^2, & y, & x^3, & yx, & x^4 & yx^2, & \dots \} \end{array} \tag{3}$$

The absent weights $\{1,\, 3\}$ form the Weierstras gap sequence of $\mathcal{C}$.

Let holomorphic (or first kind) differentials $\mathrm{d}u = (\mathrm{d}u_1, \mathrm{d}u_3)^t$ be given in the standard not normalized form:

$$\mathrm{d}u_1 = \frac{x\mathrm{d}x}{-2y}, \qquad \mathrm{d}u_3 = \frac{\mathrm{d}x}{-2y}. \tag{4}$$

Note, that $\mathrm{wgt}\, \mathrm{d}u_{\mathfrak{w}} = -\mathfrak{w}$, and the weights coincide with the negative Weierstrasss gap sequence. The Abel map is defined with respect to these differentials, with the basepoint located at infinity, namely

$$\mathcal{A}(P) = \int_\infty^P \mathrm{d}u, \qquad P = (x,y) \in \mathcal{C};$$

[1]The infinity point on an (n,s)-curve is a Weierstrass point, and a branch point where all n sheets wind.

$$\mathcal{A}(D)=\sum_{k=1}^{n}\mathcal{A}(P_k),\qquad D=\sum_{k=1}^{n}P_k\in\mathcal{C}^n.$$

Let $\mathfrak{a}_1$, $\mathfrak{b}_1$, $\mathfrak{a}_2$, $\mathfrak{b}_2$ form a canonical homology basis. Not normalized first kind period matrices are defined by

$$\omega=(\omega_{i,j})=\Big(\int_{\mathfrak{a}_j}\mathrm{d}u_i\Big),\qquad\qquad \omega'=(\omega'_{i,j})=\Big(\int_{\mathfrak{b}_j}\mathrm{d}u_i\Big),\tag{5}$$

and generate the period lattice $\{\omega,\omega'\}$, which introduces a polarization on the Jacobian variety $\mathrm{Jac}(\mathcal{C})=\mathbb{C}^2/\{\omega,\omega'\}$. Similarly to (5), second kind period matrices are defined:

$$\eta=(\eta_{ij})=\Big(\int_{\mathfrak{a}_j}\mathrm{d}r_i\Big),\qquad\qquad \eta'=(\eta'_{ij})=\Big(\int_{\mathfrak{b}_j}\mathrm{d}r_i\Big),\tag{6}$$

from second kind differentials $\mathrm{d}r=(\mathrm{d}r_1,\mathrm{d}r_3)^t$ associated with the first kind differentials $\mathrm{d}u$, see [1, Art. 138]. Namely,

$$\mathrm{d}r_1=\frac{x^2\mathrm{d}x}{-2y},\qquad\qquad \mathrm{d}r_3=\big(3x^3+2\lambda_2x^2+\lambda_4x\big)\frac{x\mathrm{d}x}{-2y}.$$

Let $D_2=(x_1,y_1)+(x_2,y_2)$ be a non-special divisor on $\mathcal{C}$. The Abel image $\mathcal{A}(D_2)\equiv u=(u_1,u_3)^t$ is computed by

$$u=\int_{\infty}^{(x_1,y_1)}\mathrm{d}u+\int_{\infty}^{(x_2,y_2)}\mathrm{d}u.\tag{7}$$

The not normalized coordinates $u=(u_1,u_3)^t$ serve as an argument of σ-, and $\wp$-functions. Normalization, which is employed by θ-function, is reached as follows

$$v=\omega^{-1}u,\qquad\qquad \tau=\omega^{-1}\omega',\tag{8}$$

where v is a vector of normalized coordinates of $\mathrm{Jac}(\mathcal{C})$, and τ belongs to the Siegel space of order 2.

2.2. **Entire functions.** Let the Riemann θ-function on $\mathbb{C}^2\supset\mathrm{Jac}(\mathcal{C})$ be defined by

$$\theta(v;\tau)=\sum_{n\in\mathbb{Z}^2}\exp\big(\imath\pi n^t\tau n+2\imath\pi n^tv\big).\tag{9}$$

Let a θ-function with characteristic $[\varepsilon]=(\varepsilon',\varepsilon)^t$ be defined by

$$\theta[\varepsilon](v;\tau)=\exp\big(\imath\pi(\varepsilon'^t\tau\varepsilon'+2\imath\pi(v+\varepsilon)^t(\varepsilon')\big)\theta(v+\varepsilon+\tau\varepsilon';\tau),\tag{10}$$

where $[\varepsilon]$ is a $2\times g$ matrix composed of two 2-component vectors ε' and ε with real entries within the interval $[0,1)$.

According to [9, Eq.(2.3)], σ-function is related to θ-function as follows

$$\sigma(u)=C\exp\big(-\tfrac{1}{2}u^t\varkappa u\big)\theta[K](\omega^{-1}u;\omega^{-1}\omega'),\tag{11}$$

where $[K]$ denotes the characteristic of the vector K of Riemann constants, a symmetric matrix $\varkappa=\eta\omega^{-1}$ is obtained from the second kind period matrix η defined by (6), and the constant C does not depend of u.

The origin $u=0$ of $\mathrm{Jac}(\mathcal{C})$ is the Abel image of infinity on $\mathcal{C}$, which also serves as the neutral point. Every point u in the fundamental domain of $\mathrm{Jac}(\mathcal{C})$ is represented by its characteristic $[\varepsilon]$, namely

$$u[\varepsilon]=\omega\varepsilon+\omega'\varepsilon'.\tag{12}$$

2.3. **Uniformization of the curve.** Every class of equivalent divisors on $\mathcal{C}$ has a representative $P_1 + P_2 - 2\infty$, and P_1, P_2 are not in involution, that is $P_2 \neq -P_1$. Such a representative is called a *reduced divisor*. Since the poles are located at infinity, which serves as the basepoint, it is convenient to define every reduced divisor by its positive part, as follows

- non-special $D_2 = (x_1, y_1) + (x_2, y_2)$ of degree 2,
- special $D_1 = (x_1, y_1) + \infty$ of degree 1
- neutral $O = 2\infty$ of degree 0, $u(2\infty) = 0$.

Let $\mathfrak{C}_2$ be a collection of all degree 2 non-special divisors. As mentioned in Introduction, we denote by $(\sigma)_0 = \{u \in \mathrm{Jac}(\mathcal{C}) \mid \sigma(u) = 0\}$ the theta divisor. Then $\mathcal{A}(\mathfrak{C}_2) = \mathrm{Jac}(\mathcal{C})\backslash(\sigma)_0$.

Uniformization of $\mathcal{C}$ is given in terms of $\wp$-functions, known as multiply periodic after [2], and Kleinian after [9]. Actually,

$$\wp_{i,j}(u) = -\frac{\partial^2 \log \sigma(u)}{\partial u_i \partial u_j}, \qquad \wp_{i,j,k}(u) = -\frac{\partial^3 \log \sigma(u)}{\partial u_i \partial u_j \partial u_k}, \qquad \text{etc.}$$

Meromorphic functions $\wp_{i,j}$, $\wp_{i,j,k}$, and all higher derivatives are $\{\omega, \omega'\}$-periodic.

Proposition 1 (**The Jacobi inversion problem**). [1, § 216] *Given $u \in \mathrm{Jac}(\mathcal{C})\backslash(\sigma)_0$, the Abel pre-image of u is a non-special divisor $D_2 = (x_1, y_1) + (x_2, y_2)$ with coordinates uniquely defined by the system*

$$\mathcal{R}_4(x; u) = 0, \qquad \mathcal{R}_5(x, y; u) = 0, \tag{13}$$

where $u = \mathcal{A}(D_2)$,

$$\begin{aligned} &\mathcal{R}_4(x; u) \equiv x^2 - x\wp_{1,1}(u) - \wp_{1,3}(u), \\ &\mathcal{R}_5(x, y; u) \equiv y + \tfrac{1}{2}x\wp_{1,1,1}(u) + \tfrac{1}{2}\wp_{1,1,3}(u). \end{aligned} \tag{14}$$

In other words, D_2 is a common divisor of zeros of the two polynomial functions $\mathcal{R}_4$, $\mathcal{R}_5$ on the curve $\mathcal{C}$.

Proposition 2. *$\mathcal{R}_4$, $\mathcal{R}_5$ defined by* (14) *on the common divisor of zeros are connected by the relation*

$$\mathcal{R}_5(x_i, y_i; u) = -\partial_{u_1}\mathcal{R}_4(x_i; u), \quad i = 1, 2. \tag{15}$$

Proof. If $D_2 = (x_1, y_1) + (x_2, y_2)$ is a common divisor of zeros of $\mathcal{R}_4$, $\mathcal{R}_5$, then $\mathcal{R}_4(x_i; u) = 0$, $i = 1, 2$. Differentiating with respect to u_1, and taking into account that the Jacobian matrix of $\mathcal{A}^{-1} : \mathfrak{C}_2 \to \mathrm{Jac}(\mathcal{C})\backslash(\sigma)_0$ has the entries

$$\frac{\partial x_1}{\partial u_1} = \frac{-2y_1}{x_1 - x_2}, \quad \frac{\partial x_2}{\partial u_1} = \frac{2y_2}{x_1 - x_2}, \quad \frac{\partial x_1}{\partial u_3} = \frac{2x_2 y_1}{x_1 - x_2}, \quad \frac{\partial x_2}{\partial u_3} = \frac{-2x_1 y_2}{x_1 - x_2}, \tag{16}$$

we immediately obtain (15). □

Remark 1. In general, $\mathcal{R}_4$, $\mathcal{R}_5$ from Proposition 1 have the form

$$\mathcal{R}_4(x) = x^2 + \alpha_2 x + \alpha_4, \qquad \mathcal{R}_5(x, y) = y + \beta_3 x + \beta_5. \tag{17}$$

Let $D_2 = (x_1, y_1) + (x_2, y_2)$ be the common divisor of zeros of $\mathcal{R}_4$ and $\mathcal{R}_5$, then

$$\alpha_2 = -(x_1 + x_2) = -\wp_{1,1}(u), \qquad \alpha_4 = x_1 x_2 = -\wp_{1,3}(u), \tag{18a}$$

$$\beta_3 = -\frac{y_1 - y_2}{x_1 - x_2} = \tfrac{1}{2}\wp_{1,1,1}(u), \qquad \beta_5 = \frac{x_2 y_1 - x_1 y_2}{x_1 - x_2} = \tfrac{1}{2}\wp_{1,1,3}(u). \tag{18b}$$

Actually, α_2, α_4, $-\beta_3$, $-\beta_5$ are known as the Mumford coordinates, and the pair of polynomials in x: $\mathcal{R}_4(x)$, $y-\mathcal{R}_5(x,y)$, are the first two from the triple of Mumford's representation of D_2. In what follows, we call α_2, α_4, β_3, β_5 the *Mumford coordinates*, for simplicify. Instead of Mumford's representation, we use polynomial functions $\mathcal{R}_4$, $\mathcal{R}_5$, which are sufficient to define any divisor from $\mathfrak{C}_2$ uniquely.

From [9, Theorem 3.2] we have the fundamental cubic relations on $\mathcal{C}$. After eliminating $\wp_{3,3}(u)$ an algebraic model of $\mathrm{Jac}(\mathcal{C})\backslash(\sigma)_0$ is obtained.

Proposition 3. *Given $u\in\mathrm{Jac}(\mathcal{C})\backslash(\sigma)_0$, the following identities define* $\mathrm{Jac}(\mathcal{C})\backslash(\sigma)_0$*:*

$$\begin{aligned}
&\tfrac{1}{2}\wp_{1,1,1}(u)\wp_{1,1,3}(u)+\tfrac{1}{4}\wp_{1,1}(u)\wp_{1,1,1}^2(u)=2\wp_{1,1}^2(u)\wp_{1,3}(u)\\
&\qquad+\wp_{1,3}^2(u)+2\lambda_2\wp_{1,1}(u)\wp_{1,3}(u)+\lambda_4\wp_{1,3}(u)+\lambda_8\\
&\qquad+\wp_{1,1}(u)\big(\wp_{1,1}(u)^3+\wp_{1,1}(u)\wp_{1,3}(u)+\lambda_2\wp_{1,1}(u)^2+\lambda_4\wp_{1,1}(u)+\lambda_6\big),\\
&\tfrac{1}{4}\wp_{1,1,3}(u)^2+\tfrac{1}{4}\wp_{1,3}(u)\wp_{1,1,1}^2(u)=\wp_{1,1}(u)\wp_{1,3}(u)^2+\lambda_2\wp_{1,3}(u)^2+\lambda_{10}\\
&\qquad+\wp_{1,3}(u)\big(\wp_{1,1}(u)^3+\wp_{1,1}(u)\wp_{1,3}(u)+\lambda_2\wp_{1,1}(u)^2+\lambda_4\wp_{1,1}(u)+\lambda_6\big).
\end{aligned}\tag{19}$$

This model is used in [20, Theorem 2.8]. The four functions $\wp_{1,1}$, $\wp_{1,3}$, $\wp_{1,1,1}$, $\wp_{1,1,3}$, which arise from (14), serve as coordinates on $\mathrm{Jac}(\mathcal{C})\backslash(\sigma)_0$. The differential field of meromorphic functions on $\mathrm{Jac}(\mathcal{C})\backslash(\sigma)_0$ is $\mathbb{C}[\wp_{1,1},\,\wp_{1,3},\,\wp_{1,1,1},\,\wp_{1,1,3}]$, that is, consists of polynomial expressions in these four functions, see [12]. For example,

$$\wp_{1,3,3}(u)=\wp_{1,3}(u)\wp_{1,1,1}(u)-\wp_{1,1}(u)\wp_{1,1,3}(u),\tag{20a}$$

$$\wp_{1,1,1,1}(u)=6\wp_{1,1}(u)^2+4\wp_{1,3}(u)+4\lambda_2\wp_{1,1}(u)+2\lambda_4,\tag{20b}$$

$$\wp_{1,1,1,3}(u)=6\wp_{1,3}(u)\wp_{1,1}(u)-2\wp_{3,3}(u)+4\lambda_2\wp_{1,3}(u),\tag{20c}$$

$$\begin{aligned}
\wp_{3,3}(u)=\tfrac{1}{4}\wp_{1,1,1}(u)^2-\wp_{1,1}(u)^3-\wp_{1,3}(u)\wp_{1,1}(u)\\
-\lambda_2\wp_{1,1}(u)^2-\lambda_4\wp_{1,1}(u)-\lambda_6.
\end{aligned}\tag{20d}$$

According to Proposition 1, the map

$$u\mapsto\big(\wp_{1,1}(u),\,\wp_{1,3}(u),\,\wp_{1,1,1}(u),\,\wp_{1,1,3}(u)\big)=\big(-\alpha_2,\,-\alpha_4,\,2\beta_3,\,2\beta_5\big)$$

takes $u\in\mathrm{Jac}(\mathcal{C})\backslash(\sigma)_0$ to $\mathfrak{C}_2$. In terms of the Mumford coordinates, (19) acquire the form

$$\begin{aligned}
&J_8(\alpha_2,\alpha_4,\beta_3,\beta_5;\lambda)\equiv 2\beta_3\beta_5-\alpha_2^2\alpha_4-\alpha_4^2+\lambda_4\alpha_4-\lambda_8\\
&\qquad-\alpha_2\big(\beta_3^2+\alpha_2^3-4\alpha_2\alpha_4+\lambda_2(2\alpha_4-\alpha_2^2)+\lambda_4\alpha_2-\lambda_6\big)=0,\\
&J_{10}(\alpha_2,\alpha_4,\beta_3,\beta_5;\lambda)\equiv\beta_5^2-2\alpha_2\alpha_4^2+\lambda_2\alpha_4^2-\lambda_{10}\\
&\qquad-\alpha_4\big(\beta_3^2+\alpha_2^3-4\alpha_2\alpha_4+\lambda_2(2\alpha_4-\alpha_2^2)+\lambda_4\alpha_2-\lambda_6\big)=0.
\end{aligned}\tag{21}$$

3. Polynomial functions on a curve

Since the base point is fixed at infinity, divisors are described by means of polynomial functions on $\mathcal{C}$, which form a ring $\mathfrak{P}(\mathcal{C})=\mathbb{C}[x,y]/f(x,y;\lambda)$. Recall, that each divisor is represented by its positive part.

Let $\mathcal{R}_{\mathfrak{w}}$ be a polynomial function of weight $\mathfrak{w}$ from $\mathfrak{P}(\mathcal{C})$. The divisor of zeros $(\mathcal{R}_{\mathfrak{w}})_0$ is of degree $\mathfrak{w}$, and defined by the system

$$\mathcal{R}_{\mathfrak{w}}(x,y)=0,\qquad\qquad f(x,y;\lambda)=0.\tag{22}$$

Polynomial functions are constructed from monomials $x^i y^j$, arranged ascendingly by the Sato weight into an ordered list $\mathfrak{M}$, see for example (3) in the case of a genus two curve.

Proposition 4. *A polynomial function $\mathcal{R}_{\mathfrak{w}}$ of weight $\mathfrak{w}$ is constructed from monomials $\{\mathfrak{m}_{\widetilde{\mathfrak{w}}} \in \mathfrak{M} \mid \widetilde{\mathfrak{w}} \leqslant \mathfrak{w}\}$, namely*

$$\mathcal{R}_{\mathfrak{w}}(x,y) = \sum_{\widetilde{\mathfrak{w}} \leqslant \mathfrak{w}} c_{\widetilde{\mathfrak{w}}} \mathfrak{m}_{\widetilde{\mathfrak{w}}}.$$

Proposition 5. *A polynomial function $\mathcal{R}_{\mathfrak{w}}$ of weight $\mathfrak{w} \geqslant 2g$ on a genus g curve $\mathcal{C}$ is uniquely defined by a positive divisor $D_{\mathfrak{w}-g}$ of degree $\mathfrak{w}-g$ such that $D_{\mathfrak{w}-g} \subset (\mathcal{R}_{\mathfrak{w}})_0$, and $D_{\mathfrak{w}-g}$ contains no groups of points in involution (repeated points are allowed). The function $\mathcal{R}_{\mathfrak{w}}$ is constructed as a linear combination of the first $\mathfrak{w}-g+1$ monomials from the ordered list $\mathfrak{M}$.*

Proof. If $\mathfrak{w} \geqslant 2g$, there exist $\mathfrak{w}-g+1$ such monomials, since g weights between 0 and $2g-1$ belong to the Weierstrass gap sequence. A monic polynomial composed as a linear combination of monomials of weights up to $\mathfrak{w}$ has $\mathfrak{w}-g$ degrees of freedom. Thus, a positive divisor $D_{\mathfrak{w}-g} = \sum_{k=1}^{\mathfrak{w}-g}(x_k, y_k)$ with no groups of points in involution defines $\mathcal{R}_{\mathfrak{w}}$ uniquely. Indeed, $\mathcal{R}_{\mathfrak{w}}$ is constructed from $D_{\mathfrak{w}-g}$ with all distinct points as follows

$$\mathcal{R}_{\mathfrak{w}}(x,y) = \frac{\begin{vmatrix} \mathfrak{m}_{\mathfrak{w}}(x,y) & \mathfrak{m}_{\mathfrak{w}-1}(x,y) & \dots & \mathfrak{m}_0(x,y) \\ \mathfrak{m}_{\mathfrak{w}}(x_1,y_1) & \mathfrak{m}_{\mathfrak{w}-1}(x_1,y_1) & \dots & \mathfrak{m}_0(x_1,y_1) \\ \vdots & \ddots & \vdots & \\ \mathfrak{m}_{\mathfrak{w}}(x_{\mathfrak{w}-g},y_{\mathfrak{w}-g}) & \mathfrak{m}_{\mathfrak{w}-1}(x_{\mathfrak{w}-g},y_{\mathfrak{w}-g}) & \dots & \mathfrak{m}_0(x_{\mathfrak{w}-g},y_{\mathfrak{w}-g}) \end{vmatrix}}{\begin{vmatrix} \mathfrak{m}_{\mathfrak{w}-1}(x_1,y_1) & \dots & \mathfrak{m}_0(x_1,y_1) \\ \vdots & \ddots & \vdots \\ \mathfrak{m}_{\mathfrak{w}-1}(x_{\mathfrak{w}-g},y_{\mathfrak{w}-g}) & \dots & \mathfrak{m}_0(x_{\mathfrak{w}-g},y_{\mathfrak{w}-g}) \end{vmatrix}}. \tag{23a}$$

If some points coincide, say $P_i = P_1$, $i = 2, \dots n$, then row $i+1$ in the numerator and row i in the denominator of (23a) are replaced with

$$\Big(\frac{\mathrm{d}^{i-1}}{\mathrm{d}x^{i-1}} \mathfrak{m}_{\widetilde{\mathfrak{w}}}(x, y(x))\Big|_{\substack{x=x_1 \\ y(x_1)=y_1}}\Big). \tag{23b}$$

Therefore, the determinant formula (23) produces a monic function, which represents $\mathcal{R}_{\mathfrak{w}}$ with $D_{\mathfrak{w}-g} \subset (\mathcal{R}_{\mathfrak{w}})_0$ uniquely. □

Corollary 1. *On a genus g hyperelliptic curve, $\mathcal{R}_{\mathfrak{w}}$ of weights $\mathfrak{w} \leqslant 2g$ are polynomials in x only, and have even weights $\mathfrak{w} = 2\mathfrak{k}$, $\mathfrak{k} \leqslant g$. Moreover, $\mathcal{R}_{2\mathfrak{k}}$ is uniquely defined by a set of distinct $\{x_i \mid i = 1, \dots \mathfrak{k}\}$, namely*

$$\mathcal{R}_{2\mathfrak{k}}(x) = \prod_{i=1}^{\mathfrak{k}} (x - x_i),$$

and $(\mathcal{R}_{\mathfrak{w}})_0$ consists of pairs of points connected by involution:

$$(\mathcal{R}_{2\mathfrak{k}})_0 = \textstyle\sum_{i=1}^{\mathfrak{k}} \big((x_i, y(x_i)) + (x_i, -y(x_i))\big).$$

Proof. The Weierstrass gap sequence on a hyperelliptic curve of genus g has the form $\mathfrak{W} = \{2i-1 \mid i = 1, \dots g\}$, and monomials of weights $\mathfrak{w} \leqslant 2g$ have the form x^k, $0 \leqslant k \leqslant g$. Thus, there exist no polynomial functions of odd weights $\mathfrak{w} = 2i-1$, $i = 1, \dots, g$, and all functions of weights $\mathfrak{w} \leqslant 2g$ are polynomials in x only. □

Corollary 2. *Let $\mathcal{R}_{\mathfrak{w}}$ be a polynomial function of weight $\mathfrak{w} > 2g$ on a hyperelliptic curve of genus g, and $D_{\mathfrak{w}-g} \subset (\mathcal{R}_{\mathfrak{w}})_0$ with $\deg D_{\mathfrak{w}-g} = \mathfrak{w} - g$. Then*

- *$\mathcal{R}_{\mathfrak{w}}$ is indecomposable, if $D_{\mathfrak{w}-g}$ contains no pairs of points connected by involution,*
- *$\mathcal{R}_{\mathfrak{w}}$ has a factor $(x - x_i)$, if $D_{\mathfrak{w}-g}$ contains a pair of points connected by involution: (x_i, y_i), $(x_i, -y_i)$.*

Proof. Suppose, $D_{\mathfrak{w}-g}$ contains a pair of points connected by involution, say $P_1 = (x_1, y_1)$, $P_2 = (x_1, -y_1)$. We use the formula (23) to construct $\mathcal{R}_{\mathfrak{w}}$. In the numerator we do the following operations with rows 2 and 3:

$$(\mathfrak{m}_{\widetilde{\mathfrak{w}}}(x_1, y_1)) \mapsto (\mathfrak{m}_{\widetilde{\mathfrak{w}}}(x_1, y_1) + \mathfrak{m}_{\widetilde{\mathfrak{w}}}(x_1, -y_1)),$$
$$(\mathfrak{m}_{\widetilde{\mathfrak{w}}}(x_1, -y_1)) \mapsto (\mathfrak{m}_{\widetilde{\mathfrak{w}}}(x_1, -y_1) - \mathfrak{m}_{\widetilde{\mathfrak{w}}}(x_1, y_1))$$

Then the first three rows acquire the form

$$\begin{vmatrix} 1 & x & \dots & x^g & y & x^{g+1} & yx & \dots & x^{k+g+1} & yx^k & \dots \\ 2 & 2x_1 & \dots & 2x_1^g & 0 & 2x_1^{g+1} & 0 & \dots & 2x_1^{k+g+1} & 0 & \dots \\ 0 & 0 & \dots & 0 & -2y_1 & 0 & -2y_1x_1 & \dots & 0 & -2y_1x_1^k & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{vmatrix} \sim$$

$$-4y_1 \begin{vmatrix} 1 & x & \dots & x^g & y & x^{g+1} & yx & \dots & x^{k+g+1} & yx^k & \dots \\ 1 & x_1 & \dots & x_1^g & 0 & x_1^{g+1} & 0 & \dots & x_1^{k+g+1} & 0 & \dots \\ 0 & 0 & \dots & 0 & 1 & 0 & x_1 & \dots & 0 & x_1^k & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{vmatrix}.$$

Subtracting row 2, and row 3 multiplied by y from row 1, we extract the common multiple $(x - x_1)$, which represents the pair of points in involution. □

Inversion and addition of divisors are conveniently implemented by means of polynomial functions from $\mathfrak{P}(\mathcal{C})$, see [8].

Theorem 1. *The inversion of a non-special divisor D_g of degree g on a curve of genus g is defined by the polynomial function $\mathcal{R}_{2g}$ of weight $2g$ with $D_g \subset (\mathcal{R}_{2g})_0$.*

Proof. Let a degree g divisor D_g^* be the complement of D_g in $(\mathcal{R}_{2g})_0$, that is $(\mathcal{R}_{2g})_0 = D_g + D_g^*$. Since $(\mathcal{R}_{2g})_0 \sim 2g\infty = O$, D_g^* serves as the inverse of D_g, that is $D_g^* = -D_g$. □

Theorem 2. *The inversion of a special divisor $D_{\mathfrak{k}}$ of degree $\mathfrak{k} < g$ on a hyperelliptic curve of genus g is defined by the polynomial function $\mathcal{R}_{2\mathfrak{k}}$ of weight $2\mathfrak{k}$ with $D_{\mathfrak{k}} \subset (\mathcal{R}_{2\mathfrak{k}})_0$.*

Proof. Let $D_{\mathfrak{k}} = \sum_{k=1}^{\mathfrak{k}} (x_k, y_k)$. From this divisor a polynomial function is constructed as a linear combination of the first $\mathfrak{k}$ monomials from the ordered list $\mathfrak{M}$. Such monomials are $1, x, \dots, x^{\mathfrak{k}-1}$, if the curve is hyperelliptic. Thus, we obtain a funciton $\mathcal{R}_{2\mathfrak{k}}$ of weight $2\mathfrak{k}$, which is a polynomial in x only; and the complement of $D_{\mathfrak{k}}$ is $-D_{\mathfrak{k}}$, as follows from Corollary 1. □

Theorem 3. *The addition of two degree g non-special divisors D_g, $\tilde{D}_g$ on a curve of genus g is defined by the polynomial function $\mathcal{R}_{3g}$ of weight $3g$ with $D_g + \tilde{D}_g \subset (\mathcal{R}_{3g})_0$.*

Proof. The required function $\mathcal{R}_{3g}$ is constructed from D_g and $\tilde{D}_g$, according to Proposition 5. Then the complement divisor D_g^* such that $D_g + \tilde{D}_g + D_g^* = (\mathcal{R}_{3g})_0$ is the inverse of $D_g + \tilde{D}_g$, and so $-D_g^*$ is the reduced divisor equivalent to the sum $D_g + \tilde{D}_g$. □

Theorem 4. *The addition of two divisors D_m, D_n of degrees m and n on a hyperelliptic curve of genus g is defined by the polynomial function $\mathcal{R}_{m+n+g}$ of weight $m+n+g$ with $D_m + D_n \subset (\mathcal{R}_{3g})_0$, if $m+n \geqslant g$ and $D_m + D_n$ contains no points in involution.*

A proof is similar to the proof of Theorem 3.

Theorem 5. *A non-special divisor D_g of degree g on a hyperelliptic curve of genus g is uniquely defined by a pair of functions $\mathcal{R}_{2g}$, $\mathcal{R}_{2g+1}$.*

Proof. The function $\mathcal{R}_{2g}$ is defined by x-coordinates of the support of D_g. The same divisor D_g can be used to construct $\mathcal{R}_{2g+1}$, according to Proposition 5, with an addition condition: the coefficient of monomial $\mathfrak{m}_{2g}$ vanishes. Such a pair of functions define a solution of the Jacobi inversion problem, see Proposition 1. □

Remark 2. If the two functions $\mathcal{R}_{2g}$, $\mathcal{R}_{2g+1}$ define D_g, then $(\mathcal{R}_{2g})_0 = D_g + D_g^*$, where $D_g^* = -D_g$, and $(\mathcal{R}_{2g+1})_0 = D_g + D_{g+1}$. We also have $-D_g + (-D_{g+1}) = (\mathcal{R}^-_{2g+1})_0$, where $\mathcal{R}^-_{2g+1}$ denotes the function $\mathcal{R}_{2g+1}(x, -y)$.

4. Addition and duplication

Below, the addition and duplication laws are derived according to [8].

4.1. **Addition law.** Addition of two degree 2 non-special divisors is defined by a polynomial function of weight 6, which has the form

$$\mathcal{R}_6(x,y) = x^3 + \gamma_1 y + \gamma_2 x^2 + \gamma_4 x + \gamma_6.$$

Let $\mathcal{R}_6$ be defined by $D_4 \subset (\mathcal{R}_6)_0$ such that $D_4 = D_{2P} + D_{2Q} = (P_1 + P_2) + (Q_1 + Q_2)$ without repeated[2] points, see Proposition 5. According to Proposition 1 and Remark 1, let D_{2A} be defined by $\mathcal{R}_4^{[A]}$ and $\mathcal{R}_5^{[A]}$ with Mumford coordinates $\alpha_2^{[A]}$, $\alpha_4^{[A]}$, $\beta_3^{[A]}$, $\beta_5^{[A]}$, where A stands for P, or Q.

With $A = P, Q$ we have the equality

$$\mathcal{R}_6(x,y) = \gamma_1 \mathcal{R}_5^{[A]}(x,y) + (x - \alpha_2^{[A]} + \gamma_2)\mathcal{R}_4^{[A]}(x) \equiv \mathsf{S}_4^{[A]} x + \mathsf{S}_6^{[A]}, \tag{24}$$

which introduces $\mathsf{S}_4^{[A]}$, $\mathsf{S}_6^{[A]}$ as polynomials in $\alpha_2^{[A]}$, $\alpha_4^{[A]}$, $\beta_3^{[A]}$, $\beta_5^{[A]}$, and coefficients γ_k of $\mathcal{R}_6$. Since $\mathcal{R}_6$ vanishes on D_{2P} and D_{2Q}, we obtain four equations, which are linear in γ_k, and admit the matrix form

$$\begin{pmatrix} \mathsf{S}_6^{[P]} \\ \mathsf{S}_4^{[P]} \\ \mathsf{S}_6^{[Q]} \\ \mathsf{S}_4^{[Q]} \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 & -\alpha_4^{[P]} & -\beta_5^{[P]} \\ 0 & 1 & -\alpha_2^{[P]} & -\beta_3^{[P]} \\ 1 & 0 & -\alpha_4^{[Q]} & -\beta_5^{[Q]} \\ 0 & 1 & -\alpha_2^{[Q]} & -\beta_3^{[Q]} \end{pmatrix} \begin{pmatrix} \gamma_6 \\ \gamma_4 \\ \gamma_2 \\ \gamma_1 \end{pmatrix} + \begin{pmatrix} \alpha_2^{[P]}\alpha_4^{[P]} \\ (\alpha_2^{[P]})^2 - \alpha_4^{[P]} \\ \alpha_2^{[Q]}\alpha_4^{[Q]} \\ (\alpha_2^{[Q]})^2 - \alpha_4^{[Q]} \end{pmatrix} = 0. \tag{25}$$

[2]There is no n-torsion divisors which contain repeated points. See the definition of an n-torsion divisor in the next section.

Solving (25), we find

$$\begin{pmatrix}\gamma_2\\ \gamma_1\end{pmatrix} = \begin{pmatrix}\alpha_4^{[P]}-\alpha_4^{[Q]} & \beta_5^{[P]}-\beta_5^{[Q]}\\ \alpha_2^{[P]}-\alpha_2^{[Q]} & \beta_3^{[P]}-\beta_3^{[Q]}\end{pmatrix}^{-1}\begin{pmatrix}\alpha_2^{[P]}\alpha_4^{[P]}-\alpha_2^{[Q]}\alpha_4^{[Q]}\\ (\alpha_2^{[P]})^2-(\alpha_2^{[Q]})^2-\alpha_4^{[P]}+\alpha_4^{[Q]}\end{pmatrix}, \tag{26a}$$

$$\begin{pmatrix}\gamma_6\\ \gamma_4\end{pmatrix} = \begin{pmatrix}\alpha_4^{[P]} & \beta_5^{[P]}\\ \alpha_2^{[P]} & \beta_3^{[P]}\end{pmatrix}\begin{pmatrix}\gamma_2\\ \gamma_1\end{pmatrix} - \begin{pmatrix}\alpha_2^{[P]}\alpha_4^{[P]}\\ (\alpha_2^{[P]})^2-\alpha_4^{[P]}\end{pmatrix}. \tag{26b}$$

Formulas (26) define $\mathcal{R}_6$ in terms of $\alpha_2^{[A]}$, $\alpha_4^{[A]}$, $\beta_3^{[A]}$, $\beta_5^{[A]}$ with $A=P$, Q.

Let D_2^* be a divisor of degree 2 such that $(\mathcal{R}_6)_0 = D_{2P}+D_{2Q}+D_2^*$. According to Remark 1, we define D_2^* by the two polynomial functions

$$\mathcal{R}_4^*(x) = x^2+\alpha_2^*x+\alpha_4^*, \qquad \mathcal{R}_5^*(x,y) = y+\beta_3^*x+\beta_5^*.$$

Recalling that $(\mathcal{R}_6)_0$ is defined by a system of the form (22), we have

$$-\gamma_1^2 f(x,y_{\mathcal{R}_6};\lambda) = \mathcal{R}_4^{[P]}(x)\mathcal{R}_4^{[Q]}(x)\mathcal{R}_4^*(x), \tag{27}$$

where $y_{\mathcal{R}_6}$ is obtained from $\mathcal{R}_6(x,y_{\mathcal{R}_6})=0$, namely

$$y_{\mathcal{R}_6} = -\gamma_1^{-1}\big(x^3+\gamma_2x^2+\gamma_4x+\gamma_6\big).$$

Coordinates α_2^*, α_4^* are computed from coefficients of x^5 and x^4 in (27). Then $\mathcal{R}_5^*$ is derived from (24), since $\mathcal{R}_6$ vanishes on D_2^* as well, namely

$$\mathcal{R}_5^*(x,y) = \gamma_1^{-1}\big(\mathcal{R}_6(x,y)-(x+\gamma_2-\alpha_2^*)\mathcal{R}_4^*(x)\big). \tag{28}$$

This produces coordinates β_3^*, β_5^*.

Finally, let $\widetilde{D}_2 \equiv -D_2^*$, and so $\widetilde{D}_2 \sim D_{2P}+D_{2Q}$, that is $\widetilde{D}_2$ is the reduced divisor equivalent to $D_{2P}+D_{2Q}$. Then $\widetilde{D}_2$ is defined by the Mumford coordinates

$$\begin{aligned}
\alpha_2^{[P+Q]} &= \alpha_2^* = -\alpha_2^{[P]}-\alpha_2^{[Q]}+2\gamma_2-\gamma_1^2,\\
\alpha_4^{[P+Q]} &= \alpha_4^* = -\alpha_4^{[P]}-\alpha_4^{[Q]}+\big(\alpha_2^{[P]}\big)^2+\alpha_2^{[P]}\alpha_2^{[Q]}+\big(\alpha_2^{[Q]}\big)^2\\
&\qquad -\big(\alpha_2^{[P]}+\alpha_2^{[Q]}\big)\big(2\gamma_2-\gamma_1^2\big)+2\gamma_4+\gamma_2^2-\lambda_2\gamma_1^2,
\end{aligned} \tag{29a}$$

$$\begin{aligned}
\beta_3^{[P+Q]} &= -\beta_3^* = -\gamma_1^{-1}\big((\alpha_2^{[P+Q]})^2-\alpha_4^{[P+Q]}-\gamma_2\alpha_2^{[P+Q]}+\gamma_4\big),\\
\beta_5^{[P+Q]} &= -\beta_5^* = -\gamma_1^{-1}\big(\alpha_2^{[P+Q]}\alpha_4^{[P+Q]}-\gamma_2\alpha_4^{[P+Q]}+\gamma_6\big).
\end{aligned} \tag{29b}$$

4.2. **Addition law on special divisors.** The case of adding a special divisor $D_{1Q}=Q_1=(x_1^{[Q]},y_1^{[Q]})$ to a non-special divisors $D_{2P}=P_1+P_2$ can be obtained from the above formulas (29) by taking the limit as $Q_2\to\infty$, that is by applying the parametrization (2) to $(x_2^{[Q]},y_2^{[Q]})$ and taking the limit as $\xi\to 0$. As a result, the following formulas are obtained ($x_1^{[Q]}\equiv x_Q$, $y_1^{[Q]}\equiv y_Q$):

$$\begin{aligned}
\alpha_2^{[P+Q]} &= -\alpha_2^{[P]}+x_Q+\lambda_2-\gamma_1^2,\\
\alpha_4^{[P+Q]} &= -\alpha_4^{[P]}+(\alpha_2^{[P]})^2+(x_Q-\alpha_2^{[P]})\big(x_Q+\lambda_2-\gamma_1^2\big)+\lambda_4-2\gamma_1\gamma_3,\\
\beta_3^{[P+Q]} &= \gamma_1\alpha_2^{[P+Q]}-\gamma_3,\\
\beta_5^{[P+Q]} &= \gamma_1\alpha_4^{[P+Q]}-\gamma_5,
\end{aligned} \tag{30}$$

where

$$\gamma_1 = -\frac{y_Q+x_Q\beta_3^{[P]}+\beta_5^{[P]}}{x_Q^2+x_Q\alpha_2^{[P]}+\alpha_4^{[P]}},$$

$$\gamma_3 = \frac{-y_Q\alpha_2^{[P]} + x_Q^2\beta_3^{[P]} + \alpha_4^{[P]}\beta_3^{[P]} - \alpha_2^{[P]}\beta_5^{[P]}}{x_Q^2 + x_Q\alpha_2^{[P]} + \alpha_4^{[P]}},$$
$$\gamma_5 = \frac{-y_Q\alpha_4^{[P]} + x_Q^2\beta_5^{[P]} - x_Q(\alpha_4^{[P]}\beta_3^{[P]} - \alpha_2^{[P]}\beta_5^{[P]})}{x_Q^2 + x_Q\alpha_2^{[P]} + \alpha_4^{[P]}}.$$

After taking the limit of (30) as $P_2 \to \infty$ in a similar way, we obtain formulas for the Mumford coordinates of the sum of two special divisors: $D_{1P} = P_1 = (x_P, y_P)$ and $D_{1Q} = Q_1 = (x_Q, y_Q)$, which, evidently, coincide with (18):

$$\alpha_2^{[P+Q]} = -x_P - x_Q, \qquad \alpha_4^{[P+Q]} = x_P x_Q,$$
$$\beta_3^{[P+Q]} = -\frac{y_P - y_Q}{x_P - x_Q}, \qquad \beta_5^{[P+Q]} = \frac{x_Q y_P - x_P y_Q}{x_P - x_Q}.$$

4.3. **Duplication law.** We are also interested in duplication: $D_4 = 2D_2$, when $D_{2P} = D_{2Q} = D_2$. Let $D_2 = (x_1, y_1) + (x_2, y_2)$, and α_2, α_4, β_3, β_5 be defined by (18). In this case, the system of equations for γ_k has the form

$$\mathsf{S}_6 = 0, \quad \mathsf{S}_4 = 0, \quad \mathrm{d}_{x_1,x_2}\mathsf{S}_6 = 0, \quad \mathrm{d}_{x_1,x_2}\mathsf{S}_4 = 0, \tag{31}$$

where $\mathrm{d}_{x_1,x_2} = \dfrac{\mathrm{d}}{\mathrm{d}x_1} + \dfrac{\mathrm{d}}{\mathrm{d}x_2}$. We denote

$$\begin{aligned} &\alpha_2' = \mathrm{d}_{x_1,x_2}\alpha_2 = -2, && \alpha_4' = \mathrm{d}_{x_1,x_2}\alpha_4 = x_1 + x_2, \\ &\beta_3' = \mathrm{d}_{x_1,x_2}\beta_3 = -\frac{y_1' - y_2'}{x_1 - x_2}, && \beta_5' = \mathrm{d}_{x_1,x_2}\beta_5 = \frac{y_1' x_2 - y_2' x_1}{x_1 - x_2} + \frac{y_1 - y_2}{x_1 - x_2}, \end{aligned} \tag{32}$$

where y_i', $i = 1, 2$, are computed by

$$y_i' = \lim_{(x,y)\to(x_i,y_i)} \frac{-\partial_x f(x, y; \lambda)}{\partial_y f(x, y; \lambda)} = \frac{\mathcal{P}'(x_i)}{2y_i}.$$

By taking into account that $\alpha_4' = -\alpha_2$, and $\beta_5' = \frac{y_1' x_2 - y_2' x_1}{x_1 - x_2} - \beta_3$, the system of equations (31) is reduced to the following matrix form

$$\begin{pmatrix} 1 & 0 & -\alpha_4 & -\beta_5 \\ 0 & 1 & -\alpha_2 & -\beta_3 \\ 0 & 1 & 0 & -\beta_5' - \beta_3 \\ 0 & 0 & 2 & -\beta_3' \end{pmatrix} \begin{pmatrix} \gamma_6 \\ \gamma_4 \\ \gamma_2 \\ \gamma_1 \end{pmatrix} + \begin{pmatrix} \alpha_2\alpha_4 \\ \alpha_2^2 - \alpha_4 \\ -3\alpha_4 \\ -3\alpha_2 \end{pmatrix} = 0. \tag{33}$$

A solution of (33) is given by

$$\begin{pmatrix} \gamma_2 \\ \gamma_1 \end{pmatrix} = \frac{1}{2\beta_5' - \alpha_2\beta_3'} \begin{pmatrix} 3\alpha_2\beta_5' - \big(\alpha_2^2 + 2\alpha_4\big)\beta_3' \\ \alpha_2^2 - 4\alpha_4 \end{pmatrix}, \tag{34a}$$

$$\begin{pmatrix} \gamma_6 \\ \gamma_4 \end{pmatrix} = \begin{pmatrix} \alpha_4 & \beta_5 \\ \alpha_2 & \beta_3 \end{pmatrix} \begin{pmatrix} \gamma_2 \\ \gamma_1 \end{pmatrix} - \begin{pmatrix} \alpha_2\alpha_4 \\ \alpha_2^2 - \alpha_4 \end{pmatrix}, \tag{34b}$$

or in terms of coordinates

$$\begin{pmatrix} \gamma_6 \\ \gamma_4 \\ \gamma_2 \\ \gamma_1 \end{pmatrix} = \begin{pmatrix} -\frac{1}{2}x_1x_2(x_1 + x_2) \\ 3x_1x_2 \\ -\frac{3}{2}(x_1 + x_2) \\ 0 \end{pmatrix} + \frac{(x_1 - x_2)^2}{(y_1' + y_2')(x_1 - x_2) - 2(y_1 - y_2)} \times \tag{35}$$

$$\times \begin{pmatrix} -\frac{1}{2}x_1x_2(y_1'-y_2')+x_2y_1-x_1y_2 \\ -(x_2y_1'-x_1y_2') \\ \frac{1}{2}(y_1'-y_2') \\ -(x_1-x_2) \end{pmatrix}.$$

Finally, the reduced divisor $\widetilde{D}_2 \sim 2D_{2Q}$ is defined by

$$\begin{aligned} \alpha_2^{[2Q]} &= -2\alpha_2^{[Q]} + 2\gamma_2 - \gamma_1^2, \\ \alpha_4^{[2Q]} &= -2\alpha_4^{[Q]} + 3\big(\alpha_2^{[Q]}\big)^2 - 2\alpha_2^{[Q]}\big(2\gamma_2 - \gamma_1^2\big) + 2\gamma_4 + \gamma_2^2 - \lambda_2\gamma_1^2, \end{aligned} \tag{36a}$$

$$\begin{aligned} \beta_3^{[2Q]} &= -\gamma_1^{-1}\big((\alpha_2^{[2Q]})^2 - \alpha_4^{[2Q]} - \gamma_2\alpha_2^{[2Q]} + \gamma_4\big), \\ \beta_5^{[2Q]} &= -\gamma_1^{-1}\big(\alpha_2^{[2Q]}\alpha_4^{[2Q]} - \gamma_2\alpha_4^{[2Q]} + \gamma_6\big), \end{aligned} \tag{36b}$$

where $\alpha_2^{[Q]} \equiv \alpha_2$, $\alpha_4^{[Q]} \equiv \alpha_4$, $\beta_3^{[Q]} \equiv \beta_3$, $\beta_5^{[Q]} \equiv \beta_5$.

4.4. **The case of $D_4 \sim D_1$.** The case of $D_{2P} + D_{2Q} \sim D_1$, when the result of addition is a special divisor $D_1 = (x_{P+Q}, y_{P+Q})$, deserves special consideration. In this case, addition is implemented through a polynomial function of weight 5 of the form

$$\widetilde{\mathcal{R}}_5(x,y) = y + \gamma_1 x^2 + \gamma_3 x + \gamma_5,$$

whose divisor of zeros is composed of D_{2P}, D_{2Q}, and D_1^* such that $D_1^* = -D_1$.

With $A = P$, Q we have the equality

$$\widetilde{\mathcal{R}}_5(x,y) = \mathcal{R}_5^{[A]}(x,y) + \gamma_1\mathcal{R}_4^{[A]}(x) \equiv \mathsf{S}_3^{[A]}x + \mathsf{S}_5^{[A]},$$

where

$$\mathsf{S}_3^{[A]} = \gamma_3 - \alpha_2^{[A]}\gamma_1 - \beta_3^{[A]}, \qquad \mathsf{S}_5^{[A]} = \gamma_5 - \alpha_4^{[A]}\gamma_1 - \beta_5^{[A]}.$$

The overdetermined system

$$\mathsf{S}_3^{[P]} = 0, \qquad \mathsf{S}_5^{[P]} = 0, \qquad \mathsf{S}_3^{[Q]} = 0, \qquad \mathsf{S}_5^{[Q]} = 0 \tag{37}$$

is consistent, and produces the condition

$$\gamma_1 = -\frac{\beta_3^{[P]} - \beta_3^{[Q]}}{\alpha_2^{[P]} - \alpha_2^{[Q]}} = -\frac{\beta_5^{[P]} - \beta_5^{[Q]}}{\alpha_4^{[P]} - \alpha_4^{[Q]}}, \tag{38}$$

which singles out pairs of divisors D_{2P}, D_{2Q} whose sum is equivalent to a special divisor D_1. This condition causes vanishing the denominator in (26). From the system (37) we also find

$$\gamma_3 = -\frac{\alpha_2^{[Q]}\beta_3^{[P]} - \alpha_2^{[P]}\beta_3^{[Q]}}{\alpha_2^{[P]} - \alpha_2^{[Q]}}, \qquad \gamma_5 = \beta_5^{[P]} - \alpha_4^{[P]}\frac{\beta_3^{[P]} - \beta_3^{[Q]}}{\alpha_2^{[P]} - \alpha_2^{[Q]}}. \tag{39}$$

Finally, with the help of the equality $y_{\widetilde{\mathcal{R}}_5} = -\big(\gamma_1x^2 + \gamma_3x + \gamma_5\big)$ used in

$$f(x, y_{\widetilde{\mathcal{R}}_5}; \lambda) = \mathcal{R}_4^{[P]}(x)\mathcal{R}_4^{[Q]}(x)\big(x - x_{P+Q}\big),$$

we obtain

$$\begin{aligned} x_{P+Q} &= \alpha_2^{[P]} + \alpha_2^{[Q]} + \gamma_1^2 - \lambda_2, \\ y_{P+Q} &= \gamma_1x_{P+Q}^2 + \gamma_3x_{P+Q} + \gamma_5. \end{aligned} \tag{40}$$

In the case of duplication $2D_{2Q} \sim D_1$, which leads to a special divisor $D_1 = (x_{2Q}, y_{2Q})$, we replace the system (37) with

$$\mathsf{S}_3^{[Q]} = 0, \qquad \mathsf{S}_5^{[Q]} = 0, \qquad \mathrm{d}_{x_1,x_2}\mathsf{S}_3^{[Q]} = 0, \qquad \mathrm{d}_{x_1,x_2}\mathsf{S}_5^{[Q]} = 0, \tag{41}$$

and obtain the condition

$$2\beta_5'^{[Q]} = \alpha_2{}^{[Q]}\beta_3'^{[Q]}, \qquad \text{or} \qquad \frac{1}{2}(y_1' + y_2') = \frac{y_1 - y_2}{x_1 - x_2}, \tag{42}$$

which singles out such D_{2Q} that $2D_{2Q} \sim D_1$. Then we find expressions for γ_k:

$$\gamma_1 = \tfrac{1}{2}\beta_3'^{[Q]}, \quad \gamma_3 = \tfrac{1}{2}\big(2\beta_3^{[Q]} + \alpha_2^{[Q]}\beta_3'^{[Q]}\big), \quad \gamma_5 = \tfrac{1}{2}\big(2\beta_5^{[Q]} + \alpha_4^{[Q]}\beta_3'^{[Q]}\big). \tag{43}$$

Finally, we find coordinates of the resulting divisor D_1:

$$\begin{aligned} x_{2Q} &= 2\alpha_2^{[Q]} + \gamma_1^2 - \lambda_2, \\ y_{2Q} &= \gamma_1 x_{2Q}^2 + \gamma_3 x_{2Q} + \gamma_5. \end{aligned} \tag{44}$$

5. Torsion divisors

Let $D \in \mathcal{C}^2$ be a reduced divisor, special or non-special. We say that D is an *n-torsion* divisor, if $nD \sim O$, where $O = 2\infty$ denotes the neutral divisor, and D generates a cyclic group of order n: $C_n = \langle O, D\rangle$. This definition implies the following criterion.

Theorem 6. *A divisor $D \in \mathcal{C}^2$ is n-torsion when the following holds*

(i) $(k+1)D \sim -kD$, *if* $n = 2k+1$; *or*
(ii) $kD \sim -kD$, *if* $n = 2k$.

Remark 3. n-Torsion divisors are the Abel pre-images of points of order n on $\mathrm{Jac}(\mathcal{C})$, that is, of $u[\varepsilon] \in \mathrm{Jac}(\mathcal{C})$ computed by (12) from characteristics $[\varepsilon]$ of order n. of such $u[\varepsilon]$. An example of computations of 2-, 3- and 4-torsion divisors on a genus four curve is implemented in Wolfram Mathematica 12, and can be found at `https://community.wolfram.com/groups/-/m/t/3314103`. This example, as well as computations on a genus two curve, shows that n-torsion divisors are non-special, except the case of $n = 2$.

Condition (i) in Theorem 6 implies

$$\alpha_2^{[(k+1)D]} = \alpha_2^{[kD]}, \qquad \alpha_4^{[(k+1)D]} = \alpha_4^{[kD]}. \tag{45}$$

Relations for β-coordinates in this case are trivial.

Condition (ii) implies that kD is 2-torsion, that is

$$\beta_3^{[kD]} = -\beta_3^{[kD]} = 0, \qquad \beta_5^{[kD]} = -\beta_5^{[kD]} = 0, \tag{46}$$

if kD is non-special. If kD is special, then $kD \sim (x_{kD}, y_{kD})$, and instead of (46) we have

$$y_{kD} = -y_{kD} = 0. \tag{46'}$$

Relations for α-coordinates in case (ii) are trivial. Equations (45) and (46) written in terms of $\alpha_2^{[D]}$, $\alpha_4^{[D]}$, $\beta_3^{[D]}$, $\beta_5^{[D]}$ can be considered as *division polynomials* in Mumford coordinates.

5.1. **2-Torsion divisors.** 2-Torsion divisors are defined by the condition $y_i = 0$, which implies that x_i are x-coordinates of branch points. That is, 2-torsion divisors are Abel pre-images of half-periods on $\mathrm{Jac}(\mathcal{C})$. Among fifteen 2-torsion divisors, ten are composed of two finite branch points, and correspond to even characteristics. The remaining five 2-torsion divisors are composed of infinity and one finite branch point, and correspond to odd characteristics.

5.2. **3-Torsion divisors.** Let $D_{2Q} = (x_1, y_1)+(x_2, y_2)$ be a 3-torsion divisor, which means that $2D_{2Q} \sim -D_{2Q}$. Note, that all 3-torsion divisors are non-special. From (45) we find the criterion

$$\alpha_2^{[2Q]} = \alpha_2^{[Q]}, \qquad \alpha_4^{[2Q]} = \alpha_4^{[Q]}. \tag{47}$$

Applying the duplication law (36), we obtain the equations which define 3-torsion divisors in terms of Mumford coordinates ($\alpha_2^{[Q]} \equiv \alpha_2$, $\alpha_4^{[Q]} \equiv \alpha_4$):

$$\begin{aligned} &3\alpha_2 = 2\gamma_2 - \gamma_1^2, \\ &3\alpha_4 = 3\alpha_2^2 - 2\alpha_2\big(2\gamma_2 - \gamma_1^2\big) + 2\gamma_4 + \gamma_2^2 - \lambda_2\gamma_1^2, \end{aligned} \tag{48}$$

where parameters γ_k are defined by (35).

Therefore, all pairs of points (x_1, y_1), (x_2, y_2) which form 3-torsion divisors can be obtained from (48), subject to $f(x_1, y_1; \lambda) = 0$, $f(x_2, y_2; \lambda) = 0$. Substituting (35) and (18), we rewrite these equations in terms of coordinates:

$$\begin{aligned} &(y_1' - y_2')\Big((y_1' + y_2')(x_1 - x_2) - 2(y_1 - y_2)\Big) - (x_1 - x_2)^4 = 0, \\ &-\big(x_2(y_1')^2 - x_1(y_2')^2\big)(x_1 - x_2) + 2\big(x_1y_1' - x_2y_2'\big)(y_1 - y_2) \\ &\qquad\qquad - 3(y_1 - y_2)^2 - (2x_1 + 2x_2 + \lambda_3)(x_1 - x_2)^4 = 0, \end{aligned}$$

or

$$\begin{aligned} \mathcal{Y}(x_1, y_1; x_2, y_2) \equiv\ & y_1y_2\big(\mathcal{P}'(x_1)\mathcal{P}(x_2) + \mathcal{P}'(x_2)\mathcal{P}(x_1)\big) \\ & + \tfrac{1}{4}(x_1 - x_2)\big(\mathcal{P}'(x_1)^2\mathcal{P}(x_2) - \mathcal{P}'(x_2)^2\mathcal{P}(x_1)\big) \\ & - \mathcal{P}(x_1)\mathcal{P}(x_2)\big(\mathcal{P}'(x_1) + \mathcal{P}'(x_2) + (x_1 - x_2)^4\big) = 0, \end{aligned} \tag{49a}$$

$$\begin{aligned} & y_1y_2\big(6\mathcal{P}(x_1)\mathcal{P}(x_2) - x_1\mathcal{P}'(x_1)\mathcal{P}(x_2) - x_2\mathcal{P}'(x_2)\mathcal{P}(x_1)\big) \\ & - \tfrac{1}{4}(x_1 - x_2)\big(x_2\mathcal{P}'(x_1)^2\mathcal{P}(x_2) - x_1\mathcal{P}'(x_2)^2\mathcal{P}(x_1)\big) \\ & + \mathcal{P}(x_1)\mathcal{P}(x_2)\big(x_1\mathcal{P}'(x_1) - 3\mathcal{P}(x_1) + x_2\mathcal{P}'(x_2) - 3\mathcal{P}(x_2) \\ & \quad - (2x_1 + 2x_2 + \lambda_2)(x_1 - x_2)^4\big) = 0. \end{aligned} \tag{49b}$$

Finally, we eliminate y_1y_2 from these two equations, and cancel the common factor $(x_1 - x_2)^4$, namely

$$\begin{aligned} \mathcal{X}(x_1, x_2) \equiv\ & -\frac{1}{4}\big(\mathcal{P}(x_2)^2\mathcal{P}'(x_1)\mathcal{T}(x_1)^2 + \mathcal{P}(x_1)^2\mathcal{P}'(x_2)\mathcal{T}(x_2)^2\big) \\ & + \frac{1}{2}\frac{\mathcal{P}(x_2)^3\mathcal{T}(x_1)^2 - \mathcal{P}(x_1)^3\mathcal{T}(x_2)^2}{(x_1 - x_2)} - \frac{1}{4}\left(\frac{\mathcal{P}(x_1) - \mathcal{P}(x_2)}{x_1 - x_2}\right)^5 \\ & + \frac{3}{4}\frac{\mathcal{P}(x_2)^2\mathcal{T}(x_1) + \mathcal{P}(x_1)^2\mathcal{T}(x_2)}{(x_1 - x_2)}\left(\frac{\mathcal{P}(x_1) - \mathcal{P}(x_2)}{x_1 - x_2}\right)^2 \\ & - \mathcal{P}(x_1)\mathcal{P}(x_2)\frac{\mathcal{P}(x_2)\mathcal{P}'(x_1) - \mathcal{P}(x_1)\mathcal{P}'(x_2)}{x_1 - x_2}\left(\frac{\mathcal{T}(x_1) + \mathcal{T}(x_2)}{x_1 - x_2}\right) \end{aligned} \tag{50}$$

$$+\mathcal{P}(x_1)\mathcal{P}(x_2)\Big(-6\mathcal{P}(x_1)\mathcal{P}(x_2)+x_1\mathcal{P}(x_2)\mathcal{P}'(x_1)+x_2\mathcal{P}(x_1)\mathcal{P}'(x_2)$$
$$+\big(\mathcal{P}(x_2)\mathcal{P}'(x_1)+\mathcal{P}(x_1)\mathcal{P}'(x_2)\big)(2x_1+2x_2+\lambda_2)\Big)=0,$$

where

$$\begin{aligned}\mathcal{T}(x_i)&=\frac{\mathcal{P}(x_1)-\mathcal{P}(x_3)-\mathcal{P}'(x_i)(x_1-x_3)}{(x_1-x_3)^2}\\&=\frac{1}{x_1-x_2}\Big(x_1^4+x_1^3x_2+x_1^2x_2^2+x_1x_3^3+x_2^4-5x_i^4\\&\quad+\lambda_2\big(x_1^3+x_1^2x_2+x_1x_2^2+x_2^3-4x_i^3\big)\\&\quad+\lambda_4\big(x_1^2+x_1x_2+x_3^2-3x_i^2\big)+\lambda_6(x_1+x_2-2x_i)\Big),\end{aligned}$$

which is a polynomial, as follows from the series expansion of $\mathcal{P}$ about x_i. By direct computations, one can verify that the following functions are polynomials

$$\frac{\mathcal{T}(x_1)+\mathcal{T}(x_2)}{x_1-x_2},\quad \frac{\mathcal{P}(x_2)^2\mathcal{T}(x_1)+\mathcal{P}(x_1)^2\mathcal{T}(x_2)}{x_1-x_2},\quad \frac{\mathcal{P}(x_2)^3\mathcal{T}(x_1)^2-\mathcal{P}(x_1)^3\mathcal{T}(x_2)^2}{x_1-x_2}.$$

The polynomial $\mathcal{X}$ in (50) has weight 40, and vanishes on 40 pairs $\{x_1,\,x_2\}$. In the system (49) we replace (49b) with (50),

Theorem 7. *The polynomials $\mathcal{X}$ and $\mathcal{Y}$ defined by* (50) *and* (49a) *on a curve $\mathcal{C}$ defined by* (1) *single out the collection of* 3*-torsion divisors, which are Abel preimages of $u[\varepsilon]\in\mathrm{Jac}(\mathcal{C})$ with characteristics $[\varepsilon]$ of order* 3.

5.3. **4-Torsion divisors.** There exist 240 characteristics of order 4 excluding half-integer characteristics. Let $\mathfrak{E}$ denote the set of these 240 characteristics. Each characteristic of $\mathfrak{E}$ produces a 4-torsion divisor $D_{2Q}=(x_1,y_1)+(x_2,y_2)$, which is non-special. We split $\mathfrak{E}$ into two parts:

- $\mathfrak{E}_{\text{non-spec}}=\{[\varepsilon]\in\mathfrak{E}\mid \mathcal{A}^{-1}(u[2\varepsilon])=D_2,\ \deg D_2=2\}$ of cardinality 160, the divisor $D_2\sim 2D_{2Q}$ is characterized by its Mumford coordinates $\alpha_2^{[2Q]}$, $\alpha_4^{[2Q]}$, $\beta_3^{[2Q]}$, $\beta_5^{[2Q]}$;
- $\mathfrak{E}_{\text{spec}}=\{[\varepsilon]\in\mathfrak{E}\mid \mathcal{A}^{-1}(u[2\varepsilon])=D_1,\ \deg D_1=1\}$ of cardinality 80, the divisor $D_1\sim 2D_{2Q}$ is characterized by x-, y-coordinates: $D_1=(x_{2Q},y_{2Q})$.

Divisors D_{2Q} produced from characteristics of $\mathfrak{E}_{\text{non-spec}}$ satisfy the conditions

$$\beta_3^{[2Q]}=0,\qquad \beta_5^{[2Q]}=0, \tag{51}$$

obtained from (46). In the Mumford coordinates of D_{2Q} the equalities (51) acquire the form ($\alpha_2^{[Q]}\equiv\alpha_2$, $\alpha_4^{[Q]}\equiv\alpha_4$)

$$\begin{aligned}&-2\alpha_4-\alpha_2^2+\big(2\alpha_2-\gamma_2+\gamma_1^2\big)\big(\gamma_2-\gamma_1^2\big)+\gamma_1^2\big(\gamma_2-\lambda_2\big)+\gamma_4=0,\\&\big(-2\alpha_4+(3\alpha_2-\gamma_2)(\alpha_2-\gamma_2)+\gamma_1^2(2\alpha_2-\lambda_2)+2\gamma_4\big)\big(2\alpha_2-\gamma_2+\gamma_1^2\big)=\gamma_6,\end{aligned} \tag{52}$$

where γ_k are defined by (34).

Divisors D_{2Q} produced from characteristics of $\mathfrak{E}_{\text{spec}}$ satisfy the condition $y_{2Q}=0$, which follows from (46'), and in terms of the Mumford coordinates of D_{2Q} acquires the form

$$\big(\gamma_1(2\alpha_2+\gamma_1^2-\lambda_2)+\gamma_3\big)\big(2\alpha_2+\gamma_1^2-\lambda_2\big)+\gamma_5=0, \tag{52'}$$

where γ_k are defined by (43).

In https://community.wolfram.com/groups/-/m/t/3338527 the reader may find an example of computing 3- and 4-torsion divisors on a genus two curve, along with derivation of the corresponding division polynomials in Mumford coordinates, and in x-, y-coordinates.

Appendix A. Transformation to canonical curve

There are several types of equations which define a genus two curve.

(I) Let a genus two curve has the form

$$\begin{aligned} 0 = f(x,y) &= -y^2 + y\mathcal{Q}(x) + \mathcal{P}(x) \\ &= -y^2 + y\big(\nu_1 x^2 + \nu_3 x + \nu_5\big) \\ &\quad + x^5 + \nu_2 x^4 + \nu_4 x^3 + \nu_6 x^2 + \nu_8 x + \nu_{10}. \end{aligned} \tag{53}$$

By the map $y \mapsto y + \frac{1}{2}\mathcal{Q}(x)$ the curve (53) transforms into the form (1), namely

$$\begin{aligned} 0 = f(x,y) &= -y^2 + \Delta(x) \\ &= -y^2 + x^5 + \lambda_2 x^4 + \lambda_4 x^3 + \lambda_6 x^2 + \lambda_8 x + \lambda_{10}, \end{aligned}$$

where $\Delta(x) = \mathcal{P}(x) + \frac{1}{4}\mathcal{Q}(x)^2$, and

$$\begin{aligned} &\lambda_2 = \nu_2 + \tfrac{1}{4}\nu_1^2, && \lambda_8 = \nu_8 + \tfrac{1}{2}\nu_3\nu_5, \\ &\lambda_4 = \nu_4 + \tfrac{1}{2}\nu_1\nu_3, && \lambda_{10} = \nu_{10} + \tfrac{1}{4}\nu_5^2, \\ &\lambda_6 = \nu_6 + \tfrac{1}{2}\nu_1\nu_5 + \tfrac{1}{4}\nu_3^2. \end{aligned} \tag{54}$$

(II) Let a genus two curve has the form

$$\begin{aligned} 0 = f(x,y;\lambda) &= -y^2 + \bar{\mathcal{P}}(x) \\ &= -y^2 + a_0 x^6 + a_1 x^5 + a_2 x^4 + a_3 x^3 + a_4 x^2 + a_5 x + a_6. \end{aligned} \tag{55}$$

Let $\{e_i\}_{i=0}^5$ be roots of $\bar{\mathcal{P}}$, ordered ascendingly in the real part, and then in the imaginary part. Transformation to a curve in the form (1) is realized by moving the smallest root e_0 to infinity, namely

$$x \mapsto e_0 + \frac{\bar{\mathcal{P}}'(e_0)}{x - \frac{1}{10}\bar{\mathcal{P}}''(e_0)}, \qquad y \mapsto \frac{y\bar{\mathcal{P}}'(e_0)}{\big(x - \frac{1}{10}\bar{\mathcal{P}}''(e_0)\big)^3}. \tag{56}$$

If a canonical basis is chosen as explained in [5, §3.4], such a transformation of the curve does not change the correspondence between characteristics and divisors.

(III) Let a genus two curve has the form

$$\begin{aligned} 0 = f(x,y) &= -y^2 + y\bar{\mathcal{Q}}(x) + \bar{\mathcal{P}}(x) \\ &= -y^2 + y\big(\bar{b}_0 x^3 + \bar{b}_1 x^2 + \bar{b}_2 x + \bar{b}_3\big) \\ &\quad + \bar{a}_0 x^6 + \bar{a}_1 x^5 + \bar{a}_2 x^4 + \bar{a}_3 x^3 + \bar{a}_4 x^2 + \bar{a}_5 x + \bar{a}_6. \end{aligned} \tag{57}$$

By the map $y \mapsto y + \frac{1}{2}\bar{\mathcal{Q}}(x)$ the curve (57) transforms into (55)

$$\begin{aligned} 0 = f(x,y;\lambda) &= -y^2 + \bar{\Delta}(x) \\ &= -y^2 + a_0 x^6 + a_1 x^5 + a_2 x^4 + a_3 x^3 + a_4 x^2 + a_5 x + a_6, \end{aligned}$$

and then by (56) to the form (1).

Appendix B. Addition law on a curve with extra terms

Addition law on a curve of the form (53):

$$
\begin{aligned}
\alpha_2^{[P+Q]} &= -\alpha_2^{[P]} - \alpha_2^{[Q]} + 2\gamma_2 - \gamma_1^2 + \nu_1\gamma_1,\\
\alpha_4^{[P+Q]} &= -\alpha_4^{[P]} - \alpha_4^{[Q]} + \big(\alpha_2^{[P]}\big)^2 + \alpha_2^{[P]}\alpha_2^{[Q]} + \big(\alpha_2^{[Q]}\big)^2\\
&\quad - \big(\alpha_2^{[P]} + \alpha_2^{[Q]}\big)\big(2\gamma_2 - \gamma_1^2 + \nu_1\gamma_1\big)\\
&\quad + 2\gamma_4 + \gamma_2^2 + \big(\nu_1\gamma_2 - \nu_2\gamma_1 + \nu_3\big)\gamma_1.
\end{aligned}
\tag{29a'}
$$

Duplication law:

$$
\begin{aligned}
\alpha_2^{[2Q]} &= -2\alpha_2^{[Q]} + 2\gamma_2 - \gamma_1^2 + \nu_1\gamma_1,\\
\alpha_4^{[2Q]} &= -2\alpha_4^{[Q]} + 3(\alpha_2^{[Q]})^2 - 2\alpha_2^{[Q]}\big(2\gamma_2 - \gamma_1^2 + \nu_1\gamma_1\big)\\
&\quad + 2\gamma_4 + \gamma_2^2 + \big(\nu_1\gamma_2 - \nu_2\gamma_1 + \nu_3\big)\gamma_1,
\end{aligned}
\tag{36a'}
$$

References

[1] Baker, H. F., *Abel's theorem and the allied theory of theta functions*, Cambridge Univ. Press, Cambridge, 1897.

[2] Baker, H. F., *Multiply periodic functions*, Cambridge Univ. Press, Cambridge, 1907.

[3] Bernatska, J.; Leykin, D., On degenerate sigma-function in genus 2. *Glasgow Mathematical Journal*, **61**:1 (2019) 169–193.

[4] Bernatska J., Leykin D. Solution of the Jacobi inversion problem on non-hyperelliptic curves, Lett. Math. Phys. **113** 110 (2023).

[5] Bernatska, J., Computation of $\wp$-functions on plane algebraic curves, arXiv:2407.05632.

[6] Bernstein, D. J., Lange, T., Hyper-and-elliptic-curve cryptography. *LMS Journal of Computation and Mathematics*, **17**, Special Issue A: Algorithmic Number Theory Symposium XI, (2014) 181–202

[7] Bos, J. W., Costello, C, Hisil, H, Lauter, K, Fast Cryptography in Genus 2, In: Johansson, T., Nguyen, P.Q. (eds) *Advances in Cryptology. EUROCRYPT 2013. Lecture Notes in Computer Science*, **7881**:194–210, Springer, Berlin, Heidelberg, 2013

[8] Buchstaber, V. M., Leikin, D. V., Hyperelliptic Addition Law, *JNMP*, **12**:1 (2005), 106–123.

[9] Buchstaber, V. M., Enolskii, V. Z., Leykin, D. V., *Hyperelliptic Kleinian Functions and Applications*, preprint ESI 380, Vienna, 1996

[10] Buchstaber, V. M., Enolskii, V. Z., Leikin, D. V., *Multi-dimensional sigma-function*, 2012, arXiv 1208.0990

[11] Buchstaber, V. M., Enolskii, V. Z., Leikin, D. V., Rational analogs of abelian functions, *Functional Analysis and Its Applications*, **33**:2 (1999) 83–94.

[12] Buchstaber, V. M., Leikin, D. V., Solution of the problem of differentiation of Abelian functions over parameters for families of (n, s)-curves, *Functional Analysis and Its Applications*, **42**:4 (2008) 268–278.

[13] D. Cantor, Computing in the Jacobian of a Hyperelliptic curve, *Mathematics of Computation*, **48**:177 (1987), pp. 95–101.

[14] Cantor, D. G. On the analogue of the division polynomials for hyperelliptic curves. *J. reine angew. Math.* **447** (1994) 91–145.

[15] Cassels, J. W. S., Flynn, E. V., *Prolegomena to a middlebrow arithmetics of curves of genus* 2, CUP, Cambridge, 1996

[16] Costello, C., Lauter, K. Group Law Computations on Jacobians of Hyperelliptic Curves. In: Miri, A., Vaudenay, S. (eds) *Selected Areas in Cryptography. SAC 2011. Lecture Notes in Computer Science*, **7118**:92–117, Springer, Berlin, Heidelberg, 2012

[17] Kanayama, N., Division polynomials and multiplication formulae of Jacobian varieties of dimension 2. *Math. Proc. Camb. Philos. Soc.* **139** (2005) 399–409

[18] *Mathematical modelling for next-generation cryptography, CREST Crypto-Math Project. Mathematics for Industry*, **29**, Springer, Singapore, 2018

[19] Ônishi,Y.: Determinant expressions for hyperelliptic functions, *Proc. Edinb. Math. Soc.* **48** (2005) 705–742
[20] Uchida, Y., Division polynomials and canonical local heights on hyperelliptic Jacobians, *Manuscripta Math.*, **134** (2011) 273–308