Addition of Divisors on Hyperelliptic Curves via Interpolation Polynomials

Julia BERNATSKA † *and Yaacov KOPELIOVICH* ‡

† *National University of Kyiv-Mohyla Academy, 2 Skovorody Str., Kyiv, 04655, Ukraine*
E-mail: *jbernatska@gmail.com*

‡ *University of Connecticut, 2100 Hillside Rd, Storrs Mansfield, 06269, USA*
E-mail: *yaacov.kopeliovich@uconn.edu*

Received February 05, 2020, in final form May 29, 2020; Published online June 14, 2020
https://doi.org/10.3842/SIGMA.2020.053

Abstract. Two problems are addressed: reduction of an arbitrary degree non-special divisor to the equivalent divisor of the degree equal to genus of a curve, and addition of divisors of arbitrary degrees. The hyperelliptic case is considered as the simplest model. Explicit formulas defining reduced divisors for some particular cases are found. The reduced divisors are obtained in the form of solution of the Jacobi inversion problem which provides the way of computing Abelian functions on arbitrary non-special divisors. An effective reduction algorithm is proposed, which has the advantage that it involves only arithmetic operations on polynomials. The proposed addition algorithm contains more details comparing with the known in cryptography, and is extended to divisors of arbitrary degrees comparing with the known in the theory of hyperelliptic functions.

Key words: reduced divisor; inverse divisor; non-special divisor; generalised Jacobi inversion problem

2020 Mathematics Subject Classification: 32Q30; 14G50

1 Introduction

In the paper we propose a method of adding arbitrary divisors on a hyperelliptic curve. We often refer to a non-special divisor, which we define by means of Riemann theorem, more accurate definition is given below in Section 2.3. However, the method covers addition of special divisors as well.

Before stating the goal we introduce the notion of *reduced divisor* corresponding to any non-special divisor on an algebraic curve. Suppose g is genus of the curve. Any non-special divisor can be represented by a collection of points of number greater than or equal to the genus, that is $D=\sum\limits_{k=1}^{g+m}P_k$, $m\geqslant 0$. A *reduced divisor* is a non-special divisor composed of g points: $\widetilde{D}=\sum\limits_{k=1}^{g}P_k$.

It follows from the Riemann–Roch theorem that every non-special divisor of the form $D-(\deg D)\infty$ is equivalent to $\widetilde{D}-g\infty$, where $\widetilde{D}$ is a reduced divisor. This immediately leads to the following

Reduction Problem. Given a non-special divisor D of degree $g+m$, $m>0$, on an algebraic curve of genus g find the corresponding reduced divisor $\widetilde{D}$ such that $D-(g+m)\infty$ is equivalent to $\widetilde{D}-g\infty$.

Addition of two special divisors can be considered as a reduction problem, if the sum forms a non-special divisor. Non-special divisors are used in the problem statement to avoid ambiguity.

The reduction problem has a close relation to

Addition Problem. Given two non-special divisors D_1 and D_2 of degrees $g+m_1$ and $g+m_2$, $m_1, m_2 \geqslant 0$ respectively find a reduced divisor $\widetilde{D}$ such that $D_1+D_2-(2g+m_1+m_2)\infty \sim \widetilde{D}-g\infty$.

Note that solving the reduction problem we immediately solve the addition problem since we can assume that D_1, D_2 together compose a non-special divisor D of degree $2g+m_1+m_2$, and then come to the reduction problem for the new divisor D. On the other hand, the standard addition problem arises when the both divisors D_1, D_2 are firstly reduced to divisors $\widetilde{D}_1$, $\widetilde{D}_2$ of degree g each, then addition of $\widetilde{D}_1$, $\widetilde{D}_2$ can be accomplished by any approach to addition law.

Much work has been done on the reduction problem starting with the classical work [1], where the Jacobi inversion problem was solved in hyperelliptic case [1, p. 32, Section 216] (briefly recalled in preliminaries). The Jacobi inversion problem is stated for a non-special divisor of degree g, that is for a reduced divisor. Points of the divisor serve as roots of two rational functions defined on a curve. Coefficients of the rational functions are expressed through multiply periodic functions $\wp$ evaluated at a point of Jacobian of the curve, and this point corresponds to the divisor. So a solution of the reduction problem coincides by the form with a solution of the Jacobi inversion problem, which provides a method of solving the generalised Jacobi inversion problem stated for divisor of degree greater than g.

The first solution of reduction problem was given in [4]. This algorithm was inspired by reduction of quadratic forms. For low genera ($g = 2, 3$) many authors worked on giving more explicit solutions to the reduction problem due to potential application in cryptography, see [6] and [9] and the literature cited there. The explicit realisation of addition law should also have applications to the theory of heights on hyperelliptic Jacobians. In [10] $\wp$ functions are used to produce formulas for division polynomials on hyperelliptic curves of low genera which was later applied in [5] to compute canonical heights on genus 2 curves. Though the question of division polynomials isn't treated explicitly in the present paper it is strongly related to the reduction algorithm we propose as it is essentially equivalent to reduced divisors of the form nP on the curve.

In preliminaries the Jacobi inversion problem is recalled and a detailed description of non-special and special divisors is given. The reduction problem is addressed in Sections 3 and 4. The proposed method of reduction is based on the ideas of [3] and [7]. A new and essential result achieved here consists in finding explicit functions defining reduced divisors in some particular cases, which are presented in Section 3. An iterative reduction algorithm is given in Section 4, as well as some comments on its application in cryptography. Section 5 is devoted to the addition problem.

In our setup we often suppose that points of divisors are known, and we use them to construct polynomials and functions defining the divisors. This approach guarantees that a divisor arising from the definition through polynomials is located on the curve. On the other hand, the reader can forget that the polynomial coefficients were computed from points, and use symbolic notations for them. All operations are applicable to polynomials in this form as well.

In this paper we tie together two directions where addition of divisors was investigated: hyperelliptic cryptography, and theory of Abelian functions on hyperelliptic curves. The viewpoint of cryptographic applications describes divisors in terms of polynomials in quite an abstract manner, when the structure of divisors is left out of consideration. Analysis of divisors by means of meromorphic functions on hyperelliptic curves helps a lot in understanding a relation between the structure of a divisor and the form of functions which define it. On the other hand, the addition law known in the theory of Abelian functions on hyperelliptic curves is established for two non-special divisors of degree g, which seems to be enough. In the present paper we extend the addition law to non-special divisors of arbitrary degree. Though we restrict our consideration to non-special divisors and use reduction to divisors of degree g, we provide some new results in computation of Abelian functions on arbitrary non-special divisors, which arise from addition of divisors.

2 Preliminaries

2.1 Hyperelliptic curve and Sato weights

In the paper we deal with the family of hyperelliptic curves with a branch point at infinity. A genus g curve is defined by the equation

$$0 = f(x,y) = -y^2 + \mathcal{P}(x) = -y^2 + \lambda_0 x^{2g+1} + \sum_{n=0}^{2g} \lambda_{4g+2-2n} x^n, \tag{2.1}$$

where λ_k are parameters of the curve, $\lambda_0 = 1$, and $x, y \in \mathbb{C}$. We use Sato weights as indices, since they are respected by the theory of rational functions, that simplifies many considerations. Sato weight equals the opposite to the exponent of the leading term in the expansion near infinity. Namely,

$$x = \xi^{-2}, \qquad y = \xi^{-2g-1}(1 + O(\lambda)), \tag{2.2}$$

where ξ is a local parameter, and Sato weights of x and y are $\operatorname{wgt} x = 2$, $\operatorname{wgt} y = 2g+1$. The weight is also assigned to every function, for example f has weight $4g+2$.

2.2 Jacobi inversion problem

The Jacobi inversion problem gives the answer how to find g points $\{(x_k, y_k)\}_{k=1}^g$ on a curve which unambiguously map into a point u of Jacobian Jac of the curve. Solution of the Jacobi inversion problem for a hyperelliptic curve is given by two rational functions

$$\mathcal{R}_{2g}(x;u) = x^g - \sum_{k=1}^{g} x^{g-k} \wp_{1,2k-1}(u), \tag{2.3a}$$

$$\mathcal{R}_{2g+1}(x,y;u) = 2y + \sum_{k=1}^{g} x^{g-k} \wp_{1,1,2k-1}(u). \tag{2.3b}$$

Here multiply periodic $\wp$ functions as in [1] are defined by

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

through g-variable σ function which can be constructed by the method given in [2]. More details about rational functions can be found in [3].

Components of $u \in \mathrm{Jac}$ are indexed by Sato weights: $u = (u_1, u_3, \ldots, u_{2g-1})$, $\operatorname{wgt} u_n = -n$, and the standard holomorphic differentials are employed

$$\mathrm{d}u_{2k-1} = \frac{x^{g-k}\mathrm{d}x}{-2y}, \qquad k = 1, \ldots, g.$$

The function $\mathcal{R}_{2g}$ is a polynomial in x and has g roots $\{x_k\}_{k=1}^g$. At the same time, $\mathcal{R}_{2g}$ is rational on the curve (2.1) with $2g$ roots, namely, $\{(x_k, y_k), (x_k, -y_k)\}_{k=1}^g$, where $\{y_k\}_{k=1}^g$ are defined by the function $\mathcal{R}_{2g+1}$. That is divisor $D_g = \{(x_k, y_k)\}_{k=1}^g$ solves uniquely the following system

$$\mathcal{R}_{2g}(x;u) = 0, \qquad \mathcal{R}_{2g+1}(x,y;u) = 0,$$

and serves as the preimage of u

$$\mathrm{Jac} \ni u = \sum_{k=1}^{g} \mathcal{A}(x_k, y_k)$$

under Abel's map

$$\mathcal{A}(x, y) = \int_{\infty}^{(x,y)} \mathrm{d}u,$$

where $\mathrm{d}u = (\mathrm{d}u_1, \mathrm{d}u_3, \ldots, \mathrm{d}u_{2g-1})^{\mathrm{t}}$. As usual, $\mathcal{A}(D_g) = \sum\limits_{k=1}^{g} \mathcal{A}(x_k, y_k)$.

Note that $\mathcal{R}_{2g+1}$ has $2g+1$ roots on the curve, but only g are common of two functions $\mathcal{R}_{2g}$ and $\mathcal{R}_{2g+1}$. Points $\{(x_k, -y_k)\}_{k=1}^{g}$ form a divisor which is inverse to $\{(x_k, y_k)\}_{k=1}^{g}$, and satisfy $\mathcal{R}_{2g+1}(x, -y; u) = 0$.

On the other hand, $\mathcal{R}_{2g}$ and $\mathcal{R}_{2g+1}$ can be obtained by determinant formulas

$$\mathcal{R}_{2g}(x, y; u) = x^g + \sum_{k=1}^{g} \alpha_{2g+2-2k} x^{k-1},$$

$$\frac{1}{2}\mathcal{R}_{2g+1}(x, y; u) = y + \sum_{k=1}^{g} \beta_{2g+3-2k} x^{k-1},$$

similar to (3.2), and coefficients α_n and β_n are expressed in terms of coordinates of points $\{(x_k, y_k)\}_{k=1}^{g}$.

2.3 Non-special divisors

First, we recall the Riemann theorem, which is used here to define a non-special divisor. Let ω and ω' be matrices of periods along the standard homology $\mathfrak{a}$- and $\mathfrak{b}$-cycles, namely,

$$\omega_{2k-1,j} = \oint_{\mathfrak{a}_j} \mathrm{d}u_{2k-1}, \qquad \omega'_{2k-1,j} = \oint_{\mathfrak{b}_j} \mathrm{d}u_{2k-1},$$

where $k, j = 1, \ldots, g$, and $\mathrm{d}u_{2k-1}$ are holomorphic differentials introduced above. In this notation $\theta\big(\omega^{-1}u; \omega^{-1}\omega'\big)$ is the Riemann theta function on Jacobian of a curve defined by (2.1). K denotes the vector of Riemann constants. Then

$$\theta\big(\mathcal{A}(P) - \mathcal{A}(D) - K\big)$$

as a function of a point P vanishes if D is a *special divisor*, and has g roots if D is a *non-special divisor*.

The same statement holds with multivariable σ-function, namely,

$$\sigma\big(\mathcal{A}(P) - \mathcal{A}(D)\big)$$

as a function of P vanishes if D is a *special divisor*, and has g roots if D is a *non-special divisor*. Let $D_g = \sum\limits_{k=1}^{g} (x_k, y_k)$ and all points of D_g are parameterised as in (2.2) with parameters ξ_k. As shown in [3, Theorem 2.7 in Russian version]

$$\sigma\big(\mathcal{A}(D_g) - \mathcal{A}(x(\xi), y(\xi))\big) = \left(\prod_{k=1}^{g}(\xi - \xi_k) \prod_{\substack{i,j=1 \\ j>i}}^{g} (\xi_i + \xi_j)\right) \exp\big(H(-\xi, \xi_1, \ldots, \xi_g; \lambda)\big), \quad (2.4)$$

where $H(0; \lambda) = H(-\xi, \xi_1, \ldots, \xi_g; 0) = 0$.

From (2.4) it is evident that a non-special divisor D_g contains no pair of points related by the hyperelliptic involution: $\xi_i = -\xi_j$. This is applicable to a degree g divisor. If a divisor D_{g+m} of degree $g+m$ contains a pair in the hyperelliptic involution, we delete this pair from the divisor, and do the same with all pairs in involution, so obtain a truncated divisor $\widehat{D}_{g+m}$ equivalent to D_{g+m}. The divisor D_{g+m} is *non-special* if its truncated version $\widehat{D}_{g+m}$ has a degree equal to or greater than g. In what follows divisors containing points in involution are not considered.

In a divisor D_{g-n} of degree less than g, say $g-n$ with $0 < n < g$, the absent n points are assigned to infinity, that is the corresponding parameters ξ_k vanish. Putting (x, y) to infinity, that is $\xi = 0$, one computes $\sigma\big(\mathcal{A}(D_{g-n})\big)$, and see that sigma function vanishes on a divisor of degree less than g, and so $\wp$ functions are not defined on such a divisor. In this case non-vanishing derivatives of sigma function are used instead of $\wp$ functions. Formula (2.4) is also applicable to a divisor of degree greater than g, when the divisor is replaced by the equivalent reduced divisor.

2.4 Special divisors

In what follows special divisors are always considered as containing less than g points of a curve.

Proposition 2.1. *A divisor D_m of degree m, $m < g$, is defined uniquely by the system*

$$\mathcal{H}(x) = 0, \qquad y = \mathcal{I}(x) \tag{2.5}$$

with polynomials $\mathcal{H}$ of degree m and $\mathcal{I}$ of degree $m-1$ or greater, the both vanishing on D_m.

The proof is evident if the points are given. For example one can use determinant formulas to construct such polynomials, at that $\mathcal{I}$ has degree $m-1$.

Now consider the system (2.5) in detail. Equation $\mathcal{H}(x) = 0$ defines $2m$ points of the curve, namely $\{(x_k, y_k), (x_k, -y_k)\}_{k=1}^{m}$ such that x_k are roots of $\mathcal{H}$. Coordinates y_k can be found from the equation of the curve (2.1), but only m points are contained in D_m. These points are singled out by the second equation of the system (2.5). It represents a rational function of weight $2g+1$, equal to $\operatorname{wgt} y$, if $\deg \mathcal{I} \leqslant g$, and so has $2g+1$ roots on the curve, m of which are common with $\mathcal{H}$. Polynomial $\mathcal{I}$ of degree greater than g is also eligible.

Obviously, a divisor with points in involution can not be covered by the definition (2.5) since the equation for y is linear and defines only one value of y for each x.

The reduction problem is not applicable to special divisors, which are in the most reduced form. However one can consider the addition problem for two or more special divisors, and the addition algorithm given in Section 5 is applicable to such divisors as well.

3 Addition on a curve

3.1 Reduction of $g+1$ degree divisor

Theorem 3.1. *Let $\widetilde{D}$ be a divisor of degree g such that $\widetilde{D} - g\infty$ is equivalent to $D_{g+1} - (g+1)\infty$, where $D_{g+1} = \sum_{k=1}^{g+1} P_k$ is a non-special divisor, and $\{P_k = (x_k, y_k)\}_{k=1}^{g+1}$ are distinct points. Then $\widetilde{D}$ is defined by the system*

$$\mathcal{H}(x) = 0, \qquad y = -\mathcal{I}(x), \tag{3.1a}$$

where

$$\mathcal{H}(x) = -\frac{1}{2} \sum_{\substack{k,l=1 \\ l \neq k}}^{g+1} \frac{(y_k - y_l)^2}{(x_k - x_l)^2} \prod_{\substack{i=1 \\ i \neq k,l}}^{g+1} \frac{(x - x_i)}{(x_l - x_i)(x_k - x_i)} + \sum_{n=0}^{g} x^n \sum_{j=0}^{g-n} \lambda_{2g-2n-2j} h_j, \tag{3.1b}$$

$$\mathcal{I}(x)=\sum_{k=1}^{g+1} y_k \frac{\prod\limits_{i=1,i\neq k}^{g+1}(x-x_i)-\mathcal{H}(x)}{\prod\limits_{i=1,i\neq k}^{g+1}(x_k-x_i)}, \tag{3.1c}$$

and h_n denotes the complete symmetric polynomial of degree n in $\{x_k\}_{k=1}^{g+1}$.

Proof. Define a rational function $\mathcal{R}_{2g+1}$ with $g+1$ fixed roots at points $\{P_k=(x_k,y_k)\}_{k=1}^{g+1}$ by the determinant formula

$$\begin{vmatrix} 1 & x & x^2 & \cdots & x^g & y \\ 1 & x_1 & x_1^2 & \cdots & x_1^g & y_1 \\ 1 & x_2 & x_2^2 & \cdots & x_2^g & y_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & x_{g+1} & x_{g+1}^2 & \cdots & x_{g+1}^g & y_{g+1} \end{vmatrix} = 0, \tag{3.2}$$

which can be written in a different form

$$y=\mathcal{G}(x) \tag{3.3}$$

with the help of interpolation polynomial $\mathcal{G}$ of degree g

$$\mathcal{G}(x)=\sum_{k=1}^{g+1} y_k L_k(x), \tag{3.4}$$

where L_k have the form of Lagrange interpolating polynomials, namely

$$L_k(x)=\prod_{i=1,i\neq k}^{g+1}\frac{(x-x_i)}{(x_k-x_i)}. \tag{3.5}$$

Note that

$$\sum_{k=1}^{g+1} L_k(x)=1.$$

Intersection of (3.3) with the curve produces the unknown g roots of $\mathcal{R}_{2g+1}$. So, substitute (3.4) for y into (2.1), and take into account that $L_k(x)L_j(x)$ with $k\neq j$ is divisible by $\mathcal{F}(x)=\prod\limits_{n=1}^{g+1}(x-x_n)$

$$\begin{aligned} -\mathcal{G}(x)^2+\mathcal{P}(x) &= -\left(\sum_{k=1}^{g+1} y_k L_k(x)\right)^2+\mathcal{P}(x)\left(\sum_{k=1}^{g+1} L_k(x)\right)^2 \\ &= \sum_{k,j=1,\,k\neq j}^{g+1}\big(\mathcal{P}(x)-y_k y_j\big)L_k(x)L_j(x)+\sum_{k=1}^{g+1}\big(\mathcal{P}(x)-\mathcal{P}(x_k)\big)L_k(x)^2 \\ &= \sum_{k,j=1,\,k\neq j}^{g+1}\big(\mathcal{P}(x_k)-y_k y_j\big)L_k(x)L_j(x)+\sum_{k=1}^{g+1}\big(\mathcal{P}(x)-\mathcal{P}(x_k)\big)L_k(x) \\ &= \mathcal{F}(x)\left(\sum_{k,j=1,\,k\neq j}^{g+1}\frac{y_k^2-y_k y_j}{\prod\limits_{i=1,i\neq k}^{g+1}(x_k-x_i)\prod\limits_{i=1,i\neq j}^{g+1}(x_j-x_i)}\prod_{\substack{i=1\\ i\neq k,j}}^{g+1}(x-x_i)\right. \end{aligned}$$

$$+\sum_{k=1}^{g+1}\frac{1}{\prod\limits_{i=1,i\neq k}^{g+1}(x_k-x_i)}\frac{\mathcal{P}(x)-\mathcal{P}(x_k)}{x-x_k}\Bigg),$$

with an arbitrary natural N it is straightforward to check

$$\sum_{k=1}^{N}\frac{x_k^n}{\prod\limits_{j=1,j\neq k}^{N}(x_k-x_j)}=h_{n-N+1}, \tag{3.6}$$

where h_n is the complete symmetric polynomial of degree n in $\{x_k\}_{k=1}^N$, and $h_n=0$ as $n<0$. Then one finds

$$\mathcal{Q}(x)=\sum_{k=1}^{g+1}\frac{1}{\prod\limits_{\substack{i=1\\i\neq k}}^{g+1}(x_k-x_i)}\frac{\mathcal{P}(x)-\mathcal{P}(x_k)}{x-x_k}=\sum_{n=0}^{g}x^n\sum_{j=0}^{g-n}\lambda_{2g-2n-2j}h_j.$$

Finally,

$$\mathcal{H}(x)=-\frac{1}{2}\sum_{\substack{k,l=1\\l\neq k}}^{g+1}\frac{(y_k-y_l)^2}{(x_k-x_l)^2}\prod_{\substack{i=1\\i\neq k,l}}^{g+1}\frac{(x-x_i)}{(x_l-x_i)(x_k-x_i)}+\mathcal{Q}(x).$$

Note that coefficient at x^g is $\mathfrak{h}_0=\lambda_0=1$, which arises from $\mathcal{Q}$.

Polynomial $\mathcal{H}$ has g roots, say $\{\tilde{x}_k\}_{k=1}^g$, and points $\big\{\big(\tilde{x}_k,\tilde{y}_k=\mathcal{G}(\tilde{x}_k)\big)\big\}_{k=1}^g$ give the unknown g roots of $\mathcal{R}_{2g+1}$ defined by (3.2). Let $\mathfrak{g}_0$ be the coefficient of $\mathcal{G}$ at x^g, then

$$\mathcal{I}(x)=\mathcal{G}(x)-\frac{\mathfrak{g}_0}{\mathfrak{h}_0}\mathcal{H}(x)=\sum_{k=1}^{g+1}y_k\frac{\prod\limits_{i=1,i\neq k}^{g+1}(x-x_i)-\mathcal{H}(x)}{\prod\limits_{i=1,i\neq k}^{g+1}(x_k-x_i)}.$$

Polynomial $\mathcal{I}$ has degree $g-1$, and $y-\mathcal{I}(x)$ vanishes at the same g points as $\mathcal{H}(x)$. These points $\big\{\big(\tilde{x}_k,\tilde{y}_k\big)\big\}_{k=1}^g$ map into $-u\in\mathrm{Jac}$, which is inverse to the Abel image u of the reduced divisor $\widetilde{D}=\sum\limits_{k=1}^{g}\widetilde{P}_k$. Therefore, the reduced divisor $\widetilde{D}$ corresponding to D_{g+1} consists of points $\big\{\widetilde{P}_k=\big(\tilde{x}_k,-\tilde{y}_k\big)\big\}$. ■

Remark 3.2. System (3.1) coincides with the solution of Jacobi inversion problem given by the rational functions (2.3), namely

$$\mathcal{R}_{2g}(x;u)=\mathcal{H}(x),\qquad \mathcal{R}_{2g+1}(x,y;u)=2y+2\mathcal{I}(x).$$

Therefore, polynomials $\mathcal{H}$ and $\mathcal{I}$ allow to compute $\wp$ functions at divisor D_{g+1}.

3.2 Reduction of $g+2$ degree divisor

Theorem 3.3. *Let $\widetilde{D}$ be a divisor of degree g such that $\widetilde{D}-g\infty$ is equivalent to $D_{g+2}-(g+2)\infty$, where $D_{g+2}=\sum\limits_{k=1}^{g+2}P_k$ is a non-special divisor, and $\{P_k=(x_k,y_k)\}_{k=1}^{g+2}$ are distinct points. Then $\widetilde{D}$ is defined by the system*

$$\mathcal{H}(x)=0,\qquad y=-\mathcal{I}(x), \tag{3.7a}$$

where

$$\mathcal{H}(x)=-\frac{1}{2}\sum_{\substack{k,l=1\\ l\neq k}}^{g+2}\frac{(y_k-y_l)^2}{(x_k-x_l)^2}\prod_{\substack{i=1\\ i\neq k,l}}^{g+2}\frac{(x-x_i)}{(x_l-x_i)(x_k-x_i)}+\sum_{n=0}^{g-1}x^n\sum_{j=0}^{g-1-n}\lambda_{2g-2-2n-2j}h_j, \tag{3.7b}$$

$$\begin{aligned}\mathcal{I}(x)=\frac{1}{\mathfrak{h}_0}\Bigg(&\mathfrak{g}_0\Bigg(\frac{1}{\mathfrak{h}_0}\mathcal{H}(x)-x\sum_{n=0}^{g-1}x^n\sum_{j=0}^{g-1-n}\lambda_{2g-2-2n-2j}h_j\Bigg)\\&+\frac{1}{2}\sum_{\substack{k,l=1\\ l\neq k}}^{g+2}\sum_{\substack{n=1\\ n\neq k,l}}^{g+2}\frac{y_n(y_k-y_l)^2}{\prod\limits_{\substack{j=1\\ j\neq n}}^{g+2}(x_n-x_j)\prod\limits_{\substack{i=1\\ i\neq l}}^{g+2}(x_l-x_i)\prod\limits_{\substack{i=1\\ i\neq k}}^{g+2}(x_k-x_i)}\\&\times\Bigg((x_n-x_k-x_l)\Bigg(x\prod_{\substack{j=1\\ j\neq n,k,l}}^{g+2}(x-x_j)-\frac{1}{\mathfrak{h}_0}\mathcal{H}(x)\Bigg)+x_kx_l\prod_{\substack{j=1\\ j\neq n,k,l}}^{g+2}(x-x_j)\Bigg)\\&-\sum_{\substack{k,l=1\\ l\neq k}}^{g+2}\frac{(y_k-y_l)^2x_ly_k}{\prod\limits_{\substack{i=1\\ i\neq l}}^{g+2}(x_l-x_i)\prod\limits_{\substack{i=1\\ i\neq k}}^{g+2}(x_k-x_i)^2}\Bigg(\prod_{\substack{j=1\\ j\neq k,l}}^{g+2}(x-x_j)-\frac{1}{\mathfrak{h}_0}\mathcal{H}(x)\Bigg)\Bigg),\end{aligned} \tag{3.7c}$$

where $\mathfrak{h}_0$ *and* $\mathfrak{g}_0$ *are defined by* (3.10a) *and* (3.11a)*, and* h_n *denotes the complete symmetric polynomial of degree* n *in* $\{x_k\}_{k=1}^{g+2}$.

Proof. Define a rational function $\mathcal{R}_{2g+2}$ with $g+2$ fixed roots at points $\{P_k=(x_k,y_k)\}_{k=1}^{g+2}$ by

$$\begin{vmatrix}1 & x & x^2 & \cdots & x^g & y & x^{g+1}\\ 1 & x_1 & x_1^2 & \cdots & x_1^g & y_1 & x_1^{g+1}\\ 1 & x_2 & x_2^2 & \cdots & x_2^g & y_2 & x_2^{g+1}\\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots\\ 1 & x_{g+2} & x_{g+2}^2 & \cdots & x_{g+2}^g & y_{g+2} & x_{g+2}^{g+1}\end{vmatrix}=0. \tag{3.8}$$

Interpolation polynomial $\mathcal{G}$ such that (3.8) acquires the form $y=\mathcal{G}(x)$, is defined by

$$\mathcal{G}(x)=\sum_{k=1}^{g+2}y_kL_k(x), \tag{3.9}$$

where

$$L_k(x)=\prod_{i=1,i\neq k}^{g+2}\frac{(x-x_i)}{(x_k-x_i)}.$$

Intersection of $y=\mathcal{G}(x)$ with the curve produces the unknown g roots of $\mathcal{R}_{2g+2}$. Substitute (3.9) for y into (2.1) and divide by $\mathcal{F}(x)=\prod\limits_{n=1}^{g+2}(x-x_n)$. Computation similar to that given in Section 3.1 leads to

$$\mathcal{H}(x)=-\frac{1}{2}\sum_{\substack{k,l=1\\ l\neq k}}^{g+2}\frac{(y_k-y_l)^2}{(x_k-x_l)^2}\prod_{\substack{i=1\\ i\neq k,l}}^{g+2}\frac{(x-x_i)}{(x_l-x_i)(x_k-x_i)}+\sum_{n=0}^{g-1}x^n\sum_{j=0}^{g-1-n}\lambda_{2g-2-2n-2j}h_j.$$

In this case coefficient at x^g is

$$\mathfrak{h}_0 = -\frac{1}{2}\sum_{\substack{k,l=1\\ l\neq k}}^{g+2}\frac{(y_k-y_l)^2}{(x_k-x_l)^2}\frac{1}{\prod\limits_{\substack{i=1\\ i\neq k,l}}^{g+2}(x_l-x_i)(x_k-x_i)}, \tag{3.10a}$$

which does not vanish, and the coefficient at x^{g-1} is

$$\mathfrak{h}_1 = \lambda_0 + \frac{1}{2}\sum_{\substack{k,l=1\\ l\neq k}}^{g+2}\frac{(y_k-y_l)^2}{(x_k-x_l)^2}\frac{\sum\limits_{\substack{i=1\\ i\neq k,l}}^{g+2} x_i}{\prod\limits_{\substack{i=1\\ i\neq k,l}}^{g+2}(x_l-x_i)(x_k-x_i)}. \tag{3.10b}$$

Let $\{\tilde{x}_k\}_{k=1}^g$ be roots of polynomial $\mathcal{H}$, then $\{(\tilde{x}_k, \tilde{y}_k = \mathcal{G}(\tilde{x}_k))\}_{k=1}^g$ are the unknown g roots of $\mathcal{R}_{2g+2}$. In this case $\mathcal{G}$ is a polynomial of degree $g+1$, and with the help of polynomial $\mathcal{H}$ it is reduced to $\mathcal{I}$ of degree $g-1$, namely,

$$\mathcal{I}(x) = \mathcal{G}(x) - \left(\frac{\mathfrak{g}_0}{\mathfrak{h}_0}x - \frac{\mathfrak{g}_0\mathfrak{h}_1}{\mathfrak{h}_0^2} + \frac{\mathfrak{g}_1}{\mathfrak{h}_0}\right)\mathcal{H}(x),$$

where

$$\mathfrak{g}_0 = \sum_{n=1}^{g+2}\frac{y_n}{\prod\limits_{j=1,j\neq n}^{g+2}(x_n-x_j)}, \tag{3.11a}$$

$$\mathfrak{g}_1 = -\sum_{n=1}^{g+2}\frac{y_n\sum\limits_{j=1,j\neq n}^{g+2}x_j}{\prod\limits_{j=1,j\neq n}^{g+2}(x_n-x_j)}. \tag{3.11b}$$

The expression for $\mathcal{I}$ is simplified to (3.7c).

Finally, the reduced divisor $\widetilde{D}$ corresponding to D_{g+2} consists of points $\{\widetilde{P}_k = (\tilde{x}_k, -\tilde{y}_k)\}$. ■

Remark 3.4. Similarly to the case of $g+1$ points, system (3.7) coincides with the solution of Jacobi inversion problem (2.3), and coefficients of polynomials $\mathcal{H}$ and $\mathcal{I}$ provide values of $\wp$ functions at divisor D_{g+2}.

3.3 Reduction of $g+1$ degree divisor with duplication

Theorem 3.5. *Let $\widetilde{D}$ be a divisor of degree g such that $\widetilde{D}-g\infty$ is equivalent to $D_{g+1}-(g+1)\infty$, where $D_{g+1} = 2P_1 + \sum\limits_{k=2}^{g} P_k$ is a non-special divisor, and $\{P_k = (x_k, y_k)\}_{k=1}^g$ are distinct points. Then $\widetilde{D}$ is defined by the system*

$$\mathcal{H}(x) = 0, \qquad y = -\mathcal{I}(x), \tag{3.12a}$$

where

$$\mathcal{H}(x) = \sum_{n=0}^{g} x^n \sum_{j=0}^{g-n}\lambda_{2g-2n-2j}h_j\big|_{x_{g+1}\to x_1}$$

$$
\begin{aligned}
&- \frac{\mathcal{P}'(x_1)}{\prod\limits_{i=2}^{g}(x_1-x_i)^2}\left(\frac{\prod\limits_{i=2}^{g}(x-x_i)-\prod\limits_{i=2}^{g}(x_1-x_i)}{(x-x_1)}-\prod_{i=2}^{g}(x-x_i)\sum_{\iota=2}^{g}(x_1-x_\iota)^{-1}\right)\\
&- \frac{\mathcal{P}'(x_1)}{2y_1\prod\limits_{i=2}^{g}(x_1-x_i)}\left(\sum_{k=2}^{g}\frac{2y_k\prod\limits_{\substack{i=1\\ i\neq k}}^{g}(x-x_i)}{(x_k-x_1)\prod\limits_{\substack{i=1\\ i\neq k}}^{g}(x_k-x_i)}+\frac{\mathcal{P}'(x_1)}{2y_1}\frac{\prod\limits_{i=2}^{g}(x-x_i)}{\prod\limits_{i=2}^{g}(x_1-x_i)}\right)\\
&+\sum_{j=2}^{g}\frac{(y_1-y_j)^2\prod\limits_{\substack{i=2\\ i\neq j}}^{g}(x-x_i)}{(x_j-x_1)\prod\limits_{\substack{i=1\\ i\neq j}}^{g}(x_j-x_i)\prod\limits_{i=2}^{g}(x_1-x_i)}\left(1-(x-x_1)\sum_{\iota=2}^{g}(x_1-x_\iota)^{-1}\right)\\
&+\sum_{\substack{k,j=2\\ k\neq j}}^{g}\frac{(y_k^2-y_ky_j)(x-x_1)^2\prod\limits_{\substack{i=2\\ i\neq k,j}}^{g}(x-x_i)}{(x_k-x_1)(x_j-x_1)\prod\limits_{\substack{i=1\\ i\neq k}}^{g}(x_k-x_i)\prod\limits_{\substack{i=1\\ i\neq j}}^{g}(x_j-x_i)},
\end{aligned}
\tag{3.12b}
$$

$$
\begin{aligned}
\mathcal{I}(x)=&\frac{(x-x_1)\prod\limits_{i=2}^{g}(x-x_i)-\mathcal{H}(x)}{\prod\limits_{i=2}^{g}(x_1-x_i)}\left(\frac{\mathcal{P}'(x_1)}{2y_1}-y_1\sum_{\iota=2}^{g}(x_1-x_\iota)^{-1}\right)\\
&+y_1\prod_{i=2}^{g}\frac{x-x_i}{x_1-x_i}+\sum_{k=2}^{g}y_k\frac{(x-x_1)\prod\limits_{\substack{i=1\\ i\neq k}}^{g}(x-x_i)-\mathcal{H}(x)}{(x_k-x_1)\prod\limits_{\substack{i=1\\ i\neq k}}^{g}(x_k-x_i)},
\end{aligned}
\tag{3.12c}
$$

and h_n denotes the complete symmetric polynomial of degree n in $\{x_k\}_{k=1}^{g+1}$.

Proof. Define a rational function $\mathcal{R}_{2g+1}$ with $g+1$ fixed roots at points $2P_1+\sum\limits_{k=2}^{g}P_k$, $P_k=(x_k,y_k)$, by the determinant formula

$$
\begin{vmatrix}
1 & x & x^2 & \cdots & x^g & y\\
1 & x_1 & x_1^2 & \cdots & x_1^g & y_1\\
1 & x_2 & x_2^2 & \cdots & x_2^g & y_2\\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots\\
1 & x_g & x_g^2 & \cdots & x_g^g & y_g\\
0 & 1 & 2x_1 & \cdots & gx_1^{g-1} & y_1'
\end{vmatrix}=0,
\tag{3.13}
$$

where y_1' denotes $\mathrm{d}y_1/\mathrm{d}x_1$, at that $P_1=(x_1,y_1)$ is a point of the curve defined by (2.1). Rewrite (3.13) as $y=\mathcal{G}(x)$, and find the interpolation polynomial

$$
\mathcal{G}(x)=\sum_{k=1}^{g}y_k\widetilde{L}_k(x)+y_1'\widetilde{L}_{g+1}(x),
\tag{3.14}
$$

where

$$\widetilde{L}_1(x) = (x-x_1)^2 \frac{\mathrm{d}}{\mathrm{d}x_1}\left(\frac{1}{(x-x_1)\prod\limits_{i=2}^{g}(x_1-x_i)}\right)\prod_{i=2}^{g}(x-x_i),$$

$$\widetilde{L}_k(x) = \frac{(x-x_1)^2}{(x_k-x_1)^2}\prod_{i=2,i\neq k}^{g}\frac{x-x_i}{x_k-x_i}, \qquad 2\leqslant k\leqslant g,$$

$$\widetilde{L}_{g+1}(x) = (x-x_1)\prod_{i=2}^{g}\frac{x-x_i}{x_1-x_i}.$$

Polynomials $\widetilde{L}_k(x)$ relate to $L_k(x)$ defined by (3.5) as follows

$$\widetilde{L}_1(x) = \lim_{x_{g+1}\to x_1}\big(L_1(x)+L_{g+1}(x)\big),$$

$$\widetilde{L}_k(x) = \lim_{x_{g+1}\to x_1} L_k(x), \qquad 2\leqslant k\leqslant g,$$

$$\widetilde{L}_{g+1}(x) = \lim_{x_{g+1}\to x_1}\frac{-L_{g+1}(x)}{\mathrm{d}\log L_{g+1}(x)/\mathrm{d}x_{g+1}}.$$

Note that

$$\sum_{k=1}^{g}\widetilde{L}_k(x) = 1.$$

Solutions of $y=\mathcal{G}(x)$ which are on the curve define the unknown g roots of $\mathcal{R}_{2g+1}$. Substitute (3.14) for y into (2.1), and take into account that $\widetilde{L}_k(x)\widetilde{L}_j(x)$ with $k,j=1,\dots,g$, $k\neq j$, and $\widetilde{L}_k(x)\widetilde{L}_{g+1}(x)$ with $k=2,\dots,g$, and $\widetilde{L}_{g+1}(x)^2$ are divisible by $\mathcal{F}(x)=(x-x_1)^2\prod\limits_{n=2}^{g}(x-x_n)$. Actually,

$$\begin{aligned}
-\mathcal{G}(x)^2+\mathcal{P}(x) &= -\left(\sum_{k=1}^{g}y_k\widetilde{L}_k(x)+y_1'\widetilde{L}_{g+1}(x)\right)^2+\mathcal{P}(x)\left(\sum_{k=1}^{g}\widetilde{L}_k(x)\right)^2\\
&= \sum_{k=1}^{g}\big(\mathcal{P}(x)-\mathcal{P}(x_k)\big)\widetilde{L}_k(x)-(y_1')^2\widetilde{L}_{g+1}(x)^2-2\sum_{k=1}^{g}y_ky_1'\widetilde{L}_k(x)\widetilde{L}_{g+1}(x)\\
&\quad+\sum_{\substack{k,j=1\\k\neq j}}^{g}\big(\mathcal{P}(x_k)-y_ky_j\big)\widetilde{L}_k(x)\widetilde{L}_j(x)\\
&= \mathcal{F}(x)\left(\frac{\mathrm{d}}{\mathrm{d}x_1}\left(\frac{\mathcal{P}(x)-\mathcal{P}(x_1)}{x-x_1}\frac{1}{A(x_1)}\right)\right.\\
&\quad+\sum_{k=2}^{g}\frac{\mathcal{P}(x)-\mathcal{P}(x_k)}{(x-x_k)}\frac{1}{(x_k-x_1)\prod\limits_{\substack{i=1\\i\neq k}}^{g}(x_k-x_i)}\\
&\quad-\frac{\mathcal{P}'(x_1)}{A(x_1)^2}\left(\frac{A(x)-A(x_1)}{(x-x_1)}-A(x)\frac{\mathrm{d}}{\mathrm{d}x_1}\log A(x_1)\right)\\
&\quad\left.-\frac{\mathcal{P}'(x_1)}{2y_1A(x_1)}\left(\sum_{k=2}^{g}\frac{2y_k\prod\limits_{\substack{i=1\\i\neq k}}^{g}(x-x_i)}{(x_k-x_1)\prod\limits_{\substack{i=1\\i\neq k}}^{g}(x_k-x_i)}+\frac{\mathcal{P}'(x_1)}{2y_1}\frac{A(x)}{A(x_1)}\right)\right)
\end{aligned}$$

$$+\sum_{j=2}^{g}\frac{(y_1-y_j)^2\prod\limits_{\substack{i=2\\ i\neq j}}^{g}(x-x_i)}{(x_j-x_1)\prod\limits_{\substack{i=1\\ i\neq j}}^{g}(x_j-x_i)A(x_1)}\left(1-(x-x_1)\frac{\mathrm{d}}{\mathrm{d}x_1}\log A(x_1)\right)$$

$$+\sum_{\substack{k,j=2\\ k\neq j}}^{g}\frac{(y_k^2-y_ky_j)(x-x_1)^2\prod\limits_{\substack{i=2\\ i\neq k,j}}^{g}(x-x_i)}{(x_k-x_1)(x_j-x_1)\prod\limits_{\substack{i=1\\ i\neq k}}^{g}(x_k-x_i)\prod\limits_{\substack{i=1\\ i\neq j}}^{g}(x_j-x_i)}\Bigg),$$

where we denote $A(x)=\prod\limits_{i=2}^{g}(x-x_i)$, and use relation $2y_1y_1'=\mathcal{P}'(x_1)$. In the above computation we used the following relations

$$\widetilde{L}_1(x)=\frac{A(x)}{A(x_1)}\left(1-(x-x_1)\frac{\mathrm{d}}{\mathrm{d}x_1}\log A(x_1)\right),\qquad \widetilde{L}_{g+1}(x)=(x-x_1)\frac{A(x)}{A(x_1)}$$

to obtain

$$\big(\mathcal{P}(x)-\mathcal{P}(x_1)\big)\widetilde{L}_1(x)-2y_1y_1'\widetilde{L}_1(x)\widetilde{L}_{g+1}(x)=(x-x_1)^2A(x)$$
$$\times\left(\frac{\mathrm{d}}{\mathrm{d}x_1}\left(\frac{\mathcal{P}(x)-\mathcal{P}(x_1)}{x-x_1}\frac{1}{A(x_1)}\right)-\frac{\mathcal{P}'(x_1)}{A(x_1)^2}\left(\frac{A(x)-A(x_1)}{(x-x_1)}-A(x)\frac{\mathrm{d}}{\mathrm{d}x_1}\log A(x_1)\right)\right).$$

Taking the limit of (3.6) as $x_{g+1}\to x_1$ one finds

$$\frac{\mathrm{d}}{\mathrm{d}x_1}\left(\frac{x_1^n}{A(x_1)}\right)+\sum_{k=2}^{g}\frac{x_k^n}{(x_k-x_1)\prod\limits_{\substack{i=1\\ i\neq k}}^{n}(x_k-x_i)}=\lim_{x_{g+1}\to x_1}h_{n-g},$$

where h_n is the complete symmetric polynomial of degree n in $\{x_k\}_{k=1}^{g+1}$, and $h_{n-g}=0$ as $n<g$. Then

$$\frac{\mathrm{d}}{\mathrm{d}x_1}\left(\frac{\mathcal{P}(x)-\mathcal{P}(x_1)}{x-x_1}\frac{1}{\prod\limits_{i=2}^{g}(x_1-x_i)}\right)+\sum_{k=2}^{g}\frac{\mathcal{P}(x)-\mathcal{P}(x_k)}{(x-x_k)}\frac{1}{(x_k-x_1)^2\prod\limits_{i=2,i\neq k}^{g}(x_k-x_i)}$$
$$=\sum_{n=0}^{g}x^n\sum_{j=0}^{g-n}\lambda_{2g-2n-2j}h_j\big|_{x_{g+1}\to x_1}.\tag{3.15}$$

Taking into account that

$$\frac{\mathrm{d}}{\mathrm{d}x_1}\log A(x_1)=\sum_{i=2}^{g}\frac{1}{x_1-x_i},$$

one obtains polynomial $\mathcal{H}$ as in (3.12b). Note that coefficient at x^g is $\mathfrak{h}_0=\lambda_0=1$, which arises from (3.15).

Let $\{\tilde{x}_k\}_{k=1}^{g}$ be roots of polynomial $\mathcal{H}$, then points $\big\{\big(\tilde{x}_k,\tilde{y}_k=\mathcal{G}(\tilde{x}_k)\big)\big\}_{k=1}^{g}$, where $\mathcal{G}$ is defined by (3.14), are the unknown g roots of $\mathcal{R}_{2g+1}$ which is defined by (3.13). Let $\mathfrak{g}_0$ be the coefficient of $\mathcal{G}$ at x^g, namely,

$$\mathfrak{g}_0=\frac{1}{A(x_1)}\left(y_1'-y_1\sum_{\iota=2}^{g}(x_1-x_\iota)^{-1}\right)+\sum_{k=2}^{g}\frac{y_k}{(x_k-x_1)\prod\limits_{\substack{i=1\\ i\neq k}}^{g}(x_k-x_i)},$$

then polynomial

$$\mathcal{I}(x) = \mathcal{G}(x) - \frac{\mathfrak{g}_0}{\mathfrak{h}_0}\mathcal{H}(x)$$

is of degree $g-1$. Then $y = \mathcal{I}(x)$ and $\mathcal{H}(x) = 0$ define points $\{(\tilde{x}_k, \tilde{y}_k)\}_{k=1}^{g}$ which map into $-u \in \mathrm{Jac}$, the inverse to the Abel image u of reduced divisor $\widetilde{D}$. Therefore, the reduced divisor $\widetilde{D}$ corresponding to $2P_1 + \sum\limits_{k=2}^{g} P_k$ consists of points $\{\widetilde{P}_k = (\tilde{x}_k, -\tilde{y}_k)\}$. ■

3.4 Reduction of divisor $(g+1)P$

Theorem 3.6. *Let $\widetilde{D}$ be a divisor of degree g such that $\widetilde{D} - g\infty$ is equivalent to $D_{g+1} - (g+1)\infty$, where $D_{g+1} = (g+1)P_1$ with non-branch point $P_1 = (x_1, y_1)$. Then $\widetilde{D}$ is defined by the system*

$$\mathcal{H}(x) = 0, \qquad y = -\mathcal{I}(x), \tag{3.16a}$$

where

$$\mathcal{H}(x) = (x-x_1)^g + 2\sum_{j=0}^{g-1}(x-x_1)^j \sum_{i=0}^{j} \frac{y_1^{(i)} y_1^{(j+g+1-i)}}{i!(j+g+1-i)!}, \tag{3.16b}$$

$$\mathcal{I}(x) = \sum_{n=0}^{g-1}(x-x_1)^n \left(\frac{y_1^{(n)}}{n!} - 2\frac{y_1^{(g)}}{g!} \sum_{i=0}^{n} \frac{y_1^{(i)} y_1^{(n+g+1-i)}}{i!(n+g+1-i)!} \right), \tag{3.16c}$$

and $y_1^{(n)}$ is found from

$$\mathcal{P}^{(n)}(x_1) = \sum_{k=0}^{n} \frac{n!}{k!(n-k)!} y_1^{(k)} y_1^{(n-k)}.$$

Proof. Define a rational function $\mathcal{R}_{2g+1}$ with $g+1$ fixed roots at points $(g+1)P_1$ with $P_1 = (x_1, y_1)$, by the determinant formula

$$\begin{vmatrix} 1 & x & x^2 & \cdots & x^g & y \\ 1 & x_1 & x_1^2 & \cdots & x_1^g & y_1 \\ 0 & 1 & 2x_1 & \cdots & g x_1^{g-1} & y_1' \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & g! x_1 & y_1^{(g-1)} \\ 0 & 0 & 0 & \cdots & g! & y_1^{(g)} \end{vmatrix} = 0, \tag{3.17}$$

where $y_1^{(n)}$ denotes $\mathrm{d}^n y_1 / \mathrm{d}x_1^n$. Then the interpolation polynomial $\mathcal{G}$ such that (3.17) acquires the form $y = \mathcal{G}(x)$ is defined by

$$\mathcal{G}(x) = \sum_{n=0}^{g} \frac{1}{n!}(x-x_1)^n y_1^{(n)}. \tag{3.18}$$

Points (x, y) of the curve (2.1) satisfying $y = \mathcal{G}(x)$ are roots of $\mathcal{R}_{2g+1}$. To find them substitute (3.18) for y into (2.1), and take into account that

$$\mathcal{G}(x)^2 = \sum_{k=0}^{2g} \frac{1}{k!}(x-x_1)^k \frac{\mathrm{d}^k y_1^2}{\mathrm{d}x_1^k} - 2\sum_{k=g+1}^{2g} \sum_{i=0}^{k-g-1} \frac{(x-x_1)^k}{i!(k-i)!} y_1^{(i)} y_1^{(k-i)},$$

and $y_1^2 = \mathcal{P}(x_1)$. Evidently,

$$-\mathcal{G}(x)^2 + \mathcal{P}(x) = (x-x_1)^{2g+1} + 2\sum_{k=g+1}^{2g}\sum_{i=0}^{k-g-1}\frac{(x-x_1)^k}{i!(k-i)!}y_1^{(i)}y_1^{(k-i)}$$
$$= (x-x_1)^{g+1}\left((x-x_1)^g + 2\sum_{k=g+1}^{2g}\sum_{i=0}^{k-g-1}\frac{(x-x_1)^{k-g-1}}{i!(k-i)!}y_1^{(i)}y_1^{(k-i)}\right)$$

is divisible by $\mathcal{F}(x) = (x-x_1)^{g+1}$. Therefore, $\mathcal{H}$ is defined by (3.16b), and coefficient at x^g is 1. Then

$$\mathcal{I}(x) = \mathcal{G}(x) - \frac{y_1^{(g)}}{g!}\mathcal{H}(x),$$

and one comes to (3.16c). ■

3.5 Reduction of $g+m$ degree divisor

Here we propose a solution of the reduction problem for a divisor of degree greater than $g+2$. Let a divisor $D_{g+m} = \sum_{k=1}^{g+m}(x_k, y_k)$ be defined by a system

$$\mathcal{F}(x) = 0, \qquad \mathcal{R}(x,y) = 0, \tag{3.19}$$

where $\mathcal{F}$ is a polynomial of degree $g+m$, and a rational function $\mathcal{R}$ of weight $2g+m$ has the form

$$\mathcal{R}(x,y) = y\gamma_y(x) + \gamma_x(x), \qquad \deg\gamma_y = [(m-1)/2], \qquad \deg\gamma_x = g + [m/2], \tag{3.20}$$

where $[\cdot]$ denotes the integer part. If points of D_{g+m} are known, $\mathcal{R}$ can be represented through a determinant similar to (3.8) constructed from the first $g+m+1$ elements in the list of monomials

$$\{1, x, \dots, x^g, y, x^{g+1}, yx, \dots, x^{g+[m/2]}, yx^{[m/2]}, \dots\}.$$

Let $\mathfrak{k} = [(m-1)/2]$, then

$$\gamma_y(x) = \sum_{l_{\mathfrak{k}}>\dots>l_1=1}^{g+m}\left(\prod_{\iota=1}^{\mathfrak{k}} y_{l_\iota}\right)M_{l_1,\dots,l_{\mathfrak{k}}}(x),$$
$$\gamma_x(x) = \sum_{l_{\mathfrak{k}+1}>\dots>l_1=1}^{g+m}(-1)^{\mathfrak{k}+1}\left(\prod_{\iota=1}^{\mathfrak{k}+1} y_{l_\iota}\right)N_{l_1,\dots,l_{\mathfrak{k}+1}}(x),$$

where $M_{l_1,\dots,l_{\mathfrak{k}}}$ and $N_{l_1,\dots,l_{\mathfrak{k}+1}}$ with repeated indices vanish, and

$$M_{l_1,\dots,l_{\mathfrak{k}}}(x) = \frac{1}{\mathfrak{k}!}\prod_{\iota=1}^{\mathfrak{k}}\frac{(x-x_{l_\iota})}{\prod\limits_{\substack{i=1,\\ i\neq l_1,\dots,l_{\mathfrak{k}}}}^{g+m}(x_{l_\iota}-x_i)},$$

$$N_{l_1,\dots,l_{\mathfrak{k}+1}}(x) = \frac{1}{(\mathfrak{k}+1)!}\prod_{\substack{i=1,\\ i\neq l_1,\dots,l_{\mathfrak{k}+1}}}^{g+m}\frac{(x-x_i)}{\prod\limits_{\iota=1}^{\mathfrak{k}+1}(x_{l_\iota}-x_i)}.$$

Note that

$$\sum_{\substack{l_\iota=1\\ l_\iota\neq l_1,\dots,\widehat{l_\iota},\dots,l_{\mathfrak{k}}}}^{g+m} M_{l_1,\dots,\widehat{l_\iota},\dots,l_{\mathfrak{k}}}(x)=0,$$

$$\sum_{\substack{l_\iota=1\\ l_\iota\neq l_1,\dots,\widehat{l_\iota},\dots,l_{\mathfrak{k}+1}}}^{g+m} N_{l_1,\dots,l_\iota,\dots,l_{\mathfrak{k}+1}}(x)=\frac{1}{\mathfrak{k}+1}M_{l_1,\dots,\widehat{l_\iota},\dots,l_{\mathfrak{k}+1}}(x),$$

where $\widehat{l_\iota}$ denotes the eliminated index. Evidently, summation of $N_{l_1,\dots,l_\iota,\dots,l_{\mathfrak{k}+1}}$ over two or more indices brings to zero.

Instead of interpolation polynomial the following rational function $\mathcal{G}$ is used

$$\mathcal{G}(x)=-\frac{\gamma_x(x)}{\gamma_y(x)}. \tag{3.21}$$

Substitution of (3.21) for y into f from (2.1) leads to

$$-\gamma_x(x)^2+\gamma_y(x)^2\mathcal{P}(x),$$

which is divisible by $\mathcal{F}$ due to the construction, and the quotient polynomial $\mathcal{H}$ has degree g, namely,

$$\mathcal{H}(x)=\frac{\gamma_y(x)^2\mathcal{P}(x)-\gamma_x(x)^2}{\mathcal{F}(x)}. \tag{3.22}$$

Finally, the reduced divisor corresponding to D_{g+m} is defined by

$$\mathcal{H}(x)=0,\qquad y=-\mathcal{G}(x), \tag{3.23}$$

where $\mathcal{G}$ is given by (3.21). If the form $y+\mathcal{I}(x)$ as in (3.1a) with polynomial $\mathcal{I}$ of degree $g-1$ is required, it can be constructed by the formula

$$\begin{aligned} &y+\mathcal{I}(x)=\mathcal{H}(x)\big(y\nu_y(x)+\nu_x(x)\big)+\big(y\gamma_y(x)-\gamma_x(x)\big)\mathcal{M}(x), \\ &\deg\nu_y=\deg\gamma_y-1,\qquad \deg\nu_x=\deg\gamma_x-1,\qquad \deg\mathcal{M}=g-1. \end{aligned} \tag{3.24}$$

Unknown coefficients of polynomials ν_y, ν_x, and $\mathcal{M}$ of number $2g+\left[m-\frac{1}{2}\right]$ are found from the same number of equations arising as vanishing coefficients at monomials $\big\{yx^{g+[(m-1)/2]-1},\dots,yx,x^{2g+[m/2]-1},\dots,x^g\big\}$ and the unit coefficient at y.

Remark 3.7. In the definition (3.19) of divisor D_{g+m} the rational function $\mathcal{R}$ has weight $2g+m$, and this is the minimal weight of a function whose $g+m$ roots can be chosen arbitrarily. This function is required in order to obtain a polynomial of degree g in (3.22).

Below we consider also the definition of a divisor by two polynomials (5.1), which usually occurs in cryptography oriented papers. In this case function $y-\mathcal{L}(x)$ has weight $2g+2m-2$, evidently it is greater than the minimal if $m>2$. This means that the intersection of this function with the curve contains $2g+2m-2$ points, which is seen by substituting $\mathcal{L}$ for y into $f(x,y)=0$. So the complement divisor to D_{g+m} in the intersection has degree $g+m-2$, and with $m>2$ formulas (3.21)–(3.23) with $\mathcal{G}$ replaced by $\mathcal{L}$ do not lead to a reduced divisor.

4 The reduction algorithm

Reduction of a degree $g+m$ divisor is realised directly in Section 3.5, which is applicable to a divisor defined by (3.19) or given as a collection of points. This realisation involves solution of a system of linear algebraic equations (3.24). To avoid this type of computation we suggest an iterative algorithm of reduction, involving only arithmetic operations on polynomials.

Recall that we deal with the hyperelliptic curve defined by (2.1). Let $D_{g+m} = \sum_{k=1}^{g+m} P_k$ be a divisor to reduce, where $m \geq 1$, and $P_k = (x_k, y_k)$. Reduction consists in finding a divisor $\widetilde{D}_g = \sum_{k=1}^{g} \widetilde{P}_k$ such that $\widetilde{D}_g - g\infty$ is equivalent to $D_{g+m} - (g+m)\infty$. The reduced divisor is defined by

- a polynomial $\mathcal{H}(x)$ of degree g, vanishing at $\widetilde{P}_k = (\tilde{x}_k, \tilde{y}_k)$,
- and an interpolation polynomial $\mathcal{I}(x)$ of degree $g-1$, such that $\tilde{y}_k = \mathcal{I}(\tilde{x}_k)$.

The pair of polynomials $\mathcal{H}$, $\mathcal{I}$ defines divisor $\widetilde{D}_g$ uniquely by the system

$$\mathcal{H}(x) = 0, \qquad y = \mathcal{I}(x).$$

In [3] and [7] the close addition problem is solved by means of the determinant construction. Here we suggest a more effective solution.

Let a divisor D of degree $g+m$ with $m > 0$ be given.

(I) If $\deg(D) = g+1$ the result is given by polynomials $\mathcal{H}$ and $\mathcal{I}$ defined by (3.1) if all $g+1$ points are distinct, by (3.12) if $P_{g+1} = P_1$, and by (3.16) in the case of $D = (g+1)P_1$.

(II) If $\deg(D) = g+2$ the result is given by polynomials $\mathcal{H}$ and $\mathcal{I}$ defined by (3.7).

(III) If $\deg(D) > g+2$ then an iterative procedure is used.

The iterative procedure is the following. Dealing with a divisor D of degree $g+m$ with $m > 2$, one performs the following steps:

Step 1. Start with any $g+1$ points, say $\{P_k = (x_k, y_k)\}_{k=1}^{g+1}$, and find polynomials $\mathcal{H}^{(1)}$, $\mathcal{I}^{(1)}$ by formulas (3.1b) and (3.1c), or (3.12b) and (3.12c), or (3.16b) and (3.16c). Then relations

$$\mathcal{H}^{(1)}(x) = 0, \qquad y = -\mathcal{I}^{(1)}(x)$$

define g points $\{\widetilde{P}_k^{(1)} = (\tilde{x}_k^{(1)}, \tilde{y}_k^{(1)})\}_{k=1}^{g}$ on curve (2.1), which replace the chosen $g+1$ points of the divisor D. In this way a new divisor D_{g+m-1} of degree $g+m-1$ is constructed.

Step 2. Suppose that a divisor D_{g+m-l} of degree $g+m-l$ is found, which consists of g points $\{\widetilde{P}_k^{(l)} = (\tilde{x}_k^{(l)}, \tilde{y}_k^{(l)})\}_{k=1}^{g}$ defined by

$$\mathcal{H}^{(l)}(x) = 0, \qquad y = -\mathcal{I}^{(l)}(x), \tag{4.1}$$

and the remaining $m-l$ points of D which form a divisor D'_{m-l}. Let P_{g+l+1} be a point from D'_{m-l}. With a collection of points $\{\widetilde{P}_k^{(l)}\}_{k=1}^{g} \cup \{P_{g+l+1}\}$ construct new polynomials

$$\mathcal{F}^{(l)}(x) = (x - x_{g+l+1})\mathcal{H}^{(l)}(x), \tag{4.2a}$$

$$\mathcal{G}^{(l)}(x) = \mathcal{I}^{(l)}(x) + \big(y_{g+l+1} - \mathcal{I}^{(l)}(x_{g+l+1})\big)\frac{\mathcal{H}^{(l)}(x)}{\mathcal{H}^{(l)}(x_{g+l+1})} \tag{4.2b}$$

of degrees $g+1$ and g, respectively. Evidently, the system

$$\mathcal{F}^{(l)}(x)=0, \qquad y=\mathcal{G}^{(l)}(x) \tag{4.3}$$

has $g+1$ solutions at points $\{\widetilde{P}_k^{(l)}\}_{k=1}^{g}\cup\{P_{g+l+1}\}$.

Step 3. Next, reduce the polynomials $\mathcal{F}^{(l)}$, $\mathcal{G}^{(l)}$ to polynomials $\mathcal{H}^{(l+1)}$ and $\mathcal{I}^{(l+1)}$ of degrees g and $g-1$

$$\mathcal{H}^{(l+1)}(x)=\frac{\mathcal{P}(x)-\mathcal{G}^{(l)}(x)^2}{\mathcal{F}^{(l)}(x)}, \tag{4.4a}$$

$$\mathcal{I}^{(l+1)}(x)=\mathfrak{g}_0\mathcal{H}^{(l+1)}(x)-\mathcal{G}^{(l)}(x), \tag{4.4b}$$

where $\mathfrak{g}_0$ is the coefficient of x^g in $\mathcal{G}^{(l)}(x)$. Note that $\mathcal{P}(x)-\mathcal{G}^{(l)}(x)^2$ is divisible by $\mathcal{F}^{(l)}(x)$ due to (4.3) and the fact that $\{\widetilde{P}_k^{(l)}\}_{k=1}^{g}\cup\{P_{g+l+1}\}$ are points of the curve $y^2=\mathcal{P}(x)$. The system

$$\mathcal{H}^{(l+1)}(x)=0, \qquad y=\mathcal{I}^{(l+1)}(x)$$

defines g points $\{\widetilde{P}_k^{(l+1)}=(\tilde{x}_k^{(l+1)},\tilde{y}_k^{(l+1)})\}_{k=1}^{g}$, which together with the remaining $m-l-1$ points of D form a new divisor $D_{g+m-l-1}$. If $l+1<m$, return to Step 2. This step is the same as the reduction algorithm given by Cantor [4].

The iterative procedure described above uses reduction by $g+1$ points at each step. One can use a different strategy, for example with $m=2\kappa$ the shortest iterative process is to apply reduction by $g+2$ points κ times, and with $m=2\kappa+1$ is to apply one reduction by $g+1$ points and κ reductions by $g+2$ points.

Remark 4.1. Note that computation of $\mathcal{I}^{(l)}(x)$ at each step is unnecessary. It is enough to replace (4.2b) by

$$\mathcal{G}^{(l)}(x)=-\mathcal{G}^{(l-1)}(x)+\big(y_{g+l+1}+\mathcal{G}^{(l-1)}(x)\big)\frac{\mathcal{H}^{(l)}(x)}{\mathcal{H}^{(l)}(x_{g+l+1})},$$

then (4.4b) can be skipped.

Remark 4.2. The reduction algorithm is expressed in terms of divisors since this explanation is geometric and the most evident. Despite the description, finding divisor is not required. Instead, coefficients of polynomials $\mathcal{H}^{(l)}$ and $\mathcal{I}^{(l)}$ completely define the intermediate divisor of degree g, as well as polynomials $\mathcal{F}^{(l)}$ and $\mathcal{G}^{(l)}$ define the intermediate divisor of degree $g+1$. So the algorithm can be realised over any field.

Remark 4.3. Let us point out that Step 2 of the reduction algorithm provides a procedure of adding one point to a divisor of degree g, or to any greater degree divisor defined by a system in the form (4.1). So the reduction algorithm solves the problem of adding a non-special divisor defined by a pair of polynomials and a special divisor given as a collection of points. A collection of points is added by one point according to the algorithm.

Another approach to addition is presented in the next section.

Remark 4.4. One can add one point to a special divisor using formulas (4.2). The special divisor is supposed to be defined as in Proposition 2.1. Then (4.3) represents the resulting divisor directly.

Application in cryptography. We would like to point out two practical setups which serve as hyperelliptic cryptography algorithms.

I. Alice and Bob choose a non-special divisor D_g, which is public. Alice chooses a number n_A and keeps in secret, and Bob chooses a number n_B and keeps in secret. Next, they are using the reduction algorithm described above to obtain a reduced form for the divisors $n_A D_g$ and $n_B D_g$. These are the divisors they exchange. Once Alice gets the divisor $n_B D_g$ from Bob (reduced form), she computes $n_A(n_B D_g)$. On the other hand, Bob computes the same divisor as $n_B(n_A D_g)$. The reduced form of this divisor is the shared secret of Bob and Alice. This is an implementation of the Diffie–Hellman exchange with the help of the reduction algorithm introduced above.

The first step of the reduction algorithm for a scalar multiple $n_j D_g$ is provided by Theorem 3.5. Divisor D_g is assumed to consist of distinct points, and only on the first step a collection of $g+1$ points contains two equal points. It is very unlikely, that a reduced divisor on any step contains points coinciding with D_g. Points of the divisor D_g can be chosen from a desired finite field to produce polynomials with coefficients from this field.

II. Alice and Bob choose a non-special divisor D_g of the form gP_1. Then Alice computes the reduced form of $n_A(gP_1)$, and Bob computes the reduced form of $n_B(gP_1)$. They exchange the reduced forms of their divisors. The first step of the reduction algorithm in this case is provided by Theorem 3.6, on further steps Theorem 3.1 or 3.3 is used. After exchange Alice and Bob compute the reduced form of divisor $n_A n_B(gP_1)$ which is the shared secret.

5 The addition algorithm

Now we suggest a procedure to solve the addition problem. We start with a different setup. Let two non-special divisors D_{g+m_1} and D_{g+m_2} of degrees $g+m_1$ and $g+m_2$ are defined by two polynomials each. Namely, polynomials $\mathcal{F}_1$ and $\mathcal{L}_1$ of degrees $g+m_1$ and $g+m_1-1$ define D_{g+m_1} by the system

$$\mathcal{F}_1(x)=0, \qquad y=\mathcal{L}_1(x);$$

and polynomials $\mathcal{F}_2$ and $\mathcal{L}_2$ of degrees $g+m_2$ and $g+m_2-1$ define D_{g+m_2} by the system

$$\mathcal{F}_2(x)=0, \qquad y=\mathcal{L}_2(x).$$

Degrees of polynomials $\mathcal{L}_1$ and $\mathcal{L}_2$ are justified as follows. Suppose we are given points $\sum_{k=1}^{g+m}(x_k,y_k) = D_{g+m}$, then a polynomial $\mathcal{L}$ such that $y-\mathcal{L}(x)$ vanishes on D_{g+m} is constructed by the determinant formula on the monomials $\{1,x,\dots,x^{g+m-1},y\}$. Since (x_k,y_k) are points of a hyperelliptic curve there is no linear relation between coordinates y_k, and so the coefficient at x^{g+m-1} does not vanish. Obviously, $y-\mathcal{L}(x)$ is not the minimal weight function to define D_{g+m}.

Lemma 5.1. *Let a non-special divisor of degree D_{g+m} is defined by two polynomials: $\mathcal{F}$ of degree $g+m$ and $\mathcal{L}$ of degree equal to or greater than $g+m-1$ as follows*

$$\mathcal{F}(x)=0, \qquad y=\mathcal{L}(x). \tag{5.1}$$

Then a rational function $\mathcal{R}$ of the minimal weight $2g+m$ exists, and the system

$$\mathcal{F}(x)=0, \qquad \mathcal{R}(x,y)=0$$

defines D_{g+m} equivalently.

Proof. The rational function $\mathcal{R}$ of weight $2g+m$ has the form (3.20). If $\deg\mathcal{L}\geqslant\deg\mathcal{F}$, then $\mathcal{L}$ in (5.1) can be replaced by $\widetilde{\mathcal{L}}=\mathcal{L} \bmod \mathcal{F}$. Suppose $\deg\mathcal{L}=g+m-1$, then $\mathcal{R}$ is constructed in the form

$$\mathcal{R}(x,y)=\mathcal{N}(x)\mathcal{F}(x)+\big(y-\mathcal{L}(x)\big)\mathcal{M}(x),$$
$$\deg\mathcal{N}=[(m-1)/2]-1, \qquad \deg\mathcal{M}=[(m-1)/2].$$

On the right hand side extra powers of x arises, namely from $x^{g+[m/2]+1}$ to $x^{g+m-1+[(m-1)/2]}$, coefficients of which should vanish. Thus, for $2[(m-1)/2]+1$ unknowns one obtains equations of number

$$m+[(m-1)/2]-[m/2]-1=2[(m-1)/2].$$

So the function $\mathcal{R}$ up to a constant multiple is found. ■

Lemma 5.2. *Let $\mathcal{F}_1$, $\mathcal{L}_1$ and $\mathcal{F}_2$, $\mathcal{L}_2$ be two pairs of polynomials, at that* $\deg \mathcal{L}_i < \deg \mathcal{F}_i$ *and* $\gcd(\mathcal{F}_1,\mathcal{F}_2)=1$. *Then a polynomial $\mathcal{L}$ exists such that $\mathcal{L}_i=\mathcal{L} \bmod \mathcal{F}_i$, $i=1,2$.*

The lemma is known as the Chinese remainder theorem, see for example [8, Theorem 16.19]. For the sake of completeness a proof is provided.

Proof. As $\gcd(\mathcal{F}_1,\mathcal{F}_2)=1$, there exist polynomials $\mathcal{M}_1$ and $\mathcal{M}_2$ such that

$$\mathcal{M}_2(x)\mathcal{F}_1(x)+\mathcal{M}_1(x)\mathcal{F}_2(x)=1. \tag{5.2}$$

A polynomial $\mathcal{M}_i$ can be taken of degree $\mathcal{F}_i-1$, then $\deg \mathcal{F}_1+\deg \mathcal{F}_2$ unknown coefficients are found by equating coefficients on the both sides of the relation (5.2). Then polynomial

$$\mathcal{L}(x)=\mathcal{M}_2(x)\mathcal{F}_1(x)\mathcal{L}_2(x)+\mathcal{M}_1(x)\mathcal{F}_2(x)\mathcal{L}_1(x) \tag{5.3}$$

satisfies the lemma conditions. Indeed,

$$\begin{aligned}\mathcal{L}(x)-\mathcal{L}_1(x)&=\mathcal{M}_2(x)\mathcal{F}_1(x)\mathcal{L}_2(x)+\mathcal{M}_1(x)\mathcal{F}_2(x)\mathcal{L}_1(x)-\mathcal{L}_1(x)\\&=\mathcal{M}_2(x)\mathcal{F}_1(x)\big(\mathcal{L}_2(x)-\mathcal{L}_1(x)\big)\end{aligned}$$

is divisible by $\mathcal{F}_1$ as required. The same is true for $\mathcal{F}_2$. ■

The algorithm of additing two divisors D_{g+m_1} and D_{g+m_2} consists of the following steps

1. The sum $D_{2g+m_1+m_2}$ of D_{g+m_1} and D_{g+m_2} is uniquely defined by two polynomials $\mathcal{F}$ and $\mathcal{L}$ such that $\mathcal{F}(x)=\mathcal{F}_1(x)\mathcal{F}_2(x)$ at that $\gcd(\mathcal{F}_1,\mathcal{F}_2)=1$, and $\mathcal{L}$ is obtained by (5.3). Note that $\deg \mathcal{L}=3g+m_1+m_2+\max(m_1,m_2)-2$. As seen from the proof of Lemma 5.2, $\mathcal{L}$ vanishes on the both divisors. This step coincides with a special case of Cantor's composition algorithm [4, p. 98].
2. By Lemma 5.1 a rational function $\mathcal{R}$ of weight $2g+m_1+m_2$ vanishing on $D_{2g+m_1+m_2}$ is constructed from $\mathcal{F}$ and $\mathcal{L}$.
3. The reduced problem for $D_{2g+m_1+m_2}$ defined by the polynomial $\mathcal{F}$ and the rational function $\mathcal{R}$ is solved as in Section 3.5.

Another approach to solution of the addition problem for two divisors of degree g can be found in [3, Theorem 1.23, p. 75–76 in Russian version].

Remark 5.3. The addition algorithm is also applicable to special divisors of degree $m<g$ provided that their sum is a non-special divisor of degree greater than g. If the resulting divisor has degree equal to g or less (and has no points in involution as we explained in preliminaries), only Step 1 is needed.

6 Conclusion

The reduction problem is solved explicitly for divisors of degrees $g+1$ and $g+2$ in the case of all distinct points (Theorems 3.1 and 3.3), for a divisor of degree $g+1$ with duplication (Theorem 3.5), for a divisor of the form $(g+1)P$ (Theorem 3.6). Polynomials defining a reduced divisor are expressed in terms of the points of an initial divisor, and their coefficients are computed directly.

It is worth to note that the mentioned polynomials also serve as a solution of the Jacobi inversion problem for a reduced divisor, see Remarks 3.2 and 3.4, similar relations hold in the other cases. And so the polynomial coefficients give values $\wp\big(u(D)\big)$ on an initial divisor D for $2g$ functions which form a basis of the differential field of Abelian functions on Jacobian of the curve. The demand for such values arises in some problems of mathematical physics. Until now this approach to computation of $\wp$ functions has not appeared in the literature.

The reduction problem introduces the relation of equivalence on the space of non-special divisors on a curve. To every non-special divisor an equivalent reduced divisor is assigned, the latter serves as a representative of an equivalence class consisting of all divisors reduced to this representative reduced divisor. A reduced divisor maps uniquely to a point of Jacobian of the curve, and its equivalence class maps to the same point of Jacobian. So a many-to-one mapping from the space of non-special divisors to Jacobian arises. This idea can be used to compute $\wp$ functions on arbitrary non-special divisors and solve the generalised Jacobi inversion problem.

The proposed iterative reduction algorithm has the advantage that all steps are realised in terms of polynomials obtained by means of arithmetic operations of addition, multiplication and division, and so the algorithm preserves the field to which coefficients of initial polynomials belong. The initial divisor is supposed to belong to the same field. The algorithm can also be interpreted as addition of a non-special divisor defined by a pair of polynomials and a special or non-special divisor given as a collection of points. Two scenarios of hyperelliptic cryptography algorithms on its base were suggested.

A solution of the reduction problem which does not involve points is also given for a degree $g+m$ divisor. Two ways to define the divisor are considered: by two polynomials, and by a polynomial and a rational function of the minimal weight. The relation between these two types of definition is described, as well as the necessity to use the rational function of the minimal weight in order to find the reduced divisor. And the proposed addition algorithm, whose first step is the standard addition algorithm producing two polynomials for the resulting divisor, is completed with finding a rational function of the minimal weight and the reduction problem.

Acknowledgements

The authors are thankful to the referees for the comments which had improved the paper substantially.

References

[1] Baker H.F., Abelian functions. Abel's theorem and the allied theory of theta functions, *Cambridge Mathematical Library*, Cambridge University Press, Cambridge, 1995.

[2] Bukhshtaber V.M., Leykin D.V., Heat equations in a nonholomic frame, *Funct. Anal. Appl.* **38** (2004), 88–101.

[3] Bukhshtaber V.M., Leykin D.V., Addition laws on Jacobians of plane algebraic curves, *Proc. Steklov Inst. Math* **251** (2005), 49–120.

[4] Cantor D.G., Computing in the Jacobian of a hyperelliptic curve, *Math. Comp.* **48** (1987), 95–101.

[5] de Jong R., Müller J.S., Canonical heights and division polynomials, *Math. Proc. Cambridge Philos. Soc.* **157** (2014), 357–373, arXiv:1306.4030.

[6] Gaudry P., Fast genus 2 arithmetic based on theta functions, *J. Math. Cryptol.* **1** (2007), 243–265.

[7] Shaska T., Kopeliovich Y., Additiona laws on Jacobians from a geometric point of view, arXiv:1907.11070.

[8] Shoup V., A computational introduction to number theory and algebra, 2nd ed., Cambridge University Press, Cambridge, 2009.

[9] Sutherland A.V., Fast Jacobian arithmetic for hyperelliptic curves of genus 3, in Proceedings of the Thirteenth Algorithmic Number Theory Symposium, *Open Book Ser.*, Vol. 2, Math. Sci. Publ., Berkeley, CA, 2019, 425–442, arXiv:1607.08602.

[10] Uchida Y., Division polynomials and canonical local heights on hyperelliptic Jacobians, *Manuscripta Math.* **134** (2011), 273–308.