ADDITION LAW ON JACOBIAN OF GENUS TWO CURVE FOR CRYPTOGRAPHY

JULIA BERNATSKA

ABSTRACT. We shall consider a genus two curve for cryptography, that is an equation of the curve contains y-term. Sigma function related to the curve is constructed by means of recurrence relations in the form of a power series in coordinates of Jacobian variety and parameters of the curve. Explicit expressions of the addition law in terms of (i) Abelian functions and (ii) coordinates of two points will be presented.

1. INTRODUCTION

We consider a family of genus two curves $\mathcal{V}$ which are of great interest in hyperelliptic cryptography. These are curves of the form

$$\begin{aligned}(1)\quad 0 = f(x,y) = -y^2 + x^5 + y(\mu_1 x^2 + \mu_3 x + \mu_5)\\ + \mu_2 x^4 + \mu_4 x^3 + \mu_6 x^2 + \mu_8 x + \mu_{10},\end{aligned}$$

In our consideration coefficients $\mu = (\mu_1, \mu_3, \mu_5, \mu_2, \mu_4, \mu_6, \mu_8, \mu_{10})$ are complex variables in $\mathbb{C}^8$, and so (1) defines a family of curves over the base $\mathbb{C}^8$.

The present paper is devoted to construction of sigma function related to curve (1) by means of the theory of multivariate sigma functions developed by Leykin and Buchstaber in [1–4]. The theory is proposed for a special class of curves called (n,s)-curves, and $(2,5)$-curve $\mathcal{V}_{(2,5)}$

$$(2)\qquad 0 = f_{(2,5)}(z,w) = -w^2 + z^5 + \lambda_4 z^3 + \lambda_6 z^2 + \lambda_8 z + \lambda_{10}.$$

serves as the main example in [4].

Sigma function related to (1) is constructed by a new method, based on a transformation from the known $(2,5)$-curve $\mathcal{V}_{(2,5)}$ to the curve in question, and is defined by the formula

$$\begin{aligned}(3)\quad \sigma(u;\mu) = \exp\Big\{\tfrac{1}{20}(\mu_1^2+4\mu_2)\Big(u_1^2 + \tfrac{1}{20}(\mu_1^2+4\mu_2)u_1u_3\\ - \tfrac{1}{2}\big(\tfrac{3}{200}(\mu_1^2+4\mu_2)^2 - \tfrac{1}{2}(\mu_1\mu_3+2\mu_4)\big)u_3^2\Big)\Big\}\times\end{aligned}$$

$$\times\, \sigma_{(2,5)}\big(u_1 + \tfrac{1}{20}(\mu_1^2 + 4\mu_2), u_3; \lambda(\mu)\big).$$

The expansion for $\sigma(u,\mu)$ is given in Appendix A. The reader could find a similar expansion obtained by C. Eilbeck for a similar curve, see `http://www.ma.hw.ac.uk/Weierstrass/Hyp25/`, though the curve in the set of problem looks slightly defective in term $\mu_1 x^2 + \mu_3 x + \mu_5$ (taken with the opposite sign). So some coefficients in the expansion and relations between Abelian functions differ from the obtained in this paper.

Addition theorem for genus 2 curve goes back to Baker [5],

$$\frac{\sigma(u+v)\sigma(u-v)}{\sigma(u)^2\sigma(v)^2} \\ = \wp_{1,1}(u)\wp_{1,3}(v) - \wp_{1,1}(v)\wp_{1,3}(u) + \wp_{1,1}(v) - \wp_{1,1}(u)$$

New results and generalization to hyperelliptic case can be found in [6, 7], a summary in [8, p. 232]. Below an alternative method of constructing addition law is used. The method proposed firstly in [9], where it is applied to a trigonal curve, gives a nice form of representing an addition law, in the case of genus 2 curve $\mathcal{V}$ we have with $u+v+w=0$

$$\operatorname{rank}\begin{pmatrix} 1 & 0 & \wp_{1,3}(u) & -\frac{1}{2}\big(\wp_{1,1,3}(u) - \mu_1\wp_{1,3}(u) - \mu_5\big) & \wp_{1,1}(u)\wp_{1,3}(u) \\ 1 & 0 & \wp_{1,3}(v) & -\frac{1}{2}\big(\wp_{1,1,3}(v) - \mu_1\wp_{1,3}(v) - \mu_5\big) & \wp_{1,1}(v)\wp_{1,3}(v) \\ 1 & 0 & \wp_{1,3}(w) & -\frac{1}{2}\big(\wp_{1,1,3}(w) - \mu_1\wp_{1,3}(w) - \mu_5\big) & \wp_{1,1}(w)\wp_{1,3}(w) \\ 0 & 1 & \wp_{1,1}(u) & -\frac{1}{2}\big(\wp_{1,1,1}(u) - \mu_1\wp_{1,1}(u) - \mu_3\big) & \wp_{1,1}(u)^2 + \wp_{1,3}(u) \\ 0 & 1 & \wp_{1,1}(v) & -\frac{1}{2}\big(\wp_{1,1,1}(v) - \mu_1\wp_{1,1}(v) - \mu_3\big) & \wp_{1,1}(v)^2 + \wp_{1,3}(v) \\ 0 & 1 & \wp_{1,1}(w) & -\frac{1}{2}\big(\wp_{1,1,1}(w) - \mu_1\wp_{1,1}(w) - \mu_3\big) & \wp_{1,1}(w)^2 + \wp_{1,3}(w) \end{pmatrix} = 4. \tag{4}$$

Here an adaptation to the curve $\mathcal{V}$ defined by (1) is given.

2. Preliminaries

In this paper we focus on the curve $\mathcal{V}$ defined by (1), which is genus 2 hyperelliptic curve with five finite branch points, and one at infinity. The curve is supposed not degenerate, that is its discriminant does not vanish. However all constructions and computations are valid in the case of degenerate curve. Homology basis $\{\mathfrak{a}_1, \mathfrak{b}_1, \mathfrak{a}_2, \mathfrak{b}_2\}$ is introduced in the standard way, see for example [10, p. 303]. The standard cohomology basis consists of first kind differentials $\mathrm{d}u = (\mathrm{d}u_1,\, \mathrm{d}u_3)^t$,

$$\mathrm{d}u_1 = \frac{x\,\mathrm{d}x}{\partial_y f}, \qquad \mathrm{d}u_3 = \frac{\mathrm{d}x}{\partial_y f},$$

and second kind differentials $\mathrm{d}r = (\mathrm{d}r_1,\, \mathrm{d}r_3)^t$ associated to the first kind differentials, see [10, p. 306] for definition. The latter are known for genus 2 curve $\mathcal{V}_{(2,5)}$ defined by (2) as in (10), and are obtained here for curve $\mathcal{V}$, see (9).

The Jacobian of a curve $\mathcal{V}$ is denoted by $\mathrm{Jac}(\mathcal{V})$, Abel's map is defined with the base point at infinity as

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

and also second kind integral

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

regardless of the singularity of $\mathrm{d}r$ at this point. The second kind integral is regularized through expansion at infinity, where

$$\begin{aligned}(5)\quad x = \xi^{-2}, \quad y = \xi^{-5}\bigg(&1 + \frac{\mu_1}{2}\xi + \frac{1}{8}(\mu_1^2 + 4\mu_2)\xi^2 + \frac{\mu_3}{2}\xi^3 \\ &+ \Big(\frac{\mu_4}{2} + \frac{\mu_1\mu_3}{4} - \frac{1}{2^7}(\mu_1^2 + 4\mu_2)^2\Big)\xi^4 + \frac{\mu_5}{2}\xi^5 + O(\xi^6)\bigg).\end{aligned}$$

Thus,

$$\mathcal{A}^{*}(\xi) = \begin{pmatrix} -\xi^{-1} \\ -\xi^{-3} \end{pmatrix} + \int_{\infty}^{P(x,y)} \begin{pmatrix} \mathrm{d}r_1(\xi) - \xi^{-2} \\ \mathrm{d}r_3(\xi) - 3\xi^{-4} \end{pmatrix}.$$

Second kind integral relates to zeta function as follows, where points (x_1, y_1), (x_2, y_2) form Abel's preimage of $u \in \mathrm{Jac}(\mathcal{V})$

$$\begin{aligned} r_1(x_1, y_1) + r_1(x_2, y_2) &= -\zeta_1(u), \\ r_3(x_1, y_1) + r_3(x_2, y_2) &= -\zeta_3(u) + \frac{1}{2}\wp_{1,1,1}(u). \end{aligned}$$

Thoughout the paper we use Satō weights as subscripts for convenience. The weight shows an exponent with opposite sign of the leading term in expansion about infinity in parameter ξ, namely $\operatorname{wgt} x = 2$, $\operatorname{wgt} y = 5$, $\operatorname{wgt} f(x, y) = 10$, $\operatorname{wgt} \mu_i = i$, and $\operatorname{wgt} u_1 = -1$, $\operatorname{wgt} u_3 = -3$, $\operatorname{wgt} r_1 = 1$, $\operatorname{wgt} r_3 = 3$. The theory we use here respects Satō weight, so every expression is homogenious in the weight.

3. Sigma function from curve transformation

Suppose we find a transformation $(z, w) \mapsto (x, y)$ from a known curve $\widetilde{f}(z, w, \lambda) = 0$ to a new one $f(x, y, \mu) = 0$, and also a transformation of coefficients $\lambda \mapsto \mu$. We need also cohomology bases on the both curves. According to [2,3] a cohomology basis on a curve consists of g first and g second kind differentials such that the period matrix with respect to these differentials is symplectic. There is a way which allows to obtain such a basis avoiding computation of periods. Let $\widetilde{R} = (\mathrm{d}\widetilde{u}, \mathrm{d}\widetilde{r})^t$ be the cohomology basis on the known curve, and $R = (\mathrm{d}u, \mathrm{d}r)^t$ be the basis on the new curve. Applying the transformations to $\widetilde{R}$ we obtain a matrix T of linear transformation from R to $\widetilde{R}$ of the form

$$\widetilde{R} = TR, \qquad \text{where} \qquad T = \begin{pmatrix} T_{11} & T_{12} \\ T_{21} & T_{22} \end{pmatrix}.$$

Evidently, $T_{12} = 0$. Moreover, T is a symplectic matrix, that is T satisfies Legendre identity

$$T^t \,\mathbb{J}\, T = \mathbb{J}, \qquad \mathbb{J} = \begin{pmatrix} 0 & J \\ -J & 0 \end{pmatrix}, \quad J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

With the transformation defined above sigma-function transforms by the rule

$$\sigma(u;\mu) = \exp\Big(\tfrac{1}{2} u^t (J T_{22}^{-1} T_{21}) u\Big) \widetilde{\sigma}\big(T_{11} u; \lambda(\mu)\big). \tag{6}$$

4. Transformation from $(2,5)$-curve

Curve (1) is obtained from (2) by the transformation

$$w = y - \frac{1}{2}\big(\mu_1 x^2 + \mu_3 x + \mu_5\big), \qquad z = x + \frac{1}{20}\big(\mu_1^2 + 4\mu_2\big), \tag{7}$$

and

(8)

$$\begin{aligned}
\lambda_4 &= \mu_4 + \frac{1}{2}\mu_1\mu_3 - \frac{2}{5}\mu_2^2 - \frac{1}{5}\mu_1^2\mu_2 - \frac{1}{40}\mu_1^4, \\
\lambda_6 &= \mu_6 + \frac{1}{2}\mu_1\mu_5 + \frac{1}{4}\mu_3^2 - \frac{2}{25}\mu_2^3 - \frac{3}{50}\mu_1^2\mu_2^2 - \frac{3}{200}\mu_1^4\mu_2 - \frac{\mu_1^6}{800} \\
&\quad - \frac{3}{20}\big(\mu_1^2 + 4\mu_2\big)\bigg(\mu_4 + \frac{1}{2}\mu_1\mu_3 - \frac{2}{5}\mu_2^2 - \frac{1}{5}\mu_1^2\mu_2 - \frac{1}{40}\mu_1^4\bigg), \\
\lambda_8 &= \mu_8 + \frac{1}{2}\mu_3\mu_5 - \frac{\mu_2^4}{125} - \frac{1}{125}\mu_1^2\mu_2^3 - \frac{3\mu_1^4\mu_2^2}{1000} - \frac{\mu_1^6\mu_2}{2000} - \frac{\mu_1^8}{32000} \\
&\quad - \frac{1}{10}\big(\mu_1^2 + 4\mu_2\big)\bigg(\mu_6 + \frac{1}{2}\mu_1\mu_5 + \frac{1}{4}\mu_3^2 - \frac{2}{25}\mu_2^3 - \frac{3}{50}\mu_1^2\mu_2^2 - \frac{3}{200}\mu_1^4\mu_2 - \frac{\mu_1^6}{800}\bigg) \\
&\quad + \frac{3}{20^2}\big(\mu_1^2 + 4\mu_2\big)^2\bigg(\mu_4 + \frac{1}{2}\mu_1\mu_3 - \frac{2}{5}\mu_2^2 - \frac{1}{5}\mu_1^2\mu_2 - \frac{1}{40}\mu_1^4\bigg), \\
\lambda_{10} &= \mu_{10} + \frac{\mu_5^2}{4} - \frac{\mu_2^5}{3125} - \frac{\mu_1^2\mu_2^4}{2500} - \frac{\mu_1^4\mu_2^3}{5000} - \frac{\mu_1^6\mu_2^2}{20000} - \frac{\mu_1^8\mu_2}{160000} - \frac{\mu_1^{10}}{3200000} \\
&\quad - \frac{1}{20}\big(\mu_1^2 + 4\mu_2\big)\bigg(\mu_8 + \frac{1}{2}\mu_3\mu_5 - \frac{\mu_2^4}{125} - \frac{1}{125}\mu_1^2\mu_2^3 - \frac{3\mu_1^4\mu_2^2}{1000} - \frac{\mu_1^6\mu_2}{2000} - \frac{\mu_1^8}{32000}\bigg)
\end{aligned}$$

$$+\frac{1}{20^2}\big(\mu_1^2+4\mu_2\big)^2\bigg(\mu_6+\frac{1}{2}\mu_1\mu_5+\frac{1}{4}\mu_3^2-\frac{2}{25}\mu_2^3-\frac{3}{50}\mu_1^2\mu_2^2-\frac{3\mu_1^4\mu_2}{200}-\frac{\mu_1^6}{800}\bigg)$$
$$+\frac{1}{20^3}\big(\mu_1^2+4\mu_2\big)^3\bigg(\mu_4+\frac{1}{2}\mu_1\mu_3-\frac{2}{5}\mu_2^2-\frac{1}{5}\mu_1^2\mu_2-\frac{1}{40}\mu_1^4\bigg).$$

By the method of [3], we find cohomology basis on $\mathcal{V}$, which consists of 2 standard first kind differentials, and 2 second kind differentials associated to the first ones

$$R=\begin{pmatrix}\mathrm{d}u_3\\ \mathrm{d}u_1\\ \mathrm{d}r_1\\ \mathrm{d}r_3\end{pmatrix}=\begin{pmatrix}1\\ x\\ x^2\\ 3x^3+\big(2\mu_2+\frac{1}{2}\mu_1^2\big)x^2+\big(\mu_4+\frac{1}{2}\mu_1\mu_3\big)x\end{pmatrix}\frac{\mathrm{d}x}{\partial_y f}. \tag{9}$$

Applying (7) and (8) to the cohomology basis on $\mathcal{V}_{(2,5)}$

$$\widetilde{R}=\begin{pmatrix}\mathrm{d}\widetilde{u}_3\\ \mathrm{d}\widetilde{u}_1\\ \mathrm{d}\widetilde{r}_1\\ \mathrm{d}\widetilde{r}_3\end{pmatrix}=\begin{pmatrix}1\\ z\\ z^2\\ 3z^3+\lambda_4 z\end{pmatrix}\frac{\mathrm{d}z}{\partial_w f}. \tag{10}$$

we figure out transformation matrix T such that $\widetilde{R}=TR$. Actually,

$$T_{11}=\begin{pmatrix}1 & 0\\ \frac{1}{20}(\mu_1^2+4\mu_2) & 1\end{pmatrix},\qquad T_{22}=\begin{pmatrix}1 & 0\\ -\frac{1}{20}(\mu_1^2+4\mu_2) & 1\end{pmatrix}$$

$$T_{21}=\begin{pmatrix}\frac{1}{20^2}(\mu_1^2+4\mu_2)^2 & \frac{1}{10}(\mu_1^2+4\mu_2)\\ -\frac{1}{20}(\mu_1^2+4\mu_2)\Big(\frac{7}{20^2}(\mu_1^2+4\mu_2)^2-\frac{1}{2}(\mu_1\mu_3+2\mu_4)\Big) & -\frac{1}{20^2}(\mu_1^2+4\mu_2)^2\end{pmatrix}.$$

Thus,

$$JT_{22}^{-1}T_{21}=\begin{pmatrix}-\frac{1}{20}(\mu_1^2+4\mu_2)\big(\frac{3}{200}(\mu_1^2+4\mu_2)^2-\frac{1}{2}(\mu_1\mu_3+2\mu_4)\big) & \frac{1}{20^2}(\mu_1^2+4\mu_2)^2\\ \frac{1}{20^2}(\mu_1^2+4\mu_2)^2 & \frac{1}{10}(\mu_1^2+4\mu_2)\end{pmatrix}.$$

Finally, we come to (6).

5. Jacobi inversion problem

Here we take into account the solution of Jacobi inversion problem, that is $\mathcal{R}_4(x,y;u)$ and $\mathcal{R}_5(x,y;u)$ vanish simultaneously at the Abel's preimage (x_k,y_k), $k=1,2$, of u, where

$$\mathcal{R}_4(x,y;u)=x^2-x\wp_{1,1}(u)-\wp_{1,3}(u), \tag{11a}$$

$$\begin{aligned}\mathcal{R}_5(x,y;u)=2y&+\frac{1}{2}\big(\wp_{1,1,1}(u)-\mu_1\wp_{1,1}(u)-\mu_3\big)x\\ &+\frac{1}{2}\big(\wp_{1,1,3}(u)-\mu_1\wp_{1,3}(u)-\mu_5\big).\end{aligned} \tag{11b}$$

The functions $\mathcal{R}_4$ and $\mathcal{R}_4$ are obtained from Klein formula

$$\frac{\mathcal{F}(x,y,x_k,y_k)+2yy_k}{(x-x_k)^2} = xx_k\wp_{1,1}(U)+(x+x_k)\wp_{1,3}(U)+\wp_{3,3}(U) \tag{12}$$

which holds for two points (x_k,y_k) of the divisor of u , where

$$U=\bigg(\int_{\infty}^{(x_1,y_1)}\mathrm{d}u+\int_{\infty}^{(x_2,y_2)}\mathrm{d}u\bigg)-\int_{\infty}^{(x,y)}\mathrm{d}u,$$

and Klein bipolar is of the following form

$$\begin{aligned}\mathcal{F}(x,y,z,w) &= -y(\mu_1z^2+\mu_3z+\mu_5)-w(\mu_1x^2+\mu_3x+\mu_5)\\ &\quad + x^2z^2(x+z)+(\mu_1^2+2\mu_2)x^2z^2+(\mu_4+\mu_1\mu_3)xz(x+z)\\ &\quad + \tfrac{1}{2}\mu_1\mu_5(x+z)^2+(\mu_3^2+2\mu_6)xz+(\mu_8+\mu_3\mu_5)(x+z)+\mu_5^2+2\mu_{10}.\end{aligned}$$

Formula (12) is expanded in the vicinity of infinity when $(x,y)\to\infty$ in parameter ξ, where (5) is applied. Function $\mathcal{R}_4$ arises as a coefficient at ξ^{-6}, and $\mathcal{R}_5$ as a coefficient at ξ^{-5}.

Only four Abelian functions $\wp_{1,1}$, $\wp_{1,3}$, $\wp_{1,1,1}$, and $\wp_{1,1,3}$ occur in (11), we use them as a basis in the differential field of Abelian functions on the Jacobian $\mathrm{Jac}(\mathcal{V})$. Equations (11) are solved for these basis functions:

$$\begin{aligned}&\wp_{1,1}(u)=x_1+x_3, &&\wp_{1,1,1}(u)=-2\frac{y_1-y_2}{x_1-x_2}+\mu_1(x_1+x_2)+\mu_3,\\ &\wp_{1,3}(u)=-x_1x_2, &&\wp_{1,1,3}(u)=2\frac{y_1x_2-y_2x_1}{x_1-x_2}-\mu_1x_1x_2+\mu_5.\end{aligned} \tag{13}$$

We use formulas (13) for computation of the basis Abelian functions in terms of a divisor.

6. Addition formulas

Here we obtain addition law from trilinear relation, see [7, p. 104], by the method developed in [9].

$$\frac{\sigma(u+\mathcal{A}(\xi))\sigma(v+\mathcal{A}(\xi))\sigma(w+\mathcal{A}(\xi))}{\psi^3(\xi)\sigma(u)\sigma(v)\sigma(w)} = \mathcal{R}_6\big(x(\xi),y(\xi)\big)\Big|_{u+v+w=0}, \tag{14}$$

where ψ is an entire function in ξ of the form, see [7, p. 79]

$$\psi(\xi)=\exp\bigg(-\int_0^{\xi}\mathcal{A}^*(\tilde{\xi})\mathrm{d}\mathcal{A}(\tilde{\xi})\bigg).$$

Function $\mathcal{R}_6$ is extracted from the expansion of Klein formula (12) as a coefficient at ξ^{-4}.

Proposition 6.1. *Assume a rational funtion of order $3g = 6$ on $\mathcal{V}$*

$$\mathcal{R}_6(x,y) = x^3 + \alpha_1 y + \alpha_2 x^2 + \alpha_4 x + \alpha_6, \tag{15}$$

vanishes at $2g = 4$ points (x_k, y_k) and (z_k, w_k), $k = 1, 2$, which are Abel's preimages of u and v in the Jacobian of $\mathcal{V}$. Then

$$\begin{aligned} &(\alpha_2, \alpha_1)^t = -\big(M(u) - M(v)\big)^{-1}\big(\pi(u) - \pi(v)\big),\\ &(\alpha_6, \alpha_4)^t = M(u)\big(M(u) - M(v)\big)^{-1}\big(\pi(u) - \pi(v)\big) - \pi(u), \end{aligned} \tag{16}$$

where

$$M(u) = \begin{pmatrix} \wp_{1,3}(u) & -\frac{1}{2}\big(\wp_{1,1,3}(u) - \mu_1\wp_{1,3}(u) - \mu_5\big)\\ \wp_{1,1}(u) & -\frac{1}{2}\big(\wp_{1,1,1}(u) - \mu_1\wp_{1,1}(u) - \mu_3\big)\end{pmatrix},$$

$$\pi(u) = \begin{pmatrix} \wp_{1,1}(u)\wp_{1,3}(u) \\ \wp_{1,1}(u)^2 + \wp_{1,3}(u)\end{pmatrix}.$$

Proof. We employ the relation in terms of (11)

$$\begin{aligned} \mathcal{R}_6(x,y) &- \tfrac{1}{2}\alpha_1\mathcal{R}_5(x,y;u)\\ &- \big(x + \alpha_2 + \tfrac{1}{2}\mu_1\alpha_1 + \wp_{1,1}(u)\big)\mathcal{R}_4(x,y;u) = (1,x)Q(u), \end{aligned} \tag{17}$$

where

$$Q(u) = (\alpha_6, \alpha_4)^t + M(u)(\alpha_2, \alpha_1)^t + \pi(u).$$

By the assumption $\mathcal{R}_6(x,y)$ vanishes sumiltaneously with $\mathcal{R}_4(x,y;u)$ and $\mathcal{R}_5(x,y;u)$ on the preimages of u and v. This implies $Q(u) = 0$ and $Q(v) = 0$, which form a system of linear equations with respect to $\{\alpha_1, \alpha_2, \alpha_4, \alpha_6\}$. And (16) solves the system. □

In fact, the function (15) has $3g = 6$ zeros on $\mathcal{V}$. Besides the sets (x_i, y_i), (z_i, w_i) it vanishes at two more points (s_i, t_i), $i = 1, 2$, coresponding to $w \in \mathrm{Jac}(\mathcal{V})$ under Abel's map. Then by the Abel's theorem $u + v + w = 0$. The addition law on $Jac(\mathcal{V})$ can be written as

$$\operatorname{rank}\begin{pmatrix} \mathbb{I}_2 & M(u) & \pi(u)\\ \mathbb{I}_2 & M(v) & \pi(v)\\ \mathbb{I}_2 & M(w) & \pi(w)\end{pmatrix} \leqslant 4 = 2g.$$

In the case of genus 2 curve it leads to (4).

Now we use (16) to obtain expressions for αs

$$\alpha_1 = 2\frac{\mathcal{G}_8(u,v)}{\mathcal{G}_7(u,v)}, \qquad \alpha_2 = \frac{\mathcal{G}_9(u,v)}{\mathcal{G}_7(u,v)},$$

where

$$\begin{aligned}
\mathcal{G}_7(u,v) &= \big(\wp_{1,3}(u)-\wp_{1,3}(v)\big)\big(\wp_{1,1,1}(u)-\wp_{1,1,1}(v)-\mu_1(\wp_{1,1}(u)-\wp_{1,1}(v))\big)\\
&\quad -\big(\wp_{1,1}(u)-\wp_{1,1}(v)\big)\big(\wp_{1,1,3}(u)-\wp_{1,1,3}(v)-\mu_1(\wp_{1,3}(u)-\wp_{1,3}(v))\big),\\
\mathcal{G}_8(u,v) &= \big(\wp_{1,3}(u)-\wp_{1,3}(v)\big)^2\\
&\quad +\big(\wp_{1,1}(u)-\wp_{1,1}(v)\big)\big(\wp_{1,3}(u)\wp_{1,1}(v)-\wp_{1,3}(v)\wp_{1,1}(u)\big),\\
\mathcal{G}_9(u,v) &= \big(\wp_{1,1}(u)^2-\wp_{1,1}(u)^2+\wp_{1,3}(u)-\wp_{1,3}(v)\big)\times\\
&\quad\times\big(\wp_{1,1,3}(u)-\wp_{1,1,3}(v)-\mu_1(\wp_{1,3}(u)-\wp_{1,3}(v))\big)\\
&\quad-\big(\wp_{1,1}(u)\wp_{1,3}(u)-\wp_{1,1}(v)\wp_{1,3}(v)\big)\times\\
&\quad\times\big(\wp_{1,1,1}(u)-\wp_{1,1,1}(v)-\mu_1(\wp_{1,1}(u)-\wp_{1,1}(v))\big).
\end{aligned}$$

Here we use basis functions $\wp_{1,1}$, $\wp_{1,3}$, $\wp_{1,1,1}$, $\wp_{1,1,3}$ of arguments u and v. It is enough to have α_1 α_2 to obtain the addition law, which is written for the same functions of $-w=u+v$.

In order to find addition law we expand (14) about infinity, where $\xi\to 0$, Since the relation holds for every ξ, we obtain an infinite sequence of equations, which are produced by a finite number of relations. Given a multi-index ν we denote $\mathfrak{p}_\nu=\wp_\nu(u)+\wp_\nu(v)+\wp_\nu(w)$ subject to $u+v+w=0$. In the case $\#\nu=1$ we have $\mathfrak{p}_i=-\zeta_i(u)-\zeta_i(v)-\zeta_i(w)$, $i=1,3$. So we are able to find all α_k in terms of $\mathfrak{p}_\nu$, namely

$$\alpha_1=-\mathfrak{p}_1, \tag{18a}$$

$$\alpha_2=-\frac{1}{2}\big(\mathfrak{p}_{1,1}-\mathfrak{p}_1^2-\mu_1\mathfrak{p}_1\big). \tag{18b}$$

Coefficient of ξ^{-3} gives the equation

$$\mathfrak{p}_3+\frac{1}{2}\mathfrak{p}_{1,1,1}=3\alpha_2\alpha_1-\alpha_1^3-\frac{1}{2}(\mu_1^2+4\mu_2)\alpha_1. \tag{19}$$

From (18a) and (19) we find addition formulas in Frobenius-Stikelberger form

$$\zeta_1(u+v)=\zeta_1(u)+\zeta_1(v)-\alpha_1, \tag{20a}$$

$$\begin{aligned}
\zeta_3(u+v)&=\zeta_3(u)+\zeta_3(v)-\frac{1}{2}\big(\wp_{1,1,1}(u)+\wp_{1,1,1}(v)\big)\\
&\quad-\frac{1}{2}\partial_{u_1}\partial_{v_1}\alpha_1+\alpha_1\big(3\alpha_2-\alpha_1^2-\frac{1}{2}(\mu_1^2+4\mu_2)\big).
\end{aligned} \tag{20b}$$

Appendix A. Expansion of sigma function

Sigma function related to curve (1) has the following expansion

$$\begin{aligned}\sigma(tu_1, t^3u_3) &= \left(u_3 - \frac{u_1^3}{3}\right)t^3 - \frac{1}{60}(\mu_1^2+4\mu_2)u_1^5t^5\\ &- \left(\frac{1}{24}(\mu_1\mu_3+2\mu_4)u_1^4u_3 + \frac{1}{2520}\big((\mu_1^2+4\mu_2)^2+(\mu_1\mu_3+2\mu_4)\big)u_1^7\right)t^7\\ &+ \Bigg(-\frac{1}{720}\big(8\mu_6+4\mu_1\mu_5+2\mu_3^2+(\mu_1^2+4\mu_2)(\mu_1\mu_3+2\mu_4)\big)u_3u_1^6\\ &- \frac{1}{24}(\mu_6+2\mu_1\mu_5+\mu_3^2)u_3^2(u_3-u_1^3) + \frac{1}{181440}\big(8(\mu_6+2\mu_1\mu_5+\mu_3^2)\\ &\qquad - 6(\mu_1^2+4\mu_2)(\mu_1\mu_3+2\mu_4)-(\mu_1^2+4\mu_2)^3\big)u_1^9\Bigg)t^9 + O(t^{11}).\end{aligned}$$

Also the expansion for sigma function related to $(2,5)$-curve (2) is given below, cf. [7, p. 124]

$$\begin{aligned}\sigma(tu_1, t^3u_3) &= \left(u_3 - \frac{u_1^3}{3}\right)t^3 - \left(\frac{\lambda_4}{12}u_1^4u_3 + \frac{\lambda_4}{1260}u_1^7\right)t^7\\ &+ \left(\frac{\lambda_6}{6}u_3^3 - \frac{\lambda_6}{6}u_3^2u_1^3 - \frac{\lambda_6}{90}u_3u_1^6 + \frac{\lambda_6}{5670}u_1^9\right)t^9 - \Bigg(\frac{\lambda_8}{6}u_3^3u_1^2 + \frac{\lambda_8}{30}u_3^2u_1^5\\ &+ \frac{\lambda_8}{1260}u_3u_1^8 + \frac{\lambda_4^2}{10080}u_1^8u_3 + \frac{\lambda_8}{24948}u_1^{11} + \frac{17\lambda_4^2}{1663200}u_1^{11}\Bigg)t^{11} + O(t^{13}).\end{aligned}$$

Appendix B. Relations between Abelian functions

Relations between Abelian functions defined on the Jacobian of $\mathcal{V}$ defined by (1) are obtained from the expansion of Klein formula as explained in Section 5

$$\begin{aligned}&(21a)\quad \wp_{1,1,1,1}(u) = 6\wp_{1,1}(u)^2 + 4\wp_{1,3}(u) + (\mu_1^2+4\mu_2)\wp_{1,1}(u)\\ &\qquad\qquad + 2\mu_4 + \mu_1\mu_3,\\ &(21b)\quad \wp_{1,1,1,3}(u) = 6\wp_{1,1}(u)\wp_{1,3}(u) - 2\wp_{3,3}(u) + (\mu_1^2+4\mu_2)\wp_{1,3}(u),\\ &(21c)\quad \wp_{1,1,3,3}(u) = 2\wp_{1,1}(u)\wp_{3,3}(u) + 4\wp_{1,3}(u)^2 + (2\mu_4+\mu_1\mu_3)\wp_{1,3}(u).\end{aligned}$$

$$\begin{aligned}&(22a)\quad \wp_{1,3,3}(u) = \wp_{1,3}(u)\wp_{1,1,1}(u) - \wp_{1,1}(u)\wp_{1,1,3}(u),\\ &\qquad \wp_{3,3,3}(u) = \big(2\wp_{1,3}\wp_{1,1} - \wp_{3,3} + \tfrac{1}{2}(\mu_1^2+4\mu_2)\wp_{1,3}\big)\wp_{1,1,1}(u)\\ &(22b)\qquad - \big(\wp_{1,3}(u) + 2\wp_{1,1}(u)^2 + \tfrac{1}{2}(\mu_1^2+4\mu_2)\wp_{1,1}(u)\\ &\qquad\qquad + \tfrac{1}{2}(\mu_1\mu_3+2\mu_4)\big)\wp_{1,1,3}(u).\end{aligned}$$

$$(23a)\quad \wp_{1,1,1}(u)^2 = 4\wp_{1,1}^3 + 4\wp_{1,1}\wp_{1,3} + 4\wp_{3,3} + (\mu_1^2+4\mu_2)\wp_{1,1}^2$$

$$+ (2\mu_1\mu_3 + 4\mu_4)\wp_{1,1} + 4\mu_6 + 2\mu_1\mu_5 + \mu_3^2,$$

$$\wp_{1,1,1}(u)\wp_{1,1,3}(u) = 4\wp_{1,1}^2\wp_{1,3} + 2\wp_{1,3}^2 - 2\wp_{1,1}\wp_{3,3} + (\mu_1^2 + 4\mu_2)\wp_{1,1}\wp_{1,3} + (\mu_1\mu_3 + 2\mu_4)\wp_{1,3} + 2\lambda_8 + \mu_3\mu_5, \tag{23b}$$

$$\wp_{1,1,3}(u)^2 = 4\wp_{1,1}\wp_{1,3}^2 - 4\wp_{1,3}\wp_{3,3} + (\mu_1^2 + 4\mu_2)\wp_{1,3}^2 + 4\mu_{10} + \mu_5^2. \tag{23c}$$

All relations are checked numerically with the expansion given in Appendix A

References

[1] V. M. Buchstaber, D. V. Leykin, *Polynomial Lie algebras*, Functional Anal. Appl., 36:4, 2002, 267–280.

[2] V. M. Buchstaber, D. V. Leykin, *Heat Equations in a Nonholonomic Frame*, Funct. Anal. Appl., 38:2, 2004, 88–101.

[3] V. M. Buchstaber, D. V. Leikin, *Differentiation of Abelian functions with respect to parameters*, Russian Math. Surveys, 62:4, 2007, 787–789.

[4] V. M. Buchstaber, D. V. Leikin, *Solution of the Problem of Differentiation of Abelian Functions over Parameters for Families of (n,s)-Curves*, Funct. Anal. Appl., 42:4, 2008, 268–278.

[5] ———, *Multiply Periodic Functions*, Cambridge Univ. Press, Cambridge, 1907.

[6] Eilbeck, J. C., Enolskii, V. Z., Previato, E. On a Generalized Frobenius-Stickelberger Addition Formula. Letters in Mathematical Physics, **63**:1 (2003), 5–17.

[7] V. M. Buchstaber, D. V. Leikin, *Addition Laws on Jacobian Varieties of Plane Algebraic Curves*, Proc. Steklov Inst. Math., 251, 2005, 49–120.

[8] V. M. Buchstaber, V. Z. Enolski, D. V. Leykin, *Multi-Dimensional Sigma-Functions*, arXiv: 1208.0990, 2012, 267 pp.

[9] Bernatska J., Leykin D. On Regularization of Second Kind Integrals, SIGMA, Vol. 14 (2018), 074, 28 pp.

[10] Baker H. F. *On the Hyperelliptic Sigma Functions*, American Journal of Mathematics Vol. 20, No. 4 (1898), pp. 301–384.