HAL open science

Computing period matrices and the Abel-Jacobi map of superelliptic curves

Pascal Molin, Christian Neurohr

To cite this version:

Pascal Molin, Christian Neurohr. Computing period matrices and the Abel-Jacobi map of superelliptic curves. Mathematics of Computation, 2019. hal-02416012

HAL Id: hal-02416012

https://inria.hal.science/hal-02416012v1

Submitted on 17 Dec 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Computing period matrices and the Abel-Jacobi map of superelliptic curves

Pascal Molin [*], Christian Neurohr [†]

September 2017

Abstract

We present an algorithm for the computation of period matrices and the Abel-Jacobi map of complex superelliptic curves given by an equation $y^m = f(x)$. It relies on rigorous numerical integration of differentials between Weierstrass points, which is done using Gauss method if the curve is hyperelliptic ($m = 2$) or the Double-Exponential method. The algorithm is implemented and makes it possible to reach thousands of digits accuracy even on large genus curves.

1 Introduction

The Abel-Jacobi map links a complex curve to a complex torus. In particular the matrix of periods allows to define the Riemann theta function of the curve, which is an object of central interest in mathematics and physics: let us mention the theory of abelian functions or integration of partial differential equations.

In the context of cryptography and number theory, periods also appear in the BSD conjecture or as a tool to identify isogenies or to find curves having prescribed complex multiplication [25]. For such diophantine applications, it is necessary to compute integrals to large precision (say thousand digits) and to have rigorous results.

1.1 Existing algorithms and implementations

For genus 1 and 2, methods based on isogenies (AGM [8], Richelot [4], Borchardt mean [16]) make it possible to compute periods to arbitrary precision in almost linear time. However, these techniques scale very badly when the genus grows.

For modular curves, the modular symbols machinery and termwise integration of expansions of modular forms give excellent algorithms [18, §3.2].

For hyperelliptic curves of arbitrary genus, the Magma implementation due to van Wamelen [25] computes period matrices and the Abel-Jacobi map. However, it is limited in terms of precision (less than 2000 digits) and some bugs are experienced on certain configurations of branch points. The shortcomings of this implementation motivated our work. Using a different strategy (integration along a tree instead of around Voronoi cells) we obtain a much faster, more reliable algorithm and rigorous results.

For general algebraic curves, there is an implementation in Maple due to Deconinck and van Hoeij [9]. We found that this package is not suitable for high precision purposes.

We also mention the Matlab implementations due to Frauendiener and Klein for hyperelliptic curves [10] and for general algebraic curves [11].

Moreover, there is an implementation available in Sage (since version 8.0) due to Nils Bruin and Alexandre Zotine that generalizes van Wamelen's approach for hyperelliptic curves to general algebraic curves.

[*]IMJ-PRG & Université Paris 7, 8 place Aurélie Nemours, 75013 Paris – France
molin@math.univ-paris-diderot.fr

[†]Carl von Ossietzky Universität Oldenburg, Institut für Mathematik, 26129 Oldenburg – Germany
neurohrchristian@googlemail.com

1.2 Main result

This paper addresses the problem of computing period matrices and the Abel-Jacobi map of algebraic curves given by an affine equation of the form (see Definition 3.1)

$$y^m = f(x), \quad m > 1, f \in \mathbb{C}[x] \text{ separable of degree } \deg(f) = n \geq 3.$$

They generalize hyperelliptic curves and we refer to them as *superelliptic curves*.

We take advantage of their specific geometry to obtain the following (see Theorem 8.1)

Theorem 1.1. *Let $\mathcal{C}$ be a superelliptic curve of genus g defined by an equation $y^m = f(x)$ where f is separable of degree n. We can compute a basis of the period lattice to precision D using*

$$O(n(g + \log D)(g + D)^2 \log^{2+\varepsilon}(g + D)) \text{ binary operations,}$$

where $\varepsilon > 0$ is chosen so that the multiplication of precision D numbers has complexity $O(D \log^{1+\varepsilon} D)$ and the implied constant depends on the configuration of complex roots of f[1]*.*

There is no clear definition of superelliptic curves in the literature and some authors will allow f to be non-separable in their definition. In this paper, we rely on the fact that f has no multiple roots in several places. This restriction could be removed though, this is discussed in Section 10.2.1.

1.3 Rigorous implementation

The algorithm has been implemented in C using the Arb library [12]. This system represents a complex number as a floating point approximation plus an error bound, and automatically takes into account all precision loss occurring through the execution of the program. With this model we can certify the accuracy of the numerical results of our algorithm (up to human or even compiler errors, as usual).

Another implementation has been done in Magma [3]. Both are publicly available on github at `https://github.com/pascalmolin/hcperiods` [21].

1.4 Interface with the LMFDB

Having rigorous period matrices is a valuable input for the methods developed by Costa et al. [7] to compute endormorphism rings of Jacobians of hyperelliptic curves. During a meeting aimed at expanding the 'L-functions and modular forms database' [17, LMFDB] to include genus 3 curves, the Magma implementation of our algorithm was incorporated in their framework to successfully compute the endomorphism rings of Jacobians of $67,879$ hyperelliptic curves of genus 3, and confirm those of the $66,158$ genus 2 curves that are currently in the database (see [2, LMFDB]).

For these applications big period matrices were computed to 300 digits precision.

1.5 Structure of the paper

In Section 2 we briefly review the objects we are interested in, namely period matrices and the Abel-Jacobi map of nice algebraic curves. The ingredients to obtain these objects, a basis of holomorphic differentials and a homology basis, are made explicit in the case of superelliptic curves in Section 3. We give formulas for the computation of periods in Section 4 and explain how to obtain from them the standard period matrices using symplectic reduction. In Section 5 we give explicit formulas for the intersection numbers of our homology basis. For numerical integration we employ two different integration schemes that are explained in Section 6: the double-exponential integration and (in the case of hyperelliptic curves) Gauss-Chebychev integration. The actual computation of the Abel-Jacobi map is explained in detail in Section 7. In Section 8 we analyze the complexity of our algorithm and share some insights on the implementation. Section 9 contains some tables with running times to demonstrate the performance of the code. Finally, in Section 10 we conclude with an outlook on what can be done in the future.

[1] In this work it involves a factor $1/r \leq \max \left|\frac{x-y}{x-z}\right|$ for x, y, z roots of f (see Lemma 6.2). Note that this dependency can be weakened as discussed in Section 8.5.4.

1.6 Acknowledgements

The first author wants to thank the crypto team at Inria Nancy, where a first version of this work was carried out in the case of hyperelliptic curves. He also acknowledges the support from Partenariat Hubert Curien under grant 35487PL.

The second author wants to thank Steffen Müller and Florian Hess for helpful discussions. Moreover, he acknowledges the support from DAAD under grant 57212102.

2 The Abel-Jacobi map

We recall, without proof, the main objects we are interested in, and which will become completely explicit in the case of superelliptic curves. The exposition follows that of [24, Section 2].

2.1 Definition

Let $\mathcal{C}$ be a smooth irreducible projective curve of genus $g > 0$. Its space of holomorphic differentials $\Omega^1_{\mathcal{C}}$ has dimension g; let us fix a basis $\omega_1, \dots \omega_g$ and denote by $\bar{\omega}$ the vector $(\omega_1, \dots \omega_g)$.

For any two points $P, Q \in \mathcal{C}$ we can consider the vector integral $\int_P^Q \bar{\omega} \in \mathbb{C}^g$, whose value depends on the chosen path from P to Q.

In fact, the integral depends on the path up to homology, so we introduce the *period lattice* of $\mathcal{C}$

$$\Lambda = \left\{ \int_\gamma \omega_j, \gamma \in H_1(\mathcal{C}, \mathbb{Z}) \right\} \subset \mathbb{C}^g,$$

where $H_1(\mathcal{C}, \mathbb{Z}) \cong \mathbb{Z}^{2g}$ is the first homology group of the curve.

Now the integral

$$P, Q \mapsto \int_P^Q \bar{\omega} \in \mathbb{C}^g/\Lambda$$

is well defined, and the definition can be extended by linearity to the group of degree zero divisors

$$\mathrm{Div}^0(\mathcal{C}) = \left\{ \sum a_i P_i, a_i \in \mathbb{Z}, \sum a_i = 0 \right\}.$$

The Abel-Jacobi theorem states that one obtains a surjective map whose kernel is formed by the set $\mathrm{Prin}^0(\mathcal{C})$ of divisors of functions, so that the integration provides an explicit isomorphism

$$\mathcal{A} : \left\{ \begin{array}{ccc} \mathrm{Jac}(\mathcal{C}) = \mathrm{Div}^0(\mathcal{C}) / \mathrm{Prin}^0(\mathcal{C}) & \longrightarrow & \mathbb{C}^g/\Lambda \\ \sum_i [Q_i - P_i] & \mapsto & \sum_k \int_{P_i}^{Q_i} \bar{\omega} \mod \Lambda \end{array} \right.$$

between the Jacobian variety and the complex torus.

2.2 Explicit basis and standard matrices

Let us choose a symplectic basis of $H_1(\mathcal{C}, \mathbb{Z})$, that is two families of cycles α_i, β_j for $1 \leq i, j \leq g$ such that the intersections satisfy

$$(\alpha_i \circ \beta_j) = \delta_{i,j},$$

the other intersections all being zero.

We define the period matrices on those cycles

$$\Omega_A = \left(\int_{\alpha_j} \omega_i \right)_{1 \leq i,j \leq g} \text{ and } \Omega_B = \left(\int_{\beta_j} \omega_i \right)_{1 \leq i,j \leq g}$$

and call the concatenated matrix

$$\Omega = (\Omega_A, \Omega_B) \in \mathbb{C}^{g \times 2g}$$

such that $\Lambda = \Omega \mathbb{Z}^{2g}$ a *big period matrix*.

If one takes as basis of differentials the dual basis of the cycles α_j, the matrix becomes

$$\Omega_A^{-1} \Omega = (I_g, \tau),$$

where $\tau = \Omega_A^{-1} \Omega_B \in \mathbb{C}^{g \times g}$, called a *small period matrix*, is in the Siegel space $\mathcal{H}_g$ of symmetric matrices with positive definite imaginary part.

3 Superelliptic curves

3.1 Definition & properties

Definition 3.1. In this paper, a superelliptic curve $\mathcal{C}$ over $\mathbb{C}$ is a smooth projective curve that has an affine model given by an equation of the form

$$\mathcal{C}_{\text{aff}}: \quad y^m = f(x) = c_f \cdot \prod_{k=1}^{n}(x - x_k), \tag{1}$$

where $m > 1$ and $f \in \mathbb{C}[x]$ is separable of degree $n \geq 3$. Note that we do not assume that $\gcd(m, n) = 1$.

There are $\delta = \gcd(m, n)$ points $P_\infty^{(1)}, \ldots, P_\infty^{(\delta)} \in \mathcal{C}$ at infinity, that behave differently depending on m and n (see [22, §1] for details). In particular, $\infty \in \mathbb{P}^1_{\mathbb{C}}$ is a branch point for $\delta \neq m$. Thus, we introduce the set of finite branch points $X = \{x_1, \ldots, x_n\}$ as well as the set of all branch points

$$\hat{X} = \begin{cases} X \cup \{\infty\} & \text{if } m \nmid d, \\ X & \text{otherwise.} \end{cases} \tag{2}$$

The ramification indices at the branch points are given by $e_x = m$ for all $x \in X$ and $e_\infty = \frac{m}{\delta}$. Using the Riemann-Hurwitz formula, we obtain the genus of $\mathcal{C}$ as

$$g = \frac{1}{2}((m-1)(n-1) - \delta + 1). \tag{3}$$

We denote the corresponding finite ramification points $P_k = (x_k, 0) \in \mathcal{C}$ for $k = 1, \ldots, n$.

Remark 3.2. Without loss of generality we may assume $c_f = 1$ (if not, apply the transformation $(x, y) \mapsto (x, \sqrt[m]{c_f}y)$).

Remark 3.3. For any $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}(2, \mathbb{C})$, the Moebius transform $\phi : u \mapsto \frac{au+b}{cu+d}$ is an automorphism of $\mathbb{P}^1$. By a change of coordinate $x = \phi(u)$ we obtain a different model of $\mathcal{C}$ given by the equation

$$\tilde{v}^m = \tilde{f}(u)$$

where $\tilde{f}(u) = f(\phi(u))(cu + d)^{\ell m}$ and $v = y(cu + d)^\ell$ for the smallest value ℓ such that $\ell m \geq n$.

If the curve was singular at infinity, the singularity is moved to $u = -d/c$ in the new model. This happens when $\delta < m$ (so that $\ell m > n$).

When $\delta = m$ we may apply such a transformation to improve the configuration of affine branch points.

3.2 Complex roots and branches of the curve

3.2.1 The complex m-th root

Working over the complex numbers we encounter several multi-valued functions which we will briefly discuss here. Closely related to superelliptic curves over $\mathbb{C}$ is the complex m-th root. Before specifying a branch it is a multi-valued function $y^m = x$ that defines an m-sheeted Riemann surface, whose only branch points are at $x = 0, \infty$, and these are totally ramified.

For $x \in \mathbb{C}$, it is natural and computationally convenient to use the *principal branch* of the m-th root $\sqrt[m]{x}$ defined by

$$-\frac{\pi}{m} < \arg(\sqrt[m]{x}) \leq \frac{\pi}{m}$$

which has a branch cut along the negative real axis $]-\infty, 0]$. Crossing it in positive orientation corresponds to multiplication by the primitive m-th root of unity

$$\zeta := \zeta_m := e^{\frac{2\pi i}{m}}.$$

on the surface. In particular, the monodromy at $x = 0$ is cyclic of order m.

3.2.2 The Riemann surface

For an introduction to the theory of Riemann surfaces, algebraic curves and holomorphic covering maps we recommend [19].

Over $\mathbb{C}$ we can identify the curve $\mathcal{C}$ with the compact Riemann surface $\mathcal{C}(\mathbb{C})$. Since our defining equation has the nice form $y^m = \prod_{k=1}^{n}(x - x_k)$ it is compelling to do all computations in the x-plane. We denote by $\mathrm{pr_x} : \mathcal{C} \to \mathbb{P}^1_{\mathbb{C}}$ the corresponding smooth cyclic branched covering of degree m of the projective line that is defined by the x-coordinate.

There are m possibilities to lift a path in x-plane to $\mathcal{C}(\mathbb{C})$ using analytic continuation, which is crucial for the integration of differentials on $\mathcal{C}$. Due to the cyclic structure of $\mathcal{C}$, these lifts are related in a convenient way:

We call a *branch of* $\mathcal{C}$ a function $y(x)$ such that $y(x)^m = f(x)$ for all $x \in \mathbb{C}$. At every x, the branches of $\mathcal{C}$ only differ by a factor ζ^l for some $l \in \{0, \dots, m-1\}$. Thus, following a path, it is sufficient to know *one* branch that is analytic in a suitable neighborhood. In the next paragraph, we will introduce locally analytic branches very explicitly.

We obtain an ordering of the sheets relative to the analytic branches of $\mathcal{C}$ by imposing that multiplication by ζ, i.e. applying the map $(x, y(x)) \mapsto (x, \zeta y(x))$, corresponds to moving one sheet up on the Riemann surface.

The local monodromy of the covering $\mathrm{pr_x}$ is cyclic of order m and equal for all $x_k \in X$ and the monodromy group is, up to conjugation, the cyclic group C_m. This makes it possible to find explicit generators for the homology group $H_1(\mathcal{C}, \mathbb{Z})$ without specifying a base point, as shown in §3.3.

3.2.3 Locally analytic branches

In order to integrate differential forms on $\mathcal{C}$ it is sufficient to be able to follow *one* explicit analytic continuation of y along a path joining two branch points $a, b \in X$.

One could of course consider the *principal branch* of the curve

$$y(x) = \sqrt[m]{f(x)},$$

but this is not a good model to compute with: it has discontinuities along the curves $f^{-1}(]-\infty, 0])$, all wandering around the x-plane in an unpredictable way (see Figure 1a). These are the *branch cuts* of $y(x)$, crossing them in positive direction requires multiplying by ζ in order to follow an analytic continuation.

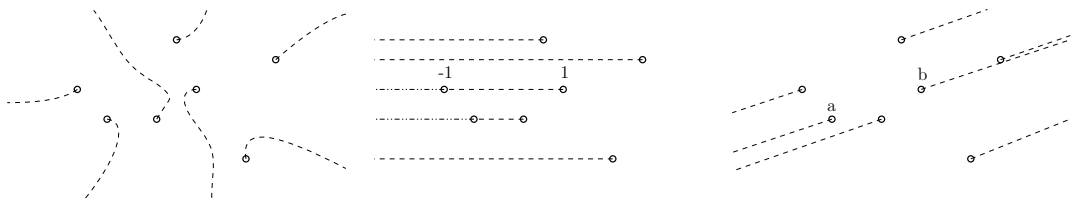
A better option is to split the product as follows: assume that $(a, b) = (-1, 1)$. Then the function

$$y(x) = \prod_{x_k \in X} \sqrt[m]{x - x_k}$$

has n branch cuts parallel to the real line (see Figure 1b). However, one of them lies exactly on the interval $[-1, 1]$ we are interested in. We work around this by taking the branch cut towards $+\infty$ for each branch point x_k with positive real part, writing

$$y(x) = e^{\frac{i\pi r^+}{m}} \prod_{\mathrm{Re}(x_k) \le 0} \sqrt[m]{x - x_k} \prod_{\mathrm{Re}(x_k) > 0} \sqrt[m]{x_k - x},$$

where r^+ is the number of points with positive real part.



(a) principal branch (b) product (c) $y_{a,b}$

Figure 1: Branch cuts of different m-th roots.

In general we proceed in the same way: For branch points $a, b \in X$ we consider the affine linear transformation

$$x_{a,b} : u \mapsto \frac{b-a}{2}\left(u + \frac{b+a}{b-a}\right),$$

which maps $[-1, 1]$ to the complex line segment $[a, b]$, and denote the inverse map by

$$u_{a,b} : x \mapsto \frac{2x-a-b}{b-a}.$$

We split the image of the branch points under $u_{a,b}$ into the following subsets

$$\{u_{a,b}(x), x \in X\} = \{-1, 1\} \cup U^+ \cup U^-, \tag{4}$$

where points in U^+ (resp. U^-) have strictly positive (resp. non-positive) real part.

Then the product

$$\tilde{y}_{a,b}(u) = \prod_{u_k \in U^-} \sqrt[m]{u - u_k} \prod_{u_k \in U^+} \sqrt[m]{u_k - u} \tag{5}$$

is holomorphic on a neighborhood $\varepsilon_{a,b}$ of $[-1, 1]$ which we can take as an ellipse [2] containing no point $u_k \in U^- \cup U^+$, while the term corresponding to a, b

$$\sqrt[m]{1 - u^2}$$

has two branch cuts $]-\infty, -1]$ and $[1, \infty[$, and is holomorphic on the complement $\overline{U}$ of these cuts.

We can now define a branch of the curve

$$y_{a,b}(x) = C_{a,b}\tilde{y}_{a,b}(u_{a,b}(x)) \sqrt[m]{1 - u_{a,b}(x)^2} \tag{6}$$

by setting $r = 1 + \#U^+ \bmod 2$ and choosing[3] the constant

$$C_{a,b} = \left(\frac{b-a}{2}\right)^{\frac{n}{m}} e^{\frac{\pi i}{m} r} \tag{7}$$

such that $y_{a,b}(x)^m = f(x)$.

The function $y_{a,b}(x)$ has n branch cuts all parallel to $[a, b]$ in outward direction and is holomorphic inside $]a, b[$ (see Figure 1c).

More precisely, $V_{a,b} = x_{a,b}(\varepsilon_{a,b} \cap \overline{U})$, is an ellipse-shaped neighborhood of $]a, b[$ with two segments removed (see Figure 2) on which the local branch $y_{a,b}$ is well defined and holomorphic.

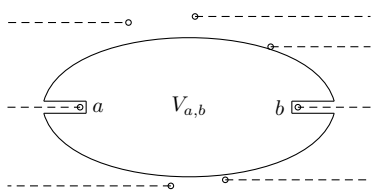


Figure 2: Holomorphic neighborhood of $y_{a,b}$.

We sum up the properties of these local branches:

Proposition 3.4. *Let $a, b \in X$ be branch points such that $X \cap]a, b[= \varnothing$. Then, with the notation as above, the functions $\tilde{y}_{a,b}$ (5) and $y_{a,b}$ (6) satisfy*

- *$\tilde{y}_{a,b}$ is holomorphic and does not vanish on $\varepsilon_{a,b}$,*
- *$y_{a,b}(x) = C_{a,b}\tilde{y}_{a,b}(u_{a,b}(x)) \sqrt[m]{1 - u_{a,b}(x)^2}$ is holomorphic on $V_{a,b}$,*
- *$y_{a,b}(x)^m = f(x)$ for all $x \in \mathbb{C}$,*
- *$y_{a,b}(x), \zeta y_{a,b}(x), \ldots, \zeta^{m-1} y_{a,b}(x)$ are the m different analytic continuations of y on $V_{a,b}$.*

Moreover, we can assume that for $x \in V_{a,b}$, applying the map $(x, y_{a,b}(x)) \mapsto (x, \zeta^l y_{a,b}(x))$ corresponds to moving up $l \in \mathbb{Z}/m\mathbb{Z}$ sheets on the Riemann surface.

[2] we will exhibit such a neighborhood in Section 6.2

[3] any choice of the m-th root is valid here

3.3 Cycles and homology

For us, a *cycle* on $\mathcal{C}$ is a smooth oriented closed path in $\pi_1(\mathcal{C})$. For simplicity we identify all cycles with their homology classes in $H_1(\mathcal{C},\mathbb{Z}) = \pi_1(\mathcal{C})/[\pi_1(\mathcal{C}),\pi_1(\mathcal{C})]$.

In the following we present an explicit generating set of $H_1(\mathcal{C},\mathbb{Z})$ that relies on the locally analytic branches $y_{a,b}$ as defined in (6) and the superelliptic structure of $\mathcal{C}$.

Let $a, b \in X$ be branch points such that $X \cap]a,b[= \varnothing$, where $[a,b]$ is the oriented line segment connecting a and b.

By Proposition 3.4 the lifts of $[a,b]$ to $\mathcal{C}$ are given by

$$\gamma^{(l)}_{[a,b]} = \{(x, \zeta^l y_{a,b}(x)) \mid x \in [a,b]\}, \quad l \in \mathbb{Z}/m\mathbb{Z}.$$

Similarly, we obtain lifts of $[b,a]$ by reversing the orientation of $\gamma^{(l)}_{[a,b]}$. We denote

$$-\gamma^{(l)}_{[a,b]} = \{(x, \zeta^l y_{a,b}(x)) \mid x \in [b,a]\}, \quad l \in \mathbb{Z}/m\mathbb{Z}.$$

These are smooth oriented paths that connect $P_a = (a,0)$ and $P_b = (b,0)$ on $\mathcal{C}$. We obtain cycles by concatenating these lifts in the following way:

$$\gamma^{(l)}_{a,b} = \gamma^{(l)}_{[a,b]} \cup -\gamma^{(l+1)}_{[a,b]} \in \pi_1(\mathcal{C}). \tag{8}$$

Definition 3.5 (Elementary cycles)**.** We say $\gamma_{a,b} = \gamma^{(0)}_{a,b}$ is an *elementary cycle* and call $\gamma^{(l)}_{a,b}$ its *shifts* for $l \in \mathbb{Z}/m\mathbb{Z}$.

In $\pi_1(\mathcal{C})$ shifts of elementary cycles are homotopic to cycles that encircle a in negative and b in positive orientation, once each and do not encircle any other branch point. This is possible because we can always find an open neighborhood V of $[a,b]$ such that $V \cap X = \{a,b\}$ and thus the homotopy class of a cycle is not changed by deformations within V. By definition of $y_{a,b}$ the branch cuts at the end points are outward and parallel to $[a,b]$. Thus, we have the following useful visualizations of $\gamma^{(l)}_{a,b}$ on $\mathcal{C}$:

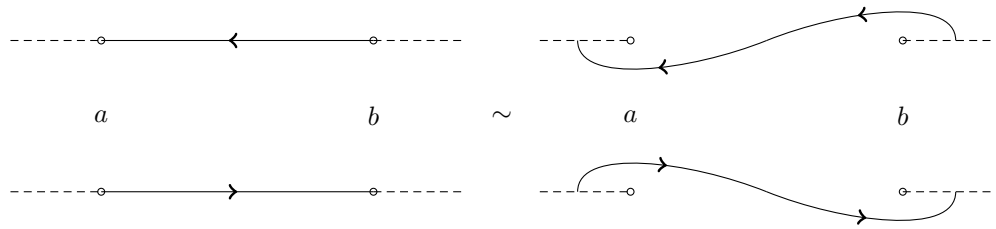


Figure 3: Homotopic representations of a cycle $\gamma^{(l)}_{a,b}$.

As it turns out, we do not need all elementary cycles and their shifts to generate $H_1(\mathcal{C},\mathbb{Z})$, but only those that correspond to edges in a *spanning tree*, that is a subset $E \in X \times X$ of directed edges (a,b) such that all branch points are connected without producing any cycle. It must contain exactly $n-1$ edges. The actual tree will be chosen in §4.3 in order to minimize the complexity of numerical integration.

For an edge $e = (a,b) \in E$, we denote by $\gamma^{(l)}_e$ the shifts of the corresponding elementary cycle $\gamma_{a,b}$.

Theorem 3.6. *Let E be a spanning tree for the branch points X. The set of cycles $\Gamma = \left\{\gamma^{(l)}_e \mid 0 \le l < m-1, e \in E\right\}$ generates $H_1(\mathcal{C},\mathbb{Z})$.*

Proof. Denote by $\alpha_a \in \pi_1(\mathbb{P}^1 \setminus \hat{X})$ a closed path that encircles the branch point $a \in \hat{X}$ exactly once. Then, due to the relation $1 = \prod_{a\in\hat{X}} \alpha_a$, $\pi_1(\mathbb{P}^1 \setminus \hat{X})$ is freely generated by $\{\alpha_a\}_{a\in X}$, i.e. in the case $\delta \neq m$ we can omit α_∞.

Since our covering is cyclic, we have that $\pi_1(\mathcal{C}\setminus {\mathrm{pr_x}}^{-1}(\hat{X})) \cong \ker(\pi_1(\mathbb{P}^1\setminus\hat{X}) \xrightarrow{\Phi} \mathrm{Aut}(\mathcal{C}\setminus {\mathrm{pr_x}}^{-1}(\hat{X})))$ where $\mathrm{Aut}(\mathcal{C}\setminus {\mathrm{pr_x}}^{-1}(\hat{X})) \cong C_m \subset S_m$ and $\Phi(\alpha_a)$ is cyclic of order m for all $a \in X$. Hence, for every word $\alpha = \alpha_1^{s_1}\dots\alpha_n^{s_n} \in \pi_1(\mathbb{P}^1\setminus\hat{X})$ we have that $\alpha \in \ker(\Phi) \Leftrightarrow \sum_{i=1}^n s_i \equiv 0 \bmod m$.

We now claim that $\pi_1(\mathcal{C}\setminus {\mathrm{pr_x}}^{-1}(\hat{X})) = \langle \alpha_a^{-s}\alpha_b^s, \alpha_a^m \mid s\in\mathbb{Z}, a,b\in X\rangle$ and prove this by induction on n: for $\alpha = \alpha_1^{s_1}$, m divides s_1 and therefore α is generated by α_1^m. For $n > 1$ we write $\alpha = \alpha_1^{s_1}\dots\alpha_n^{s_n} = (\alpha_1^{s_1}\dots\alpha_{n-1}^{s_{n-1}+s_n})(\alpha_{n-1}^{-s_n}\alpha_n^{s_n})$.

We obtain the fundamental group of $\mathcal{C}$ as $\pi_1(\mathcal{C}) \cong \pi_1(\mathcal{C}\setminus {\mathrm{pr_x}}^{-1}(\hat{X}))/\langle \alpha_a^{e_a} \mid a\in\hat{X}\rangle$, which is generated by $\{\alpha_a^{-s}\alpha_b^s \mid s\in\mathbb{Z}/m\mathbb{Z}, a,b\in X\}$.

All branch points $a,b\in X$ are connected by a path $(a, v_1,\dots,v_t,b)$ in the spanning tree, so we can write $\alpha_a^{-s}\alpha_b^s = (\alpha_a^{-s}\alpha_{v_1}^s)(\alpha_{v_1}^{-s}\alpha_{v_2}^s)\dots(\alpha_{v_{t-1}}^{-s}\alpha_{v_t}^s)(\alpha_{v_t}^{-s}\alpha_b^s)$ and hence we have that $\{\alpha_a^{-s}\alpha_b^s \mid s\in\mathbb{Z}/m\mathbb{Z}, (a,b)\in E\}$ generates $\pi_1(\mathcal{C})$ and therefore $H_1(\mathcal{C},\mathbb{Z})$.

If we choose basepoints $p_0\in\mathbb{P}^1\setminus\hat{X}$ for $\pi_1(\mathbb{P}^1\setminus\hat{X})$ and $P_0\in {\mathrm{pr_x}}^{-1}(p_0)$ for $\pi_1(\mathcal{C}\setminus {\mathrm{pr_x}}^{-1}(\hat{X}))$ and $\pi_1(\mathcal{C})$ respectively, then, depending on the choice of P_0, for all $e=(a,b)\in E$ there exists $l_0\in\mathbb{Z}/m\mathbb{Z}$ such that $\gamma_e^{(l_0)}$ is homotopic to $\alpha_a^{-1}\alpha_b$ in $\pi_1(\mathcal{C},P_0)$. In $H_1(\mathcal{C},\mathbb{Z})$ we have that $\alpha_a^{-s}\alpha_b^s = (\alpha_a^{-1}\alpha_b)^s$, so we obtain the other powers by concatenating the shifts $\prod_{l=0}^{s-1}\gamma_e^{(l_0+l)} = (\alpha_a^{-1}\alpha_b)^s$. This implies $1 = \prod_{l=0}^{m-1}\gamma_e^{(l_0+l)} = \prod_{l=0}^{m-1}\gamma_e^{(l)}$ and

$$\{\alpha_a^{-s}\alpha_b^s \mid s\in\mathbb{Z}/m\mathbb{Z}\} \subset \langle \gamma_e^{(l)} \mid 0\le l < m-1\rangle,$$

and therefore $H_1(\mathcal{C},\mathbb{Z}) = \langle\Gamma\rangle$. □

Remark 3.7.
- For $\delta = 1$, we have that $\#\Gamma = (m-1)(n-1) = 2g$. Therefore, Γ is a basis for $H_1(\mathcal{C},\mathbb{Z})$ in that case.
- In the case $\delta = m$, the point at infinity is not a branch point. Leaving out one finite branch point in the spanning tree results in only $n-2$ edges. Hence, we easily find a subset $\Gamma'\subset\Gamma$ such that $\#\Gamma' = (m-1)(n-2) = 2g$ and Γ' is a basis for $H_1(\mathcal{C},\mathbb{Z})$.

3.4 Differential forms

The computation of the period matrix and the Abel-Jacobi map requires a basis of $\Omega^1_{\mathcal{C}}$ as a $\mathbb{C}$-vector space. In this section we provide a basis that only depends on m and n and is suitable for numerical integration.

Among the meromorphic differentials

$$\mathcal{W}^{\mathrm{mer}} = \{\omega_{i,j}\}_{\substack{1\le i\le n-1,\\ 1\le j\le m-1}} \quad \text{with} \quad \omega_{i,j} = \frac{x^{i-1}\mathrm{d}x}{y^j},$$

there are exactly g that are holomorphic and they can be found by imposing a simple combinatorial condition on i and j. The following proposition is basically a more general version of [22, Proposition 2].

Proposition 3.8. *Let $\delta = \gcd(m,n)$. The following differentials form a $\mathbb{C}$-basis of $\Omega^1_{\mathcal{C}}$:*

$$\mathcal{W} = \{\omega_{i,j}\in\mathcal{W}^{mer} \mid -mi + jn - \delta \ge 0\}$$

Proof. First we show that the differentials in $\mathcal{W}$ are holomorphic. Let $\omega_{i,j} = x^{i-1}y^{-j}\mathrm{d}x \in \mathcal{W}^{\mathrm{mer}}$. We write down the relevant divisors

$$\mathrm{div}(x) = \sum_{k=1}^m \left(0, \zeta^k \sqrt[m]{f(0)}\right) - \frac{m}{\delta}\cdot\sum_{l=1}^{\delta} P_\infty^{(l)},$$

$$\mathrm{div}(y) = \sum_{k=1}^n P_k - \frac{n}{\delta}\cdot\sum_{l=1}^{\delta} P_\infty^{(l)},$$

$$\mathrm{div}(\mathrm{d}x) = (m-1)\sum_{k=1}^n P_k - \left(\frac{m}{\delta}+1\right)\cdot\sum_{l=1}^{\delta} P_\infty^{(l)}.$$

Putting together the information, for $P \in \mathcal{C}$ lying over $x_0 \in \mathbb{P}^1_{\mathbb{C}}$, we obtain

$$v_P(\omega_{i,j}) = (i-1)v_P(x) + v_P(\mathrm{d}x) - jv_P(y) = \begin{cases} \geq 0 & \text{if } x_0 \neq x_k, \infty, \\ m-1-j \geq 0 & \text{if } x_0 = x_k, \\ \frac{(-mi-\delta+jn)}{\delta} & \text{if } x_0 = \infty. \end{cases} \tag{9}$$

We conclude: $\omega_{i,j} \in \mathcal{W}^{\mathrm{mer}}$ is holomorphic if and only if $\omega_{i,j} \in \mathcal{W}$.
Since the differentials in $\mathcal{W}$ are clearly $\mathbb{C}$-linearly independent, it remains to show that there are enough of them, i.e. $\#\mathcal{W} = g$.

Counting the elements in $\mathcal{W}$ corresponds to counting lattice points $(i,j) \in \mathbb{Z}^2$ in the trapezoid given by the faces

$$\begin{aligned} 1 \leq i \leq n-1, \\ 1 \leq j \leq m-1, \\ i \leq \frac{n}{m}j - \frac{\delta}{m}. \end{aligned}$$

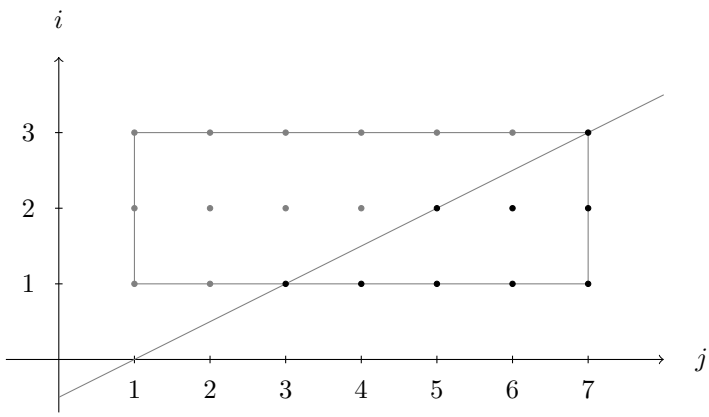


Figure 4: The points below the line correspond to holomorphic differentials. Illustrated is the case $n = 4, m = 8$, and thus $g = 9$.

Summing over the vertical lines of the trapezoid (see Figure 4), we find the following formula that counts the points.

$$\#\mathcal{W} = \sum_{j=1}^{m-1} \left\lfloor \frac{n}{m}j - \frac{\delta}{m} \right\rfloor = \sum_{j=1}^{m-1} \frac{nj - \delta - r_j}{m} = \frac{n}{m}\sum_{j=1}^{m-1} j - \frac{m-1}{m}\delta - \frac{1}{m}\sum_{j=1}^{m-1} r_j, \tag{10}$$

where $r_j = nj - \delta \bmod m$.

The desired equality $\#\mathcal{W} = \frac{1}{2}((n-1)(m-1) - \delta + 1) = g$ immediately follows from

Lemma 3.9.

$$\sum_{j=1}^{m-1} r_j = \frac{1}{2}(m^2 - (\delta+2)m + 2\delta).$$

Proof. Let $l := \frac{m}{\delta}$. First we note that $r_j = r_{j+l}$:

$$r_{j+l} = n(j+l) - \delta \bmod m = nj + \frac{n}{\delta}m - \delta \bmod m = nj - \delta \bmod m = r_j,$$

and hence

$$\sum_{j=1}^{m-1} r_j = \delta \cdot \sum_{j=1}^{l} r_j - r_m = \delta \cdot \sum_{j=1}^{l} r_j - (-\delta + m). \tag{11}$$

Furthermore, r_j can be written as a multiple of δ:

$$r_j = \delta\left(\frac{n}{\delta}j - 1\right) \bmod m.$$

From $\gcd(\frac{n}{\delta}, l) = 1$ we conclude $\left\{\frac{n}{\delta}j - 1 \bmod l \mid 1 \le j \le l\right\} = \{0, \dots, l-1\}$. Therefore,

$$\sum_{j=1}^{l} r_j = \sum_{j=0}^{l-1} \delta j = \delta \cdot \frac{l(l-1)}{2}, \tag{12}$$

and thus (11) and (12) imply

$$\sum_{j=1}^{m-1} r_j = \delta \cdot \sum_{j=1}^{l} r_j + \delta - m = \delta^2 \cdot \frac{l(l-1)}{2} + \delta - m = \frac{1}{2}(m^2 - (\delta+2)m + 2\delta).$$

□

Remark 3.10.

- Note that from (9) it follows that the meromorphic differentials in $\mathcal{W}^{\text{mer}}$ are homolorphic at all finite points.
- In practice we order the differentials in $\mathcal{W}$ lexicographically by j, i:

$$\omega_{i,j} < \omega_{\tilde{i},\tilde{j}} \quad \text{iff.} \quad j < \tilde{j} \text{ or } (j = \tilde{j} \text{ and } i < \tilde{i}).$$

4 Strategy for the period matrix

In this section we present our strategy to obtain period matrices $\Omega_\Gamma, \Omega_A, \Omega_B$ and τ as defined in §2.2. Although this paper is not restricted to the case $\gcd(m, n) = 1$, we will briefly assume it in this paragraph to simplify notation.

The main ingredients were already described in Section 3: we integrate the holomorphic differentials in $\mathcal{W}$ (§3.4) over the cycles in Γ (§3.3) using numerical integration (§6.1), which results in a period matrix (§4.1)

$$\Omega_\Gamma = \left(\int_\gamma \omega\right)_{\substack{\omega \in \mathcal{W}, \\ \gamma \in \Gamma}} \in \mathbb{C}^{g \times 2g}.$$

The matrices Ω_A and Ω_B require a symplectic basis of $H_1(\mathcal{C}, \mathbb{Z})$. So, we compute the intersection pairing on Γ, as explained in Section 5, which results in a intersection matrix $K_\Gamma \in \mathbb{Z}^{2g \times 2g}$. After computing a symplectic base change $S \in \mathrm{GL}(\mathbb{Z}, 2g)$ for K_Γ (§4.4), we obtain a big period matrix

$$(\Omega_A, \Omega_B) = \Omega_\Gamma S, \tag{13}$$

and finally a small period matrix in the Siegel upper half-space

$$\tau = \Omega_A^{-1}\Omega_B \in \mathfrak{H}_g. \tag{14}$$

4.1 Periods of elementary cycles

The following theorem provides a formula for computing the periods of the curve. It relates integration of differential forms on the curve to numerical integration in $\mathbb{C}$.

Note that the statement is true for all differentials in $\mathcal{W}^{\text{mer}}$, not just the holomorphic ones. We continue to use the notation from Section 3.

Theorem 4.1. *Let $\gamma_e^{(l)} \in \Gamma$ be a shift of an elementary cycle corresponding to an edge $e = (a, b) \in E$. Then, for all differentials $\omega_{i,j} \in \mathcal{W}^{mer}$, we have*

$$\int_{\gamma_e^{(l)}} \omega_{i,j} = \zeta^{-lj}(1 - \zeta^{-j}) C_{a,b}^{-j} \left(\frac{b-a}{2}\right)^i \int_{-1}^{1} \frac{\varphi_{i,j}(u)}{(1-u^2)^{\frac{j}{m}}} \mathrm{d}u, \tag{15}$$

where

$$\varphi_{i,j} = \left(u + \frac{b+a}{b-a}\right)^{i-1} \tilde{y}_{a,b}(u)^{-j}$$

is holomorphic in a neighbourhood $\epsilon_{a,b}$ *of* $[-1,1]$.

Proof. By the definition in (8) we can write $\gamma_e^{(l)} = \gamma_{[a,b]}^{(l)} \cup \gamma_{[b,a]}^{(l+1)}$. Hence we split up the integral and compute

$$\begin{aligned}\int_{\gamma_{[a,b]}^{(l)}} \omega_{i,j} &= \int_{\gamma_{[a,b]}^{(l)}} \frac{x^{i-1}}{y^j}\mathrm{d}x = \zeta^{-lj}\int_a^b \frac{x^{i-1}}{y_{a,b}(x)^j}\mathrm{d}x \\ &= \zeta^{-lj} C_{a,b}^{-j} \int_a^b \frac{x^{i-1}}{\tilde{y}_{a,b}(u_{a,b}(x))^j (1-u_{a,b}(x)^2)^{\frac{j}{m}}}\mathrm{d}x.\end{aligned}$$

Applying the transformation $x \mapsto x_{a,b}(u)$ introduces the derivative $\mathrm{d}x = \left(\frac{b-a}{2}\right)\mathrm{d}u$ yields

$$\begin{aligned}\int_{\gamma_{[a,b]}^{(l)}} \omega_{i,j} &= \zeta^{-lj} C_{a,b}^{-j}\left(\frac{b-a}{2}\right)\int_{-1}^1 \frac{x_{a,b}(u)^{i-1}}{\tilde{y}_{a,b}(u)^j(1-u^2)^{\frac{j}{m}}}\mathrm{d}u \\ &= \zeta^{-lj} C_{a,b}^{-j}\left(\frac{b-a}{2}\right)^i \int_{-1}^1 \frac{\left(u+\frac{b+a}{b-a}\right)^{i-1}}{\tilde{y}_{a,b}(u)^j(1-u^2)^{\frac{j}{m}}}\mathrm{d}u\end{aligned}$$

Similarly, we obtain

$$\int_{\gamma_{[b,a]}^{(l+1)}} w_{i,j} = -\zeta^{-j}\int_{\gamma_{[a,b]}^{(l)}} w_{i,j}.$$

By Proposition 3.4, $\tilde{y}_{a,b}$ is holomorphic and has no zero on $\epsilon_{a,b}$, therefore $\varphi_{i,j} = \left(u+\frac{b+a}{b-a}\right)^{i-1}\tilde{y}_{a,b}(u)^{-j}$ is holomorphic on $\epsilon_{a,b}$. □

4.2 Numerical integration

In order to compute a period matrix Ω_Γ the only integrals that have to be numerically evaluated are the *elementary integrals*

$$\int_{-1}^1 \frac{\varphi_{i,j}(u)}{(1-u^2)^{\frac{j}{m}}}\mathrm{d}u \tag{16}$$

for all $\omega_{i,j} \in \mathcal{W}$ and $e \in E$. By Theorem 4.1, all the periods in Ω_Γ are then obtained by multiplication of elementary integrals with constants.

As explained in §8.4.2, the actual computations will be done on integrals of the form

$$I_{a,b}(i,j) = \int_{-1}^1 \frac{u^{i-1}\mathrm{d}u}{(1-u^2)^{\frac{j}{m}}\tilde{y}_{a,b}(u)^j} \tag{17}$$

(that is, replacing $(u+\frac{b+a}{b-a})^{i-1}$ by u^{i-1} in the numerator of $\varphi_{i,j}$), the value of elementary integrals being recovered by the polynomial shift

$$\int_{-1}^1 \frac{\varphi_{i,j}(u)}{(1-u^2)^{\frac{j}{m}}}\mathrm{d}u = \sum_{l=0}^{i-1}\binom{i-1}{l}\left(\frac{b+a}{b-a}\right)^{i-1-l} I_{a,b}(l,j). \tag{18}$$

The rigorous numerical evaluation of (17) is addressed in Section 6: for any edge (a,b), Theorems 6.3 and 6.9 provide explicit schemes allowing to attain any prescribed precision.

4.3 Minimal spanning tree

From the a priori analysis of all numerical integrals $I_{a,b}$ along the interval $[a,b]$, we choose an optimal set of edges forming a spanning tree as follows:

- Consider the complete graph on the set of finite branch points $G' = (X, E')$ where $E' = \{(a,b) \mid a,b \in X\}$.

- Each edge $e = (a, b) \in E'$ gets assigned a capacity r_e that indicates the cost of numerical integration along the interval $[a, b]$.
- Apply a standard 'maximal-flow' algorithm from graph theory, based on a greedy approach. This results in a spanning tree $G = (X, E)$, where $E \subset E'$ contains the $n-1$ best edges for integration that connect all vertices without producing cycles.

Note that the integration process is most favourable between branch points that are far away from the others (this notion is made explicit in Section 6).

4.4 Symplectic basis

By definition, a big period matrix (Ω_A, Ω_B) requires integration along a symplectic basis of $H_1(\mathcal{C}, \mathbb{Z})$. In §3.3 we gave a generating set Γ for $H_1(\mathcal{C}, \mathbb{Z})$, namely

$$\Gamma = \left\{ \gamma_e^{(l)} \mid 0 \leq l < m-1, e \in E \right\},$$

where E is the spanning tree chosen above. This generating set is in general not a (symplectic) basis.

We resolve this by computing the intersection pairing on Γ, that is all intersections $\gamma_e^{(k)} \circ \gamma_f^{(l)} \in \{0, \pm 1\}$ for $e, f \in E$ and $k, l \in \{0, \dots m-1\}$, as explained in Section 5.

The resulting intersection matrix K_Γ is a skew-symmetric matrix of dimension $(n-1)(m-1)$ and has rank $2g$.

Hence, we can apply an algorithm, based on [15, Theorem 18], that outputs a symplectic basis for K_Γ over $\mathbb{Z}$, i.e. a unimodular matrix base change matrix S such that

$$S^T K_\Gamma S = J, \quad \text{where} \quad J = \begin{pmatrix} 0 & I_g & 0 \\ -I_g & 0 & 0 \\ 0 & 0 & 0_{\delta-1} \end{pmatrix}.$$

The linear combinations of periods given by the first $2g$ columns of $\Omega_\Gamma S$ then correspond to a symplectic homology basis

$$(\Omega_A, \Omega_B, 0_{\delta-1}) = \Omega_\Gamma S,$$

whereas the last $\delta - 1$ columns are zero and can be ignored, as they correspond to the dependent cycles in Γ and contribute nothing.

5 Intersections

Let (a, b) and (c, d) be two edges of the spanning tree E. The formulas in Theorem 5.1 allow to compute the intersection between shifts of elementary cycles $\left(\gamma_{a,b}^{(k)} \circ \gamma_{c,d}^{(l)}\right)$.

Note that by construction of the spanning tree, we can restrict the analysis to intersections $\left(\gamma_{a,b}^{(k)} \circ \gamma_{c,d}^{(l)}\right)$ such that c is either a or b. Moreover, we may discard the case $(a, b) = (c, d)$.

Theorem 5.1 (Intersection numbers)**.** *Let $(a, b), (c, d) \in E$. The intersections of the corresponding cycles $\gamma_{a,b}^{(k)}, \gamma_{c,d}^{(l)} \in \Gamma$ are given by*

$$\left(\gamma_{a,b}^{(k)} \circ \gamma_{c,d}^{(l)}\right) = \begin{cases} 1 & \text{if } l - k \equiv s_+ \bmod m, \\ -1 & \text{if } l - k \equiv s_- \bmod m, \\ 0 & \text{otherwise,} \end{cases}$$

where s_+, s_- are given by the following table, which covers all cases occurring in the algorithm

	case	s_+	s_-
(i)	$a = c$ and $b = d$	1	-1
(ii)	$b = c$	$-s_b$	$1 - s_b$
(iii)	$a = c$ and $\varphi > 0$	$1 - s_a$	$-s_a$
(iv)	$a = c$ and $\varphi < 0$	$-s_a$	$-1 - s_a$
(v)	$\{a, b\} \cap \{c, d\} = \varnothing$	no intersection	

and where $s_x \in \mathbb{Z}$ *for* $x \in \{a, b\}$ *is given by*

$$s_x := \frac{1}{2\pi}\left(\varphi + m \cdot \arg\left(\frac{C_{c,d}\tilde{y}_{c,d}(x)}{C_{a,b}\tilde{y}_{a,b}(x)}\right)\right)$$

and

$$\varphi = \arg\left(\frac{b-a}{d-c}\right) + \delta_{b=c}\pi.$$

Remark 5.2. Note that the intersection matrix K_Γ is composed of $(n-1)^2$ blocks of dimension $m-1$, each block corresponding to the intersection of shifts of two elementary cycles in the spanning tree. It is very sparse.

The proof of Theorem 5.1 is contained in the following exposition.

Consider two cycles $\gamma_{a,b}^{(k)}, \gamma_{c,d}^{(l)} \in \Gamma$ and recall from Definition 3.5 that

$$\gamma_{a,b}^{(k)} = \{(x, \zeta^k y_{a,b}(x)) \mid x \in [a,b]\} \cup \{(x, \zeta^{k+1} y_{a,b}(x)) \mid x \in [b,a]\},$$
$$\gamma_{c,d}^{(l)} = \{(x, \zeta^l y_{c,d}(x)) \mid x \in [c,d]\} \cup \{(x, \zeta^{l+1} y_{c,d}(x)) \mid x \in [c,d]\},$$

where $\zeta^k y_{a,b}(x), \zeta^l y_{c,d}(x)$ are branches of $\mathcal{C}$ that are analytic on open sets $V_{a,b}$ and $V_{c,d}$ (see Figure 2) respectively.

From the definition we see that $\gamma_{a,b}^{(k)} \cap \gamma_{c,d}^{(l)} = \varnothing$, whenever $[a,b] \cap [c,d] = \varnothing$. For edges in a spanning tree this is equivalent to $\{a,b\} \cap \{c,d\} = \varnothing$, thus proving (v).

Henceforth, we can assume $\{a,b\} \cap \{c,d\} \neq \varnothing$. In order to prove (i)-(iv) we have to introduce some machinery. Since the $y_{a,b}(x), y_{c,d}(x)$ are branches of $\mathcal{C}$, on the set $\mathbb{C} \setminus X$ we can define the *shifting function* $s(x)$, that takes values in $\mathbb{Z}/m\mathbb{Z}$, implicitly via

$$\zeta^{s(x)} = \frac{y_{c,d}(x)}{y_{a,b}(x)}. \tag{19}$$

Naturally, (19) extends to the other analytic branches via

$$\zeta^{s(x)+l-k} = \frac{\zeta^l y_{c,d}(x)}{\zeta^k y_{a,b}(x)}.$$

We can now define the non-empty, open set

$$V := V_{a,b} \cap V_{c,d} \subset \mathbb{C} \setminus X.$$

The shifting function $s(x)$ is well-defined on V and, since $y_{a,b}(x)$ and $y_{c,d}(x)$ are both analytic on V, $s(x)$ is constant on its connected components.

In §3.2.2 we established that multiplication of a branch by ζ corresponds to moving one sheet up on the Riemann surface. We can interpret the value of the shifting function geometrically as $\gamma_{c,d}^{(l)}$ running $s(\tilde{x}) + l - k$ sheets above $\gamma_{a,b}^{(k)}$ at a point $\tilde{x} \in V$.

This can be used to determine the intersection number in the following way. The homotopy class of a cycle on $\mathcal{C}$ is not changed by deformations that avoid encircling additional branch points. Since $V \cap X = \varnothing$ we can deform the cycles homotopically (as shown in Figure 3) such that

$$\mathrm{pr_x}\left(\gamma_{a,b}^{(k)}\right) \cap \mathrm{pr_x}\left(\gamma_{c,d}^{(l)}\right) = \{\tilde{x}\} \text{ for some } \tilde{x} \in V.$$

Consequently, the cycles can at most intersect at the points in the fiber above $\tilde{x}$, i.e.

$$\gamma_{a,b}^{(k)} \cap \gamma_{c,d}^{(l)} \subset \mathrm{pr}_x^{-1}(\tilde{x}).$$

Note that, by definition, any cycle in Γ only runs on two neighbouring sheets, which already implies

$$\left(\gamma_{a,b}^{(k)} \circ \gamma_{c,d}^{(l)}\right) = 0, \text{ if } s(\tilde{x}) + l - k \notin \{-1, 0, 1\}.$$

In the other cases we can determine the sign of possible intersections by taking into account the orientation of the cycles.

We continue the proof with case (i): Here we have $[a,b]=[c,d]$. Trivially, $\left(\gamma_{a,b}^{(k)}\circ\gamma_{a,b}^{(k)}\right)=0$ holds. For $k\neq l$ we deform the cycles such that they only intersect above $\tilde{x}=\frac{b+a}{2}\in V_{a,b}=V$. We easily see that $s(\tilde{x})=0$ and therefore $s(\tilde{x})+l-k=l-k$. The remaining non-trivial cases ($l=k\pm 1$), are shown in Figure 5 below where the cycles $\gamma_{a,b}^{(k)}$ (black), $\gamma_{a,b}^{(k+1)}$ (red) and $\gamma_{a,b}^{(k-1)}$ (green) are illustrated.

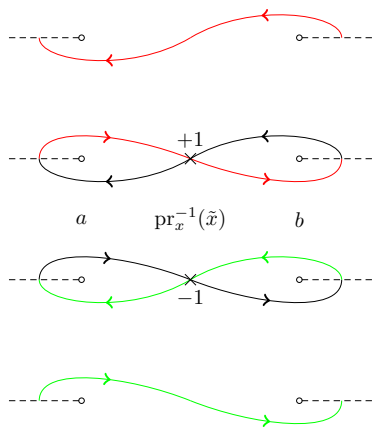


Figure 5: Intersections of self-shifts.

We see that, independently of $s(\tilde{x})$, $s_+=(k+1)-k=1$ and $s_-=(k-1)-k=-1$ are as claimed.

For (ii)-(iv) we have that $[a,b]\cap[c,d]=\{c\}$, where c is either a or b. Unfortunately, in these cases $s(c)$ is not well-defined.

Instead, we choose a point $\tilde{x}\in\mathbb{C}\setminus X$ on the bisectrix of $[a,b]$ and $[c,d]$ that is close enough to c such that $[\tilde{x},c[\subset V=V_{a,b}\cap V_{c,d}$ (see Figure 6 below), and where

$$s(\tilde{x})=\frac{m}{2\pi}\arg\left(\frac{y_{c,d}(\tilde{x})}{y_{a,b}(\tilde{x})}\right). \tag{20}$$

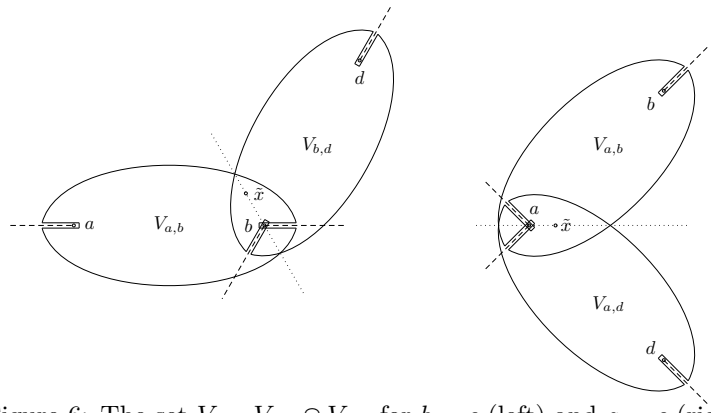


Figure 6: The set $V=V_{a,b}\cap V_{c,d}$ for $b=c$ (left) and $a=c$ (right).

Case (ii):
In this case we have $b=c$. Choosing $\tilde{x}$ on the upper bisectrix (as shown in Figure 6) and computing $s(\tilde{x})$ with (20) makes it possible to determine the intersection numbers geometrically.

Figure 7 shows the non-trivial cases $s(\tilde{x})+l-k\in\{-1,0,1\}$. There the cycles $\gamma_{a,b}^{(k)}$ (black), $\gamma_{b,d}^{(k-s(\tilde{x}))}$ (gray), $\gamma_{b,d}^{(k-s(\tilde{x})+1)}$ (green) and $\gamma_{b,d}^{(k-s(\tilde{x})-1)}$ (red) are illustrated.

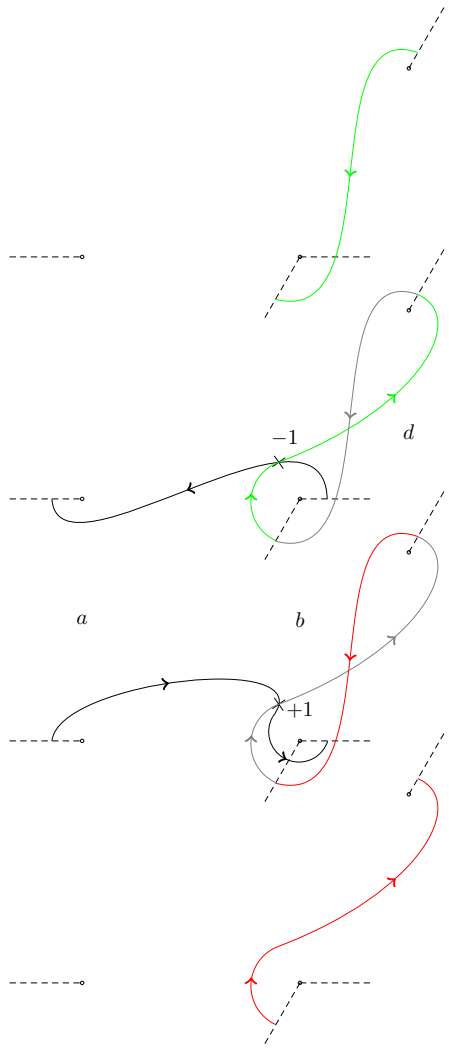


Figure 7: Intersections for $b = c$.

By Lemma 5.3 (1) we have $s(\tilde{x}) \equiv s_b$, which implies (as claimed)

$$\begin{aligned} s_+ &\equiv k - s(\tilde{x}) - k \equiv -s_b \mod m, \\ s_- &\equiv k - s(\tilde{x}) + 1 - k \equiv 1 - s_b \mod m. \end{aligned}$$

Case (iii):
In this case we have $a = c$. We choose $\tilde{x}$ on the inner bisectrix (as shown in Figure 6) and compute $s(\tilde{x})$ with (20).

For $\varphi = \arg\left(\frac{b-a}{d-a}\right) > 0$, the non trivial cases, i.e. $s(\tilde{x}) + l - k \in \{-1, 0, 1\}$, are shown in Figure 8 We illustrate the cycles $\gamma_{a,b}^{(k)}$ (black), $\gamma_{a,d}^{(k-s(\tilde{x}))}$ (gray), $\gamma_{a,d}^{(k-s(\tilde{x})+1)}$ (green) and $\gamma_{a,d}^{(k-s(\tilde{x})-1)}$ (red).

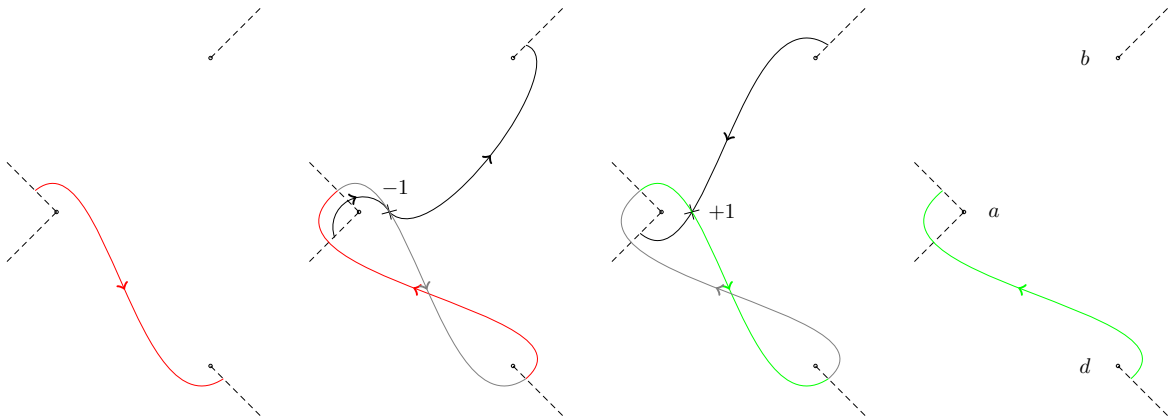


Figure 8: Intersections for $a = c$ and $\varphi > 0$.

Lemma 5.3 (2) gives us $s(\tilde{x}) \equiv s_a$, which implies (as claimed for $\varphi > 0$)

$$s_+ = k - s(\tilde{x}) + 1 - k \equiv 1 - s_a \mod m,$$
$$s_- = k - s(\tilde{x}) - k \equiv -s_a \mod m.$$

Case (iv):
When $\varphi < 0$ we can use the antisymmetry of the intersection pairing to fall back to case (iii) by looking the intersection of the swapped cycles

$$\left(\gamma_{a,b}^{(k)} \circ \gamma_{a,d}^{(l)}\right) = -\left(\gamma_{a,d}^{(l)} \circ \gamma_{a,b}^{(k)}\right).$$

The intersection on the right is then determined by case (iii) with the quantities $\varphi' = -\varphi > 0$, $s'_a = -s_a$ and $s'_\pm = s_\mp$.

Alternatively, we can see this directly from the picture: if we mirror Figure 8 at the horizontal line through a we are in case (iv). There, the intersection is positive if $\gamma_{a,b}^{(k)}$ and $\gamma_{a,d}^{(l)}$ start on the same sheet and negative if $\gamma_{a,d}^{(l)}$ starts one sheet below $\gamma_{a,b}^{(k)}$.

Lemma 5.3. *With the choices made in the proof of Theorem 5.1 the following statements hold*

(1) $s(\tilde{x}) \equiv s_b \bmod m$ *in case* (ii),

(2) $s(\tilde{x}) \equiv s_a \bmod m$ *in the case* (iii).

Proof. Starting from equation (20), for all $x \in \mathbb{C} \setminus X$ we have

$$\begin{aligned} s(x) &= \frac{m}{2\pi} \arg\left(\frac{y_{c,d}(x)}{y_{a,b}(x)}\right) \equiv \frac{m}{2\pi}\left(\arg\left(\frac{(1-u_{c,d}(x)^2)^{\frac{1}{m}}}{(1-u_{a,b}(x)^2)^{\frac{1}{m}}}\right) + \arg\left(\frac{C_{c,d}\tilde{y}_{c,d}(x)}{C_{a,b}\tilde{y}_{a,b}(x)}\right)\right) \\ &\equiv \frac{1}{2\pi}\left(\arg(1+u_{c,d}(x)) + \arg(1-u_{c,d}(x)) - \arg(1+u_{a,b}(x)) - \arg(1-u_{a,b}(x))\right) \\ &+ \frac{m}{2\pi}\left(\arg\left(\frac{C_{c,d}\tilde{y}_{c,d}(x)}{C_{a,b}\tilde{y}_{a,b}(x)}\right)\right) \mod m. \end{aligned}$$

In case (ii) we have $b = c$ and denote $\varphi_0 = \arg\left(\frac{b-a}{d-b}\right)$. Then, we can parametrize all points $\tilde{x} \neq b$ on the upper bisectrix of $[a, b]$ and $[a, d]$ (see Figure 6) via

$$\tilde{x} = x_{b,d}(-1 + t\exp(i(\pi + \varphi_0)/2)) \text{ as well as}$$
$$\tilde{x} = x_{a,b}(1 - t\exp(-i(\pi + \varphi_0)/2))$$

for some $t > 0$, where $x_{b,d}$ and $x_{a,b}$ are defined as in (3.2.3). Therefore,

$$\arg(1 + u_{b,d}(\tilde{x})) = \frac{\pi + \varphi_0}{2} \text{ and}$$
$$\arg(1 - u_{a,b}(\tilde{x})) = -\frac{\pi + \varphi_0}{2}.$$

For $\tilde{x}$ chosen close enough to b we have that $[\tilde{x}, b[\subset V$ and the shifting function $s(\tilde{x})$ is constant as $\tilde{x}$ tends towards b. Hence, we can compute its value at $\tilde{x}$ as

$$\begin{aligned} s(\tilde{x}) &\equiv \frac{1}{2\pi}\left(\pi + \varphi_0 + \arg(1 - u_{b,d}(\tilde{x})) - \arg(1 + u_{a,b}(\tilde{x})) + m \arg\left(\frac{C_{b,d}\tilde{y}_{b,d}(\tilde{x})}{C_{a,b}\tilde{y}_{a,b}(\tilde{x})}\right)\right) \\ &\equiv \frac{1}{2\pi}\left(\varphi + \arg(1 - u_{b,d}(b)) - \arg(1 + u_{a,b}(b)) + m \arg\left(\frac{C_{b,d}\tilde{y}_{b,d}(b)}{C_{a,b}\tilde{y}_{a,b}(b)}\right)\right) \\ &\equiv \frac{1}{2\pi}\left(\varphi + \arg(2) - \arg(2) + m \arg\left(\frac{C_{b,d}\tilde{y}_{b,d}(b)}{C_{a,b}\tilde{y}_{a,b}(b)}\right)\right) \equiv s_b \mod m, \end{aligned}$$

thus proving (1).

In the cases (iii) and (iv) we have $a = c$ and denote $\varphi = \arg\left(\frac{b-a}{d-a}\right)$. For $\varphi > 0$ we can parametrize all points $\tilde{x} \neq a$ on the inner bisectrix of $[a, b]$ and $[a, d]$ (see Figure 6) via

$$\begin{aligned} &\tilde{x} = x_{a,d}(-1 + t\exp(i\varphi/2)) \text{ as well as} \\ &\tilde{x} = x_{a,b}(-1 + t\exp(-i\varphi/2)) \end{aligned}$$

for some $t > 0$, where $x_{a,d}$ and $x_{a,b}$ are defined as in (3.2.3). Therefore,

$$\begin{aligned} &\arg(1 + u_{a,d}(\tilde{x})) = \frac{\varphi}{2} \text{ and} \\ &\arg(1 + u_{a,b}(\tilde{x})) = -\frac{\varphi}{2}. \end{aligned}$$

As before, we let $\tilde{x}$ tend towards a and compute the shifting function at $\tilde{x}$ as

$$\begin{aligned} s(\tilde{x}) &\equiv \frac{1}{2\pi}\left(\varphi + \arg(1 - u_{a,d}(\tilde{x})) - \arg(1 + u_{a,b}(\tilde{x})) + m \arg\left(\frac{C_{a,d}\tilde{y}_{a,d}(\tilde{x})}{C_{a,b}\tilde{y}_{a,b}(\tilde{x})}\right)\right) \\ &\equiv \frac{1}{2\pi}\left(\varphi + \arg(1 - u_{a,d}(a)) - \arg(1 - u_{a,b}(a)) + m \arg\left(\frac{C_{a,d}\tilde{y}_{a,d}(a)}{C_{a,b}\tilde{y}_{a,b}(a)}\right)\right) \\ &\equiv \frac{1}{2\pi}\left(\varphi + \arg(2) - \arg(2) + m \arg\left(\frac{C_{a,d}\tilde{y}_{a,d}(a)}{C_{a,b}\tilde{y}_{a,b}(a)}\right)\right) \equiv s_a \mod m. \end{aligned}$$

□

Remark 5.4. The intersection numbers given by Theorem 5.1 are independent of the choices of $\tilde{x}$ that were made in the proof. This approach works for any $\tilde{x} \in V$.

Even though the value of $s(\tilde{x})$ changes, if we choose $\tilde{x}$ in a different connected component of V, e.g. on the lower bisectrix in case (ii), the parametrization of the bisectrix and the corresponding arguments will change accordingly.

6 Numerical integration

As explained in Section 4.2, the periods of the generating cycles $\gamma \in \Gamma$ are expressed in terms of elementary integrals (17)

$$I_{a,b}(i,j) = \int_{-1}^{1} \frac{u^{i-1}\mathrm{d}u}{(1-u^2)^{\frac{j}{m}}\tilde{y}_{a,b}(u)^j}$$

where $(a, b) \in E$ and $\omega_{i,j} \in \mathcal{W}$. We restrict the numerical analysis to this case.

In this section, we denote by α the value $1 - j/m$, which is the crucial parameter for numerical integration. Note that $\alpha = 1/2$ for hyperelliptic curves, while for general superelliptic curves α ranges from $1/m$ to $\frac{m-1}{m}$ depending on the differential form $\omega_{i,j}$ considered.

We study here two numerical integration schemes which are suitable for arbitrary precision computations:

- the double-exponential change of variables is completely general [20] and its robustness allows to compute rigorously all integrals of periods in a very unified setting even with different values of α;

- in the special case of hyperelliptic curves however, the Gauss-Chebychev method [1, 25.4.38] applies and provides a better scheme (fewer and simpler integration points).

For $m > 2$, the periods could also be computed using general Gauss-Jacobi integration of parameters α, α. However, a different scheme has to be computed for each α and it now involves computing roots of general Jacobi polynomials to large accuracy, which makes it hard to compete with the double-exponential scheme.

Remark 6.1. Even for hyperelliptic curves it can happen that the double exponential scheme outperforms Gauss-Chebychev on particular integrals. This is easy to detect in practice and we can always switch to the best method.

6.1 Double-exponential integration

Throughout this section, $\lambda \in [1, \frac{\pi}{2}]$ is a fixed parameter. By default the value $\lambda = \frac{\pi}{2}$ is a good choice, however smaller values may improve the constants. We will not address this issue here.

Using the double-exponential change of variable

$$u = \tanh(\lambda \sinh(t)), \tag{21}$$

the singularities of (17) at ± 1 are pushed to infinity and the integral becomes

$$I_{a,b}(i,j) = \int_{\mathbb{R}} g(t)\mathrm{d}t$$

with

$$g(t) = \frac{u(t)^{i-1}}{\tilde{y}_{a,b}(u(t))^j} \frac{\lambda \cosh(t)}{\cosh(\lambda \sinh(t))^{2\alpha}}.$$

Let

$$Z_r = \{\tanh(\lambda \sinh(z)), -r < \mathrm{Im}(z) < r\}$$

be the image of the strip of width $2r$ under the change of variable (21).

Since we can compute the distance of each point $u_k \in U^+ \cup U^-$ (see 4) to both $[-1, 1]$ and the neighborhood Z_r (see §8.3.2), we obtain

Lemma 6.2. *Let $r \in]0, \frac{\pi}{2}[$ be such that $\lambda \sin(r) < \frac{\pi}{2}$ and $(U^+ \cup U^-) \cap Z_r = \varnothing$, then g is holomorphic on $\{-r < \mathrm{Im}(z) < r\}$ and there exist explicitly computable constants M_1, M_2 such that*

- $\left|\frac{u^{i-1}}{\tilde{y}_{a,b}(u)^j}\right| \leq M_1$ *for all* $u \in [-1, 1]$,
- $\left|\frac{u^{i-1}}{\tilde{y}_{a,b}(u)^j}\right| \leq M_2$ *for all* $u \in Z_r$.

Fixing such a value r, we also introduce the following quantities

$$\begin{cases} X_r & = \cos(r)\sqrt{\frac{\pi}{2\lambda \sin r} - 1} \\ B(r,\alpha) & = \frac{2}{\cos r}\left(\frac{X_r}{2}\left(\frac{1}{\cos(\lambda \sin r)^{2\alpha}} + \frac{1}{X_r^{2\alpha}}\right) + \frac{1}{2\alpha \sinh(X_r)^{2\alpha}}\right). \end{cases}$$

Once we have computed the two bounds M_1, M_2 and the constant $B(r, \alpha)$, we obtain a rigorous integration scheme as follows:

Theorem 6.3. *With notation as above, for all $D > 0$, choose h and N such that*

$$\begin{cases} h \leq \frac{2\pi r}{D + \log(2M_2 B(r,\alpha) + e^{-D})} \\ Nh \geq \operatorname{asinh}\left(\frac{D + \log\left(\frac{2^{2\alpha+1} M_1}{\alpha}\right)}{2\alpha\lambda}\right), \end{cases} \tag{22}$$

then

$$\left| I_{a,b}(i,j) - h \sum_{\ell=-N}^{N} w_\ell \frac{u_\ell^{i-1}}{\tilde{y}_{a,b}(u_\ell)^j} \right| \leq e^{-D},$$

where

$$\begin{cases} u_\ell = \tanh(\lambda \sinh(\ell h)), \\ w_\ell = \frac{\lambda \cosh(\ell h)}{\cosh(\lambda \sinh(\ell h))^{2\alpha}}. \end{cases}$$

The proof follows the same lines as the one in [20, Thm. 2.10]: we write the Poisson formula on $h\mathbb{Z}$ for the function g

$$\underbrace{h\sum_{|k|>N} g(kh)}_{e_T} + h\sum_{k=-N}^{N} g(kh) = \int_{\mathbb{R}} g(t)\mathrm{d}t + \underbrace{\sum_{k\in\mathbb{Z}^*} \hat{g}\left(\frac{k}{h}\right)}_{e_Q}$$

and control both error terms e_T and e_Q by Lemma 6.4 and 6.5 below. The actual parameters h and N follow from bounding each error by $e^{-D}/2$ (the condition of Lemma 6.4 being automatically satisfied).

Lemma 6.4 (truncation error)**.** *For all N, h such that $2\alpha\lambda\cosh(Nh) > 1$ we have*

$$\sum_{|k|>N} |hg(kh)| \leq \frac{2^{2\alpha}M_1}{\alpha}\exp(-2\alpha\lambda\sinh(Nh)).$$

Proof. We bound the sum by an integral (the condition ensures the function is decreasing)

$$\begin{aligned}\sum_{|k|>N} |hg(kh)| &\leq 2M_1\int_{Nh}^{\infty}\frac{\lambda\cosh(t)}{\cosh(\lambda\sinh(t))^{2\alpha}} = 2M_1\int_{\lambda\sinh(Nh)}^{\infty}\frac{\mathrm{d}t}{\cosh(t)^{2\alpha}}\\ &\leq 2^{2\alpha+1}M_1\int_{\lambda\sinh(Nh)}^{\infty} e^{-2\alpha t}\mathrm{d}t = \frac{2^{2\alpha}M_1}{\alpha}e^{-2\alpha\lambda\sinh(Nh)}.\end{aligned}$$

□

Lemma 6.5 (discretization error)**.** *With the current notations,*

$$\sum_{k\neq 0}\left|\hat{g}\left(\frac{k}{h}\right)\right| \leq \frac{2M_2B(r,\alpha)}{e^{2\pi r/h}-1}.$$

Proof. We first bound the Fourier transform by a shift of contour

$$\forall X > 0, \hat{g}(\pm X) = e^{-2\pi Xr}\int_{\mathbb{R}} g(t\mp ir)e^{-2i\pi tX}\mathrm{d}t$$

so that

$$\sum_{k}\left|\hat{g}\left(\frac{k}{h}\right)\right| \leq \frac{2M_2}{e^{2\pi r/h}-1}\int_{\mathbb{R}}\left|\frac{\lambda\cosh(t+ir)}{\cosh(\lambda\sinh(t+ir))^{2\alpha}}\right|\mathrm{d}t.$$

Now the point $\lambda\sinh(t+ir) = X(t)+iY(t)$ lies on the hyperbola $Y^2 = \lambda^2(\sin^2 r + \tan^2 rX^2)$, and

$$\begin{cases}|\lambda\cosh(t+ir)| & \leq \lambda\cosh(t) = \frac{X'(t)}{\cos(r)}\\ |\cosh(X+iY)|^2 & = \sinh(X)^2+\cos(Y)^2,\end{cases}$$

so that

$$\int_{\mathbb{R}}\left|\frac{\lambda\cosh(t+ir)}{\cosh(\lambda\sinh(t+ir))^{2\alpha}}\right|\mathrm{d}t \leq \frac{2}{\cos r}\int_0^{\infty}\frac{\mathrm{d}X}{(\sinh(X)^2+\cos(Y)^2)^{\alpha}}.$$

For $X_0 = 0$ we get $Y_0 = \lambda\sin r < \frac{\pi}{2}$, and $Y_r = \frac{\pi}{2}$ for $X_r = \cos(r)\sqrt{\frac{\pi}{2Y_0}-1}$.

We cut the integral at $X = X_r$ and write

$$\begin{aligned}\int_0^{X_r}\frac{\mathrm{d}X}{(\sinh(X)^2+\cos(Y)^2)^{\alpha}} &\leq \int_0^{X_r}\frac{\mathrm{d}X}{(X^2+\cos^2 Y)^{\alpha}}\\ \int_{X_r}^{\infty}\frac{\mathrm{d}X}{(\sinh(X)^2+\cos(Y)^2)^{\alpha}} &\leq \int_{X_r}^{\infty}\frac{\mathrm{d}X}{(\sinh X)^{2\alpha}}.\end{aligned}$$

We bound the first integral by convexity: since $Y(X)$ is convex and cos is concave decreasing for $Y \leq Y_r$ we obtain by concavity of the composition

$$\forall X \leq X_r, \cos(Y) \geq \cos(Y_0)\left(1-\frac{X}{X_r}\right).$$

Now $X^2 + \cos^2 Y \geq P_2(X)$ where

$$P_2(X) = \left(1 + \frac{\cos^2(Y_0)}{X_r^2}\right) X^2 - 2\frac{\cos^2(Y_0)}{X_r} X + \cos^2(Y_0)$$

is a convex quadratic, so $X \mapsto P_2(X)^{-\alpha}$ is still convex and the integral is bounded by a trapezoid

$$\int_0^{X_r} \frac{\mathrm{d}X}{P_2(X)^\alpha} \leq \frac{X_r}{2}\left(P_2(0)^{-\alpha} + P_2(X_r)^{-\alpha}\right) = \frac{X_r}{2}\left(\frac{1}{\cos(Y_0)^{2\alpha}} + \frac{1}{X_r^{2\alpha}}\right).$$

For the second integral we use $\sinh(X) \geq \sinh(X_r)e^{X-X_r}$ to obtain

$$\int_{X_r}^{\infty} \frac{\mathrm{d}X}{\sinh(X)^{2\alpha}} \leq \frac{1}{2\alpha \sinh(X_r)^{2\alpha}}.$$

□

6.2 Gauss-Chebychev integration

In the case of hyperelliptic curves, we have $\alpha = \frac{1}{2}$ (and $j = 1$) and the integral

$$\int_{-1}^{1} \frac{\varphi_{i,1}(u)}{\sqrt{1-u^2}} \mathrm{d}u$$

can be efficiently handled by Gaussian integration with weight $1/\sqrt{1-u^2}$, for which the corresponding orthogonal polynomials are Chebychev polynomials.

In this case, the integration formula is particularly simple: there is no need to actually compute the Chebychev polynomials since their roots are explicitly given as cosine functions [1, 25.4.38].

Theorem 6.6 (Gauss-Chebychev integration)**.** *Let g be holomorphic around $[-1, 1]$. Then for all N, there exists $\xi \in]-1, 1[$ such that*

$$\int_{-1}^{1} \frac{g(u)}{\sqrt{1-u^2}} \mathrm{d}u - \sum_{\ell=1}^{N} w_k g(u_\ell) = \frac{\pi 2^{2N+1}}{2^{4N}} \frac{g^{(2N)}(\xi)}{(2N)!} = E(N), \tag{23}$$

with constant weights $w_\ell = w = \frac{\pi}{N}$ and nodes $u_\ell = \cos\left(\frac{2\ell-1}{2N}\pi\right)$.

Moreover, very nice estimates on the error $E(N)$ can by obtained if g is holomorphic on an ellipse ε_r of the form (see Figure 9)

$$\varepsilon_r = \{z \in \mathbb{C}, |z-1| + |z+1| = 2\cosh(r)\}.$$

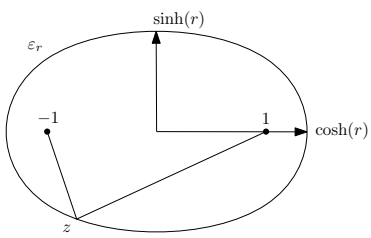


Figure 9: ellipse parameters.

Theorem 6.7 ([6, Theorem 5])**.** *Let $r > 0$ such that g is holomorphic on ε_r. Then the error in* (23) *satisfies*

$$|E(N)| \leq \frac{2\pi M(r)}{e^{2rN} - 1}$$

where $M(r) = \max\{|g(z)|, z \in \varepsilon_r\}$.

Now we apply this theorem with a function $g_i(u) = \frac{u^i}{\sqrt{\prod(u-u_k)}}$, so that the error can be explicitly controlled a priori.

Lemma 6.8. *Let $r > 0$ be such that $2\cosh(r) < |u_k - 1| + |u_k + 1|$ for all points $u_k \in U^+ \cup U^-$, then there exists an explicitly computable constant $M(r)$ such that for all $u \in \varepsilon_r$*

$$\left| \frac{u^{i-1}}{\tilde{y}_{a,b}(u)} \right| \leq M(r).$$

Proof. We simply compute the distance $d_r(u_k) = \inf_{z \in \varepsilon_r} |z - u_k|$ from a point u_k to the ellipse ε_r, and let $M(r) = \frac{\cosh(r)^{i-1}}{\sqrt{\prod d_r(u_k)}}$. For simplicity, we can use the triangle inequality $d_r(u_k) \geq \cosh(r_k) - \cosh(r)$, where $2\cosh(r_k) = |u_k - 1| + |u_k + 1|$. □

Theorem 6.9. *With r and $M(r)$ satisfying Lemma 6.8, for all N such that*

$$N \geq \frac{D + \log(2\pi M(r)) + 1}{2r},$$

we have

$$\left| I_{a,b}(i,1) - \frac{\pi}{N} \sum_{\ell=1}^{N} \frac{u_\ell^{i-1}}{\tilde{y}_{a,b}(u_\ell)} \right| \leq e^{-D},$$

where $u_\ell = \cos\left(\frac{2\ell-1}{2N}\pi\right)$.

More details on the choice of r and the computation of $M(r)$ are given in §8.3.1.

7 Computing the Abel-Jacobi map

Here we are concerned with explicitly computing the Abel-Jacobi map of degree zero divisors; for a general introduction see Section 2.

Assume for this section that we have already computed a big period period matrix (and all related data) following the Strategy from Section 4.

Let $D = \sum_{P \in \mathcal{C}} v_P P \in \mathrm{Div}^0(\mathcal{C})$. After choosing a basepoint $P_0 \in \mathcal{C}$, the computation of $\mathcal{A}$ reduces (using linearity) to

$$\mathcal{A}([D]) \equiv \sum_{P \in \mathcal{C}} v_P \int_{P_0}^{P} \bar{\omega} \mod \Lambda.$$

For every $P \in \mathcal{C}$, $\int_{P_0}^{P} \bar{\omega}$ is a linear combination of vector integrals of the form

$$\int_{P_0}^{P_k} \bar{\omega} \quad \text{(see §7.1)}, \qquad \int_{P_k}^{P} \bar{\omega} \quad \text{(see §7.2)} \quad \text{and} \quad \int_{P_0}^{P_\infty} \bar{\omega} \quad \text{(see §7.3)}, \quad \text{where}$$

- $\bar{\omega}$ is the vector of differentials in $\mathcal{W}$,
- $P = (x_P, y_P) \in \mathcal{C}$ is a finite point on the curve,
- $P_k = (x_k, 0) \in \mathcal{C}$ is a finite ramification point, i.e. $x_k \in X$, and
- $P_\infty \in \mathcal{C}$ is an infinite point.

Typically, we choose as basepoint the ramification point $P_0 = (x_0, 0)$, where $x_0 \in X$ is the root of the spanning tree $G = (X, E)$.

Finally, the resulting vector integral has to be reduced modulo the period lattice Λ, which is covered in §7.4.

Remark 7.1 (Image of Abel-Jacobi map). For practical reasons, we will compute the image of the Abel-Jacobi map in the canonical torus $\mathbb{R}^{2g}/\mathbb{Z}^{2g}$. This representation has the following advantages:

- Operations on the Jacobian variety $\mathrm{Jac}(\mathcal{C})$ correspond to operations in $\mathbb{R}^{2g}/\mathbb{Z}^{2g}$.
- m-torsion divisors under $\mathcal{A}$ are mapped to vectors of rational numbers with denominator dividing m.

7.1 Between ramification points

Suppose we want to integrate $\bar{\omega}$ from $P_0 = (x_0, 0)$ to $P_k = (x_k, 0)$. By construction there exists a path $(x_0 = x_{k_0}, x_{k_1}, \ldots, x_{k_{n-1}}, x_{k_t} = x_k)$ in the spanning tree which connects x_0 and x_k. Thus, the integral splits into

$$\int_{P_0}^{P_k} \bar{\omega} = \sum_{j=0}^{t-1} \int_{P_{k_j}}^{P_{k_{j+1}}} \bar{\omega}.$$

Denote $a = x_{k_j}, b = x_{k_{j+1}} \in X$. From §3.3 we know that for $(a, b) \in E$ a smooth path between $P_a = (a, 0)$ and $P_b = (b, 0)$ is given by

$$\gamma^{(0)}_{[a,b]} = \{(x, y_{a,b}(x)) \mid x \in [a, b]\}.$$

Let $\omega_{i,j} \in \mathcal{W}$ be a differential. According to the proof of Theorem 4.1 the corresponding integral is given by

$$\int_{\gamma^{(0)}_{[a,b]}} \omega_{i,j} = C_{a,b}^{-j} \left(\frac{b-a}{2}\right)^i \int_{-1}^{1} \frac{\varphi_{i,j}(u)}{(1-u^2)^{\frac{j}{m}}} \mathrm{d}u,$$

which is (up to the constants) an elementary integral (16) and has already been evaluated during the period matrix computation.

Remark 7.2. Moreover, the image of the Abel-Jacobi map between ramification points is m-torsion, i.e. for any two $k, j \in \{1, \ldots, n\}$ we have

$$m \int_{P_j}^{P_k} \bar{\omega} \equiv \mathcal{A}([mP_k - mP_j]) \equiv 0 \mod \Lambda, \tag{24}$$

since $\operatorname{div}\left(\frac{x-x_k}{x-x_j}\right) = mP_k - mP_j$ is a principal divisor.

7.2 Reaching non-ramification points

Let $P = (x_P, y_P) \in \mathcal{C}$ be a finite point and $P_a = (a, 0)$ a ramification point such that $X \cap]a, x_P] = \varnothing$. In order to define a smooth path between P and P_a we need to find a suitable analytic branch of $\mathcal{C}$.

This can be done following the approach in §3.2.3, the only difference being that x_P is not a branch point. Therefore, we are going to adjust the definitions and highlight the differences.

Let u_{a,x_P} be the affine linear transformation that maps $[a, x_P]$ to $[-1, 1]$. Similar to (4) we split up the image of X under u_{a,x_P} into subsets, but this time

$$u_{a,x_P}(X) = \{-1\} \cup U^+ \cup U^-.$$

Then, $\tilde{y}_{a,x_P}(u)$ can be defined exactly as in (5) and is holomorphic in a neighbourhood ϵ_{a,x_P} of $[-1, 1]$. The term corresponding to a, that is

$$\sqrt[m]{1+u},$$

has a branch cut $]-\infty, -1]$ and is holomorphic on the complement of this cut.

Now we can define a branch of the curve, that is analytic in a neighbourhood V_{a,x_P} of $]a, x_P]$, by

$$y_{a,x_P}(x) = C_{a,x_P} \tilde{y}_{a,x_P}(u_{a,x_P}(x)) \sqrt[m]{1 + u_{a,x_P}(x)},$$

where

$$C_{a,x_P} = \left(\frac{x_P - a}{2}\right)^{\frac{n}{m}} e^{\frac{\pi i}{m}(\#U^+ \bmod 2)},$$

so that the statements of Proposition 3.4 continue to hold for $\tilde{y}_{a,x_P}$ and y_{a,x_P}, if we choose the sets ϵ_{a,x_P} and V_{a,x_P} as if x_P was a branch point.

Therefore, the lifts of $[a, x_P]$ to $\mathcal{C}$ are given by

$$\gamma^{(l)}_{[a,x_P]} = \{(x, \zeta^l y_{a,x_P}(x)) \mid x \in [a, x_P]\}, \quad l \in \mathbb{Z}/m\mathbb{Z}.$$

In order to reach $P = (x_P, y_P)$ we have to pick the correct lift. This is done by computing a *shifting number* $s \in \mathbb{Z}/m\mathbb{Z}$ at the endpoint x_P:

$$\zeta^s = \frac{y_P}{y_{a,x_P}(x_P)} = \frac{y_P}{C_{a,x_P}\tilde{y}_{a,x_P}(u_{a,x_P}(x_P))\sqrt[m]{2}}$$

Consequently, $\gamma^{(s)}_{[a,x_P]}$ is a smooth path between P_a and P on $\mathcal{C}$. We can now state the main theorem of this section.

Theorem 7.3. *Let $\omega_{i,j} \in \mathcal{W}^{mer}$ be a differential. With the choices and notation as above we have*

$$\int_{P_a}^{P} \omega_{i,j} = \zeta^{-sj} C_{a,x_P}^{-j} \left(\frac{x_P - a}{2}\right)^i \int_{-1}^{1} \frac{\varphi_{i,j}(u)}{(1+u)^{\frac{j}{m}}} \mathrm{d}u,$$

where

$$\varphi_{i,j} = \left(u + \frac{x_P + a}{x_P - a}\right)^{i-1} \tilde{y}_{a,x_P}(u)^{-j}$$

is holomorphic in a neighbourhood ϵ_{a,x_P} of $[-1,1]$ and

$$s = \frac{m}{2\pi} \arg\left(\frac{y_P}{C_{a,x_P}\tilde{y}_{a,x_P}(u_{a,x_P}(x_P))}\right).$$

Proof. We have

$$\begin{aligned}\int_{P_a}^{P} \omega_{i,j} &= \int_{\gamma^{(s)}_{[a,x_P]}} \frac{x^{i-1}}{y^j}\mathrm{d}x = \zeta^{-sj}\int_a^{x_P} \frac{x^{i-1}}{y_{a,x_P}(x)^j}\mathrm{d}x \\ &= \zeta^{-sj} C_{a,x_P}^{-j} \int_a^{x_P} \frac{x^{i-1}}{(1+u_{a,x_P}(x))^{\frac{j}{m}}\tilde{y}_{a,x_P}(u_{a,x_P}(x))^j}\mathrm{d}x\end{aligned}$$

Applying the transformation $u = u_{a,x_P}(x)$ introduces the derivative $\mathrm{d}x = \left(\frac{x_P - a}{2}\right)\mathrm{d}u$. Hence

$$\begin{aligned}\int_{P_a}^{P} \omega_{i,j} &= \zeta^{-sj} C_{a,x_P}^{-j}\left(\frac{x_P - a}{2}\right)\int_a^{x_P} \frac{x_{a,x_P}(u)^{i-1}}{(1+u)^{\frac{j}{m}}\tilde{y}_{a,x_P}(u)^j}\mathrm{d}u \\ &= \zeta^{-sj} C_{a,x_P}^{-j}\left(\frac{x_P - a}{2}\right)^i \int_a^{x_P} \frac{\left(u + \frac{x_P+a}{x_P-a}\right)^{i-1}}{(1+u)^{\frac{j}{m}}\tilde{y}_{a,x_P}(u)^j}\mathrm{d}u.\end{aligned}$$

The statement about holomorphicity of $\varphi_{i,j}$ is implied, since Proposition 3.4 holds for $\tilde{y}_{a,x_P}$ and y_{a,x_P} as discussed above. □

Remark 7.4. By Theorem 7.3, the problem of integrating $\bar{\omega}$ from P_0 to P reduces to numerical integration of

$$\int_{-1}^{1} \frac{\varphi_{i,j}(u)}{(1+u)^{\frac{j}{m}}}\mathrm{d}u.$$

Although these integrals are singular at only one end-point, they can still be computed using the double-exponential estimates presented in Section 6 (this is not true for the Gauss-Chebychev method).

7.3 Infinite points

Recall from §3.1 that there are $\delta = \gcd(m,n)$ points $P_\infty^{(i)}$ at infinity on our projective curve $\mathcal{C}$, so we introduce the set $\mathcal{P} = \{P_\infty^{(1)}, \ldots, P_\infty^{(\delta)}\}$.

Suppose we want to integrate from P_0 to $P_\infty \in \mathcal{P}$, which is equivalent to computing the Abel-Jacobi map of the divisor $D_\infty = P_\infty - P_0$.

Our strategy is to explicitly apply Chow's moving lemma to D_∞: we construct a principal divisor $D \in \mathrm{Prin}(\mathcal{C})$ such that $\mathrm{supp}(D) \cap \mathcal{P} = \{P_\infty\}$ and $\mathrm{ord}_{P_\infty}(D) = \pm 1$. Then, by definition of the Abel-Jacobi map,

$$\mathcal{A}([D_\infty \mp D]) \equiv \mathcal{A}([D_\infty]) \equiv \int_{P_0}^{P_\infty} \bar{\omega} \mod \Lambda$$

and $\operatorname{supp}(D_\infty \mp D) \cap \mathcal{P} = \varnothing$.

The exposition in this paragraph will explain the construction of D, while distinguishing three different cases.

In the following denote by $\mu, \nu > 0$ the coefficients of the Bézout identity

$$-\mu m + \nu n = \delta.$$

Remark 7.5. Note that there are other ways of computing $\mathcal{A}([D_\infty])$. For instance, using transformations or direct numerical integration. Especially in the case $\delta = m$ a transformation (see Remark 3.3) is the better option and may be used in practice. The advantage of this approach is that we can stay in our setup, i.e. we can compute solely on $\mathcal{C}_{\text{aff}}$ and keep the integration scheme.

7.3.1 Coprime degrees

For $\delta = 1$ there is only one infinite point $\mathcal{P} = \{P_\infty\}$ and we can easily compute $\mathcal{A}([D_\infty])$ by adding a suitable principal divisor D

$$\begin{aligned}
\operatorname{div}(y^\nu) &= \nu \sum_{k=1}^{n} P_k - \nu n P_\infty, \\
\operatorname{div}((x - x_0)^{-\mu}) &= \mu m P_\infty - \mu m P_0, \\
D = \operatorname{div}(y^\nu (x - x_0)^{-\mu}) &= \nu \sum_{k=1}^{n} P_k - \mu m P_0 - P_\infty.
\end{aligned}$$

We immediately obtain

$$\begin{aligned}
\mathcal{A}([D_\infty]) \equiv \mathcal{A}([D_\infty + D]) &= \mathcal{A}([\nu \sum_{k=1}^{n} P_k - (\mu m + 1) P_0]) \\
&\equiv \nu \sum_{k=1}^{n} \int_{P_0}^{P_k} \bar{\omega} \mod \Lambda
\end{aligned}$$

and conclude that $\mathcal{A}([D_\infty])$ can be expressed in terms of integrals between ramification points (see §7.1).

Remark 7.6. In general, the principal divisor

$$D := \operatorname{div}(y^\nu (x - x_0)^{-\mu}) = \nu \sum_{k=1}^{n} P_k - \mu m P_0 - \sum_{l=1}^{\delta} P_\infty^{(l)}$$

yields the useful relation

$$\nu \sum_{k=1}^{n} \int_{P_0}^{P_k} \bar{\omega} \equiv \sum_{l=1}^{\delta} \int_{P_0}^{P_\infty^{(l)}} \bar{\omega} \mod \Lambda.$$

7.3.2 Non-coprime degrees

For $\delta > 1$ the problem becomes a lot harder. First we need a way to distinguish between the infinite points in $\mathcal{P} = \{P_\infty^{(1)}, \ldots, P_\infty^{(\delta)}\}$ and second they are singular points on the projective closure of our affine model $\mathcal{C}_{\text{aff}}$ whenever $m \neq \{n, n \pm 1\}$.

As shown in [22, §1] we obtain a second affine patch of $\mathcal{C}$ that is non-singular along $\mathcal{P}$ in the following way:

Denoting $M = \frac{m}{\delta}$ and $N = \frac{n}{\delta}$, we consider the birational transformation

$$(x, y) = \Phi(r, t) = \left(\frac{1}{r^\nu t^M}, \frac{1}{r^\mu t^N} \right)$$

which results in an affine model

$$\tilde{\mathcal{C}}_{\text{aff}} : r^\delta = \prod_{k=1}^{n} (1 - x_k r^\nu t^M).$$

The inverse transformation is given by

$$(r,t) = \Phi^{-1}(x,y) = \left(\frac{y^M}{x^N}, \frac{x^\mu}{y^\nu}\right).$$

Under this transformation the infinite points on $\mathcal{C}_{\text{aff}}$ are mapped to points on $\tilde{\mathcal{C}}_{\text{aff}}$ with either $r = 0$ or $t = 0$. Since there are no points with $r = 0$ on $\tilde{\mathcal{C}}_{\text{aff}}$, all infinite points in $\mathcal{P}$ are mapped to points with $t = 0$, namely the finite non-singular points

$$(r,t) = (\zeta_\delta^s, 0), \quad s = 1, \dots, \delta,$$

where $\zeta_\delta = e^{\frac{2\pi i}{\delta}}$. Hence, we can describe the points in $\mathcal{P} \subset \mathcal{C}$ via

$$P_\infty^{(s)} = \Phi(\zeta_\delta^s, 0).$$

Note that the infinite points with $r = \infty$ on $\tilde{\mathcal{C}}_{\text{aff}}$ are exactly the images of points with $x = 0$ on $\mathcal{C}_{\text{aff}}$ (i.e. the fiber ${\text{pr}_\text{x}}^{-1}(0)$) under Φ^{-1}, while the infinite points with $t = \infty$ correspond to points with $y = 0$ (i.e. the ramification points P_k) respectively.

Suppose we want to compute the Abel-Jacobi map of $D_\infty^{(s)} = P_\infty^{(s)} - P_0$ for $s \in \{1, \dots, \delta\}$. Again following our strategy, this time working on $\tilde{\mathcal{C}}_{\text{aff}}$, we look at the intersection of the vertical line through $(\zeta_\delta^s, 0)$ with $\tilde{\mathcal{C}}_{\text{aff}}$. We write down the corresponding principal divisor

$$E_1 = \text{div}(r - \zeta_\delta^s) = \sum_{i=1}^{d} \left(\zeta_\delta^s, t_i^{(s)}\right) - NE_1'$$

where the $t_i^{(s)}$ are the zeros (up to multiplicity) of $h(t) = \prod_{k=1}^n (1 - x_k \zeta_\delta^{s\nu} t^M) - 1 \in \mathbb{C}[t]$, $d = \deg(h)$ and

$$E_1' = \begin{cases} (m-M)\Phi^{-1}(0,0), & \text{if } 0 \in X, \\ \sum_{Q \in \text{pr}_x^{-1}(0)} \Phi^{-1}(Q) & \text{otherwise.} \end{cases} \tag{25}$$

Note that E_1 satisfies $\text{supp}(E_1) \cap \Phi^{-1}(\mathcal{P}) = \{(\zeta_\delta^s, 0)\}$. Now, we can define the corresponding principal divisor on $\mathcal{C}_{\text{aff}}$ by

$$D_1 := \text{div}\left(\frac{y^M}{x^N} - \zeta_\delta^s\right);$$

then $\text{ord}_{P_\infty^{(s)}}(D_1) \geq 1$ by construction.

Theorem 7.7. *Assume* $\text{ord}_{P_\infty^{(s)}}(D_1) = 1$ *and* $0 \notin X$. *Then, for* $s = 1, \dots, \delta$, *there exist points* $Q_1^{(s)}, \dots, Q_{n-1}^{(s)} \in \mathcal{C} \setminus \mathcal{P}$ *such that*

$$\mathcal{A}([D_\infty^{(s)}]) \equiv -\sum_{i=1}^{n-1} \int_{P_0}^{Q_i^{(s)}} \bar{\omega} \mod \Lambda. \tag{26}$$

Proof. First note that $\text{ord}_{P_\infty^{(s)}}(D_1) = 1$ implies $M = 1$, i.e. $m = \delta$. Together with the assumption $0 \notin X$, this gives us $\deg(h) = n$. Moreover, we can assume that $t_n^{(s)} = 0$ and $t_i^{(s)} \neq 0$ for $i = 1, \dots, n-1$. Therefore,

$$\mathcal{A}([D_\infty^{(s)}]) \equiv \mathcal{A}([D_\infty^{(s)} - D_1]) \equiv -\mathcal{A}\Big(\Big[\sum_{i=1}^{n-1} \Phi(\zeta_\delta^s, t_i^{(s)}) - N \sum_{Q \in \text{pr}_x^{-1}(0)} Q\Big]\Big) \mod \Lambda.$$

Since $0 \notin X$ the sum over the integrals from P_0 to all $Q \in \text{pr}_x^{-1}(0)$ vanishes modulo the period lattice Λ (in fact this is true for any non-branch point). Let x_k be the branch point that is closest to 0, then for every $\omega_{\tilde{i},j} \in \mathcal{W}$ we have

$$\begin{aligned} \sum_{Q \in \text{pr}_x^{-1}(0)} \int_{P_0}^{Q} \omega_{\tilde{i},j} &= \sum_{l=0}^{m-1} \int_{P_0}^{(0, \zeta^l \sqrt[m]{f(0)})} \omega_{\tilde{i},j} \\ &\equiv m \int_{P_0}^{P_k} \omega_{\tilde{i},j} + \left(1 + \zeta^{-j} + \dots + \zeta^{-j(m-1)}\right) \int_{P_k}^{(0, \sqrt[m]{f(0)})} \omega_{\tilde{i},j} \\ &\equiv 0 \mod \Lambda \end{aligned}$$

by equation (24) and Theorem 7.3. If we take $Q_i^{(s)} = \Phi(\zeta_\delta^s, t_i^{(s)}) \in \mathcal{C} \setminus \mathcal{P}$, $i = 1, \ldots, n-1$, we are done:

$$-\mathcal{A}\Big(\Big[\sum_{i=1}^{n-1} \Phi(\zeta_\delta^s, t_i^{(s)}) - N \sum_{Q \in \mathrm{pr}_x^{-1}(0)} Q\Big]\Big) \equiv -\sum_{i=1}^{n-1} \int_{P_0}^{Q_i^{(s)}} \bar{\omega} \mod \Lambda.$$

□

In the case of Theorem 7.7 there exist additional relations between the vector integrals in (26) which we are going to establish now. Given $i \in \{1, \ldots, n-1\}$ and denoting $t^{(s)} = t_i^{(s)}$ we have that on $\tilde{\mathcal{C}}_{\mathrm{aff}}$

$$(\zeta_\delta^s, t^{(s)}) = (\zeta_\delta^s, \zeta_\delta^{-\nu s} t^{(\delta)}) \quad \text{for all } s = 1, \ldots, \delta.$$

Therefore, if we write $(x^{(s)}, y^{(s)}) := \Phi(\zeta_\delta^s, t^{(s)})$ and denote $Q^{(s)} = Q_i^{(s)}$, then

$$Q^{(s)} = (x^{(s)}, y^{(s)}) = (x^{(\delta)}, \zeta_\delta^{(\mu+\nu N)s} y^{(\delta)})).$$

The $Q^{(s)}$ having identical x-coordinates implies that there exists a $k \in \{1, \ldots, n\}$ such that

$$\int_{P_0}^{Q^{(s)}} \bar{\omega} \equiv \int_{P_0}^{P_k} \bar{\omega} + \int_{P_k}^{Q^{(s)}} \bar{\omega} \mod \Lambda,$$

while the relation between their y-coordinates yields

$$\int_{P_k}^{Q^{(s)}} \omega_{\tilde{i},j} = \zeta_\delta^{-(\mu+\nu N)sj} \int_{P_k}^{Q^{(\delta)}} \omega_{\tilde{i},j}$$

for all $\omega_{\tilde{i},j} \in \mathcal{W}$ and $s = 1, \ldots, \delta$. This proves the following corollary:

Corollary 7.8. *Under the assumptions of Theorem 7.7 and with the above notation we can obtain the image of $D_\infty^{(s)}$ under the Abel-Jacobi map for all $s = 1, \ldots, \delta$ from the $n-1$ vector integrals*

$$\int_{P_k}^{Q_i^{(\delta)}} \bar{\omega}, \quad i = 1, \ldots, n-1.$$

Unfortunately, this is just a special case. If $\mathrm{ord}_{P_\infty^{(s)}}(D_1)$ is greater than 1 (for instance, if $\delta \neq m$), the vertical line defined by $r - \zeta_\delta^s$ is tangent to the curve $\tilde{\mathcal{C}}_{\mathrm{aff}}$ at $(\zeta_\delta^s, 0)$ and cannot be used for our purpose.

Consequently, we must find another function. One possible choice here is the line defined by $r - t - \zeta_\delta^s$, which is now guaranteed to have a simple intersection with $\tilde{\mathcal{C}}_{\mathrm{aff}}$ at $(\zeta_\delta^s, 0)$ and does not intersect $\tilde{\mathcal{C}}_{\mathrm{aff}}$ in $(\zeta_\delta^{s'}, 0)$, $s \neq s'$.

The corresponding principal divisor is given by

$$E_2 = \mathrm{div}(r - t - \zeta_\delta^s) = \sum_{i=1}^{d} (t_i^{(s)} + \zeta_\delta^s, t_i^{(s)}) - \nu \sum_{k=1}^{n} \Phi^{-1}(x_k, 0) - N E_2',$$

where the $t_i^{(s)}$ are the zeros (up to multiplicity) of $h(t) = \prod_{k=1}^{n} (1 - x_k (t + \zeta_\delta^{(s)})^\nu t^M) - 1 \in \mathbb{C}[t]$, $d = \deg(h)$ and

$$E_2' = \begin{cases} (m - \frac{M+\nu}{N}) \Phi^{-1}(0,0), & \text{if } 0 \in X, \\ \sum_{Q \in \mathrm{pr}_x^{-1}(0)} \Phi^{-1}(Q), & \text{otherwise.} \end{cases} \tag{27}$$

Now,

$$D_2 := \mathrm{div}\left(\frac{y^M}{x^N} - \frac{x^\mu}{y^\nu} - \zeta_\delta^s\right)$$

is a principal divisor on $\mathcal{C}_{\mathrm{aff}}$ such that $\mathrm{ord}_{P_\infty^{(s)}}(D_2) = 1$.

Theorem 7.9. *Assume* $\mathrm{ord}_{P_\infty^{(s)}}(D_1) > 1$ *and* $0 \notin X$. *Then, for* $s = 1, \ldots, \delta$, *there exist points* $Q_1^{(s)}, \ldots, Q_{d-1}^{(s)} \in \mathcal{C} \setminus \mathcal{P}$ *such that*

$$\mathcal{A}([D_\infty^{(s)}]) \equiv -\sum_{i=1}^{d-1} \int_{P_0}^{Q_i^{(s)}} \bar{\omega} + \nu \sum_{k=1}^{n} \int_{P_0}^{P_k} \bar{\omega} \mod \Lambda,$$

where $d = n(\nu + M)$.

Proof. First note that $0 \notin X$ implies $d = \deg(h) = n(\nu + M)$. Moreover, our assumption implies $\mathrm{ord}_{P_\infty^{(s)}}(D_2) = 1$ so that we may assume $t_d^{(s)} = 0$ and $t_i^{(s)} \neq 0$ for $i = 1, \ldots, d-1$. Then,

$$\begin{aligned}\mathcal{A}([D_\infty^{(s)}]) \equiv& \mathcal{A}([D_\infty^{(s)} - D_2]) \\ \equiv& -\mathcal{A}\Big(\Big[\sum_{i=1}^{d-1} \Phi(t_i^{(s)} + \zeta_\delta^s, t_i^{(s)}) - \nu \sum_{k=1}^{n} (x_k, 0) - N \sum_{Q \in \mathrm{pr}_x^{-1}(0)} Q\Big]\Big) \mod \Lambda.\end{aligned}$$

Choosing the points $Q_i^{(s)} = \Phi(t_i^{(s)} + \zeta_\delta^s, t_i^{(s)}) \in \mathcal{C} \setminus \mathcal{P}$ and using the same reasoning as in the proof of Theorem 7.7 proves the statement. □

Remark 7.10. We can easily modify the statements of the Theorems 7.7 and 7.9 to hold for $0 \in X$, i.e. when 0 is a branch point. Using equation (25), the statement of Theorem 7.7 becomes

$$\mathcal{A}([D_\infty^{(s)}]) \equiv -\sum_{i=1}^{n-2} \int_{P_0}^{Q_i^{(s)}} \bar{\omega} + N(m - M) \int_{P_0}^{(0,0)} \bar{\omega} \mod \Lambda,$$

whereas, using equation (27), the statement of Theorem 7.9 becomes

$$\mathcal{A}([D_\infty^{(s)}]) \equiv -\sum_{i=1}^{d-1} \int_{P_0}^{Q_i^{(s)}} \bar{\omega} + \nu \sum_{k=1}^{n} \int_{P_0}^{P_k} \bar{\omega} + (Nm - M - \nu) \int_{P_0}^{(0,0)} \bar{\omega} \mod \Lambda,$$

with $d = (n-1)(\nu + M)$.

7.4 Reduction modulo period lattice

In order for the Abel-Jacobi map to be well defined we have to reduce modulo the period lattice $\Lambda = \Omega\mathbb{Z}^{2g}$, where $\Omega = (\Omega_A, \Omega_B)$ is the big period matrix, computed as explained in Section 4.

Let $v = \int_P^Q \bar{\omega} \in \mathbb{C}^g$ be a vector obtained by integrating the holomorphic differentials in $\mathcal{W}$. We identify $\mathbb{C}^g$ and $\mathbb{R}^{2g}$ via the bijection

$$\iota : v = (v_1, \ldots, v_g)^T \mapsto (\mathrm{Re}(v_1), \ldots, \mathrm{Re}(v_g), \mathrm{Im}(v_1), \ldots, \mathrm{Im}(v_g))^T.$$

Applying ι to the columns of Ω yields the invertible real matrix

$$\Omega_{\mathbb{R}} = \begin{pmatrix} \mathrm{Re}(\Omega_A) & \mathrm{Re}(\Omega_B) \\ \mathrm{Im}(\Omega_A) & \mathrm{Im}(\Omega_B) \end{pmatrix} \in \mathbb{R}^{2g \times 2g}.$$

Now, reduction of v modulo Λ corresponds bijectively to taking the fractional part of $\Omega_{\mathbb{R}}^{-1}\iota(v)$

$$v \bmod \Lambda \leftrightarrow \lfloor \Omega_{\mathbb{R}}^{-1}\iota(v) \rceil.$$

8 Computational aspects

8.1 Complexity analysis

We recall the parameters of the problem: we consider a superelliptic curve $\mathcal{C}$ given by $\mathcal{C}_{\mathrm{aff}} : y^m = f(x)$ with $f \in \mathbb{C}[x]$ separable of degree n. The genus g of $\mathcal{C}$ satisfies

$$g \leq \frac{(m-1)(n-1)}{2} = O(mn).$$

Let D be some desired accuracy (a number of decimal digits). The computation of the Abel-Jacobi map on $\mathcal{C}$ has been decomposed into the following list of tasks:

1. computing the $(n-1)$ vectors of elementary integrals,
2. computing the big period matrix $\Omega = (\Omega_A, \Omega_B)$ (13),
3. computing the small period matrix $\tau = \Omega_A^{-1}\Omega_B$ (14),
4. evaluating the Abel-Jacobi map at a point $P \in \mathcal{C}$,

all of these to absolute precision D.

Let $N(D)$ be the number of points of numerical integration. If $m = 2$, we have $N(D) = O(D)$ using Gauss-Chebychev integration, while $N(D) = O(D \log D)$ via double-exponential integration.

For multiprecision numbers, we consider (see [5]) that the multiplication has complexity $\mathcal{M}(D) = O(D \log^{1+\varepsilon} D)$, while simple transcendental functions (log, exp, tanh, sinh,...) can be evaluated in complexity $\mathcal{T}(D) = O(D \log^{2+\varepsilon} D)$. For complex m-th roots we also consider the complexity $\mathcal{T}(D)$ using $\exp(\frac{1}{m}\log(\cdot))$. Moreover, we assume that multiplication of a $g \times g$ matrix can be done using $O(g^{2.8})$ multiplications.

8.1.1 Computation of elementary integrals

For each elementary cycle $\gamma_e \in \Gamma$, we numerically evaluate the vector of g elementary integrals from (17) as sums of the form

$$I_{a,b} \approx \sum_{\ell=1}^{N} w_\ell \frac{u_\ell^{i-1}}{y_\ell^j},$$

where $N = N(D)$ is the number of integration points, w_ℓ, u_ℓ are integration weights and points, and $y_\ell = \tilde{y}_{a,b}(u_\ell)$.

We proceed as follows:

- for each ℓ, we evaluate the abscissa and weight u_ℓ, w_ℓ using a few [4] trigonometric or hyperbolic functions,
- we compute $y_\ell = \tilde{y}_{a,b}(u_\ell)$ using $n-2$ multiplications and one m-th root, as shown in §8.4.1 below;
- starting from $\frac{w_\ell}{y_\ell}$, we evaluate all g terms $w_\ell \frac{u_\ell^{i-1}}{y_\ell^j}$ each time either multiplying by u_ℓ or by $\frac{1}{y_\ell}$, and add each to the corresponding integral.

Altogether, the computation of one vector of elementary integrals takes

$$\mathcal{E}(D) = N(D)\mathcal{T}(D) + N(D)(n-2+\log D)\mathcal{M}(D) + N(D)g\mathcal{M}(D) \tag{28}$$

operations, so that depending on the integration scheme we obtain:

Theorem 8.1. *Each of the $(n-1)$ elementary vector integrals can be computed to precision D using*

$$O(N(D)\mathcal{M}(D)(g+\log D)) = \begin{cases} O(D^2 \log^{1+\varepsilon} D(g+\log D)) \text{ operations, if } m=2, \\ O(D^2 \log^{2+\varepsilon} D(g+\log D)) \text{ operations, if } m>2. \end{cases}$$

8.1.2 Big period matrix

One of the nice aspects of the method is that we never compute the dense matrix $\Omega_\Gamma \in \mathbb{C}^{g\times 2g}$ from Section 4, but keep the decomposition of periods in terms of the elementary integrals $\int_{\gamma_e} \omega_{i,j}$ in $\mathbb{C}^{g\times(n-1)}$.

Using the symplectic base change matrix S introduced in §4.4, the symplectic homology basis is given by cycles of the form

$$\alpha_i = \sum_{\substack{e\in E \\ l\in\mathbb{Z}/m\mathbb{Z}}} s_{e,l}\gamma_e^{(l)} \tag{29}$$

where $\gamma_e^{(l)} \in \Gamma$ is a generating cycle and $s_{e,l} \in \mathbb{Z}$ is the corresponding entry of S.

[4] this can be reduced to evaluating a few multiplications and at most one exponential.

We use (15) to compute the coefficients of the big period matrix (Ω_A, Ω_B), so that each term of (29) involves only a fixed number of multiplications.

In practice, these sums are sparse and their coefficients are very small integers (less than m), so that the change of basis is performed using $O(g^3 D \log^{1+\varepsilon} D)$ operations (each of the $O(g^2)$ periods is a linear combination of $O(g)$ elementary integrals, the coefficients involving precision D roots of unity).

However, we have no proof of this fact and in general the symplectic reduction could produce dense base change with coefficients of size $O(g)$, so that we state the following far from optimal result.

Theorem 8.2. *Given the $(n-1) \times g$ elementary integrals to precision D, we compute the big period matrix using $O(g^3(D+g)\log^{1+\varepsilon}(D+g))$ operations.*

8.1.3 Small period matrix

Finally, the small period matrix is obtained by solving $\Omega_A \tau = \Omega_B$, which can be done using $O(g^{2.8})$ multiplications.

8.1.4 Abel-Jacobi map

This part of the complexity analysis is based on the results of Section 7 and assumes that we have already computed a big period matrix and all related data.

Let $\mathcal{E}(D)$ be the number of operations needed to compute a vector of g elementary integrals (see (28)). The complexity class of $\mathcal{E}(D)$ in O-notation is given in Theorem 8.1.

Theorem 8.3.

(i) *For each finite point $P \in \mathcal{C}_{aff}$ we can compute $\int_{P_0}^{P} \bar{\omega}$ to precision D using $\mathcal{E}(D)$ operations.*

(ii) *For each infinite point $P_\infty \in \mathcal{C}$ we can compute a representative of $\int_{P_0}^{P_\infty} \bar{\omega} \mod \Lambda$ to precision D using*

- *n vector additions in $\mathbb{C}^g$, if $\delta = \gcd(m,n) = 1$,*
- *$n\mathcal{E}(D)$ operations in the case of Theorem 7.7,*
- *$n(n + \frac{m}{\delta})\mathcal{E}(D)$ operations in the case of Theorem 7.9.*

(iii) *Reducing a vector $v \in \mathbb{C}^g$ modulo Λ can be done using $O(g^{2.8})$ multiplications.*

Proof. (i) Follows from combining the results from §7.1 and Remark 7.4.

(ii) The statements follow immediately from §7.3.1, Theorem 7.7 and Theorem 7.9.

(iii) By §7.4, the reduction modulo the period lattice requires one $2g \times 2g$ matrix inversion and one multiplication.

□

8.2 Precision issues

As explained in §1.3, the ball arithmetic model allows to certify that the results returned by the Arb program [12] are correct. It does not guarantee that the result actually achieves the desired precision.

As a matter of fact, we cannot prove a priori that bad accuracy loss will not occur while summing numerical integration terms or during matrix inversion.

However, we take into account all predictable loss of precision:

- While computing the periods using equations (15) and (18), we compute a sum with coefficients
$$C_{a,b}^{-j} \left(\frac{b-a}{2}\right)^i \binom{i-1}{l} \left(\frac{b+a}{b-a}\right)^{i-1-l}$$
whose magnitude can be controlled a priori. It has size $O(g)$.

- The size of the coefficients of the symplectic reduction matrix are tiny (less than m in practice), but we can take their size into account before entering the numerical steps. Notice that generic HNF estimates lead to a very pessimistic estimate of size $O(g)$ coefficients.
- Matrix inversion of size g needs $O(g)$ extra bits.

This leads to increasing the internal precision from D to $D+O(g)$, the implied constant depending on the configuration of branch points.

Remark 8.4. In case the end result is imprecise by d bits, the user simply needs to run another instance to precision $D+d$ to reach the desired accuracy.

In fact, the mathematical quantities and the sequence of arithmetic operations performed in the algorithm remain the same. Now if the absolute error is reduced by d bits on input of an elementary operation this remains true on output; by induction this is true for the final result.

8.3 Integration parameters

8.3.1 Gauss-Chebychev case

Recall from §6.2 that we can parametrize the ellipse ε_r via $\varepsilon_r = \{\cosh(r+it) = \cos(t-ir), t \in]-\pi,\pi]\}$.

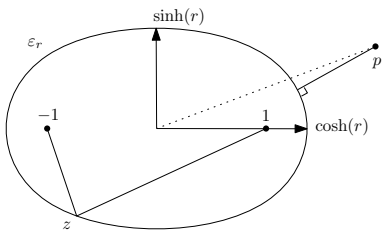


Figure 10: ellipse parameters.

The sum of its semi-axes is e^r and one needs

$$N \geq \frac{D + \log(2\pi M(r) + e^{-D})}{2r}$$

to have $|E(N)| \leq e^{-D}$.

The distance $d_k = \mathrm{dist}(u_k, \varepsilon_r)$ from a branch point $u_k \in U^+ \cup U^-$ to the ellipse ε_r can be computed applying Newton's method to the scalar product function $s(t) = \mathrm{Re}(\overline{z'}(u_k - z))$, where $z = \cos(t-ir)$ and we take $t = \mathrm{Re}(\arccos(u_k))$ as a starting point (see Figure 10). By convexity of the ellipse, the solution is unique on the quadrant containing u_k.

Choice of r Let $|u_k - 1| + |u_k + 1| = 2\cosh(r_k)$. We need to choose $r < r_0 = \min_k r_k$ (so that $u_k \notin \varepsilon_r$) in order to minimize the number of integration points (6.9). We first estimate how the bound $M(r)$ varies for $r < r_0$.

- For all k such that $r_k > r_0$, we compute explicitly the distance $d_k = \mathrm{dist}(u_k, \varepsilon_{r_0}) < \mathrm{dist}(u_k, \varepsilon_r)$.
- For all k such that $r_k = r_0$, we use first order approximation $\mathrm{dist}(u_k, Z_{r-\eta}) = \eta D_k + O(\eta^2)$, where $D_k = \left|\frac{\partial u_k}{\partial r_k}\right| = |\sin(t_k - ir_k)|$.

Let K be the number of branch points $u_k \in U^+ \cup U^-$ such that $r_k = r_0$ and

$$M_0 = \sqrt{\prod_{r_k = r_0} D_k \prod_{r_k > r_0} d_k}^{\,-1},$$

then the integrand is bounded on $\varepsilon_{r_0-\eta}$ by

$$M(r_0 - \eta) = M_0 \sqrt{\eta}^{-K}(1 + O(\eta)).$$

Plugging this into (6.9), the number of integration points satisfies

$$2N = \frac{D + \log(2\pi M_0) - K/2\log(\eta)}{r_0 - \eta}(1 + O(\eta)).$$

The main term is minimized for η satisfying $\eta\left(2\frac{D+\log(2\pi M_0)}{K} + 1 - \log(\eta)\right) = r_0$. The solution can be written as a Lambert function or we use the approximation

$$r = r_0 - \eta = r_0\left(1 - \frac{1}{A + \log\frac{A}{r_0}}\right),$$

where $A = 1 + \frac{2}{K}(D + \log(2\pi M_0))$.

8.3.2 Double-exponential case

For the double-exponential integration (§6.1) we use the parametrization

$$\partial Z_r = \{z = \tanh(\lambda\sinh(t + ir)), t \in \mathbb{R}\}$$

to compute the distance from a branch point $u_k \in U^+ \cup U^-$ to Z_r by Newton's method as before.

Unfortunately, the solution may not be unique, so once the parameter $r < r_0$ is chosen (see below), we use ball arithmetic to compute a rigorous bound of the integrand on the boundary of Z_r. The process consists in recursively subdividing the interval until the images of the subintervals by the integrand form an ε-covering.

Choice of r We adapt the method used for Gauss-Chebychev. This time the number N of integration points is obtained from equation (22).

Writing $u_k = \tanh(\lambda\sinh(t_k + ir_k))$, we must choose $r < r_0 = \min_k\{r_k\}$ to ensure $u_k \notin Z_r$. Let

$$M_0 = (\prod_{r_k = r_0} D_k \prod_{r_k > r_0} d_k)^{-j/m}$$

where $d_k = \mathrm{dist}(u_k, Z_{r_0}) < \mathrm{dist}(u_k, Z_r)$ and

$$D_k = \left|\frac{\partial u_k}{\partial r_k}\right| = \left|\frac{\lambda\cosh(t_k + ir_k)}{\cosh(\lambda\sinh(t_k + ir_k))^2}\right|$$

is such that $\mathrm{dist}(u_k, Z_{r-\eta}) = \eta D_k + O(\eta^2)$, then the integrand is bounded on $Z_{r_0-\eta}$ by

$$M_2 = M_0\eta^{-\frac{jK}{m}}(1 + O(\eta)).$$

Then

$$h = \frac{2\pi(r_0 - \eta)}{D + \log(2B(r_0, \alpha)M_0) - jK/m\log(\eta)} + O(\eta)$$

and the maximum is obtained for the solution η of $\eta(A - \log\eta) = r_0$ where $A = 1 + \frac{m}{jK}(D + \log(2B(r_0, \alpha)M_0))$.

8.4 Implementation tricks

Here we simply give some ideas that we used in our implementation(s) to improve constant factors hidden in the big-O notation, i.e. the absolute running time.

In practice, 80 to 90% of the running time is spent on numerical integration of integrals (15). According to §8.1.1, for each integration point $u_\ell \in]-1, 1[$ one first evaluates the y-value $y_\ell = \tilde{y}_{a,b}(u_\ell)$, then adds the contributions $w_\ell\frac{u_\ell^i}{y_\ell^j}$ to the integral of each of the g differential forms.

We shall improve on these two aspects, the former being prominent for hyperelliptic curves, and the latter when the $g \gg n$.

8.4.1 Computing products of complex roots

Following our definition (6), computing $\tilde{y}_{a,b}(u_\ell)$ involves $(n-2)$ m-th roots for each integration point.

Instead, we fall back to one single (usual) m-th root by computing $q(u) \in \frac{1}{2}\mathbb{Z}$ such that

$$\tilde{y}_{a,b}(u) = \zeta^{q(u)} \Big(\prod_{u_k \in U^-} (u - u_k) \prod_{u_k \in U^+} (u_k - u) \Big)^{\frac{1}{m}}. \tag{30}$$

This can be done by tracking the winding number of the product while staying away from the branch cut of the m-th root. For complex numbers $z_1, z_2 \in \mathbb{C}$ we can make a diagram of $\frac{\sqrt[m]{z_1}\,\sqrt[m]{z_2}}{\sqrt[m]{z_1 z_2}} \in \{1, \zeta, \zeta^{-1}\}$, depending on the position of z_1, z_2 and their product $z_1 z_2$ in the complex plane, resulting in the following lemma:

Lemma 8.5. *Let $z_1, z_2 \in \mathbb{C} \backslash]\infty, 0]$. Then,*

$$\frac{\sqrt[m]{z_1}\,\sqrt[m]{z_2}}{\sqrt[m]{z_1 z_2}} = \begin{cases} \zeta, & \text{if} \quad \mathrm{Im}(z_1), \mathrm{Im}(z_2) > 0 \quad \text{and} \quad \mathrm{Im}(z_1 z_2) < 0, \\ \zeta^{-1}, & \text{if} \quad \mathrm{Im}(z_1), \mathrm{Im}(z_2) < 0 \quad \text{and} \quad \mathrm{Im}(z_1 z_2) > 0, \\ 1, & \text{otherwise.} \end{cases}$$

For $z \in]\infty, 0]$ we use $\sqrt[m]{z} = \zeta^{\frac{1}{2}} \cdot \sqrt[m]{-z}$.

Proof. Follows from the choices for $\sqrt[m]{\cdot}$ and ζ that were made in §3.2. □

Lemma 8.5 can easily be turned into an algorithm that computes $q(u)$.

8.4.2 Doing real multiplications

Another possible bottleneck comes from the multiplication by the numerator u_ℓ, which is usually done $g - m - 1$ times for each of the N integration points (more precisely, as we saw in the proof of Proposition 3.8, for each exponent j we use the exponents $0 \le i \le n_i = \lfloor \frac{nj-\delta}{m} \rfloor$, with $\sum n_i = g$).

Without polynomial shift (18), this numerator would be $x_\ell = u_\ell + \frac{b+a}{b-a}$. However, x_ℓ is a complex number while u_ℓ is real, so computing with u_ℓ saves a factor almost 2 on this aspect.

8.5 Further ideas

8.5.1 Improving branch points

As we saw in Section 6, the number of integration points closely depends on the configuration of branch points.

In practice, when using double-exponential integration, the constant r is usually bigger than 0.5 for random points, but we can exhibit bad configurations with $r \approx 0.1$. In this case however, we can perform a change of coordinate by a Moebius transform $x \mapsto \frac{ax+b}{cx+d}$, as explained in Remark 3.3, to redistribute the points more evenly.

Improving r from 0.1 to say 0.6 immediately saves a factor 6 on the running time.

8.5.2 Near-optimal tree

As explained in §3.3 we integrate along the edges of a maximal-flow spanning tree $T = (X, E)$, where the capacity r_e of an edge $e = (a, b) \in E$ is computed as

$$r_e = \min_{c \in X \backslash \{a,b\}} \left\{ \left| \mathrm{Im}(\sinh^{-1}(\tanh^{-1}(\tfrac{2c-b-a}{b-a})/\lambda) \right|, \text{ if } m > 2. \right.$$

Although this can be done in low precision, computing r_e for all $(n-1)(n-2)/2$ edges of the complete graph requires $O(n^3)$ evaluations of elementary costs (involving transcendental functions if $m > 2$).

For large values of n (comparable to the precision), the computation of these capacities has a noticeable impact on the running time. This can be avoided by computing a *minimal spanning tree* that uses the euclidean distance between the end points of an edge as capacity, i.e. $r_e = |b - a|$, which reduces the complexity to $O(n^2)$ multiplications.

Given sufficiently many branch points that are randomly distributed in the complex plane, the shortest edges of the complete graph tend to agree with the edges that are well suited for integration.

8.5.3 Taking advantage of rational equation

In case the equation (1) is given by a polynomial $f(x)$ with small rational coefficients, one can still improve the computation of $\tilde{y}_{a,b}(u)$ in (30) by going back to the computation of $y(x_{a,b}(u)) = f(x)^{\frac{1}{m}}$. The advantage is that baby-step giant-step splitting can be used for the evaluation of $f(x)$, reducing the number of multiplications to $O(\sqrt{n})$. In order to recover $\tilde{y}_{a,b}(u)$, one needs to divide by $\sqrt[m]{1-u^2}$ and adjust a multiplicative constant including the winding number $q(u)$, which can be evaluated at low precision. This technique must not be used when u gets close to ± 1.

8.5.4 Splitting bad integrals or moving integration path

Numerical integration becomes quite inefficient when there are other branch points relatively close to an edge. The spanning tree optimization does not help if some branch points tend to cluster while others are far away. A simple example is given by the curve $y^2 = x(x-i)(x-1000)$: the branch point i is too close to the integration path $[0, 1000]$ and imposes a value $r = 0.04$ for Gauss-Chebychev integration and a better but still small $r = 0.2$ with double-exponential integration.

In a case like this, one can always split the bad integrals to improve the relative distances to the singularities: in the case of double-exponential integration, writing $\int_0^{1000} = \int_0^6 + \int_6^{1000}$ gives two integrals with $r = 0.48$ each. Splitting further at 2 and 33 gives $r = 0.63$.

Another option with double exponential integration, as explained in [20, II.3.5], is to shift the integration path that is used for the change of variable.

9 Examples and timings

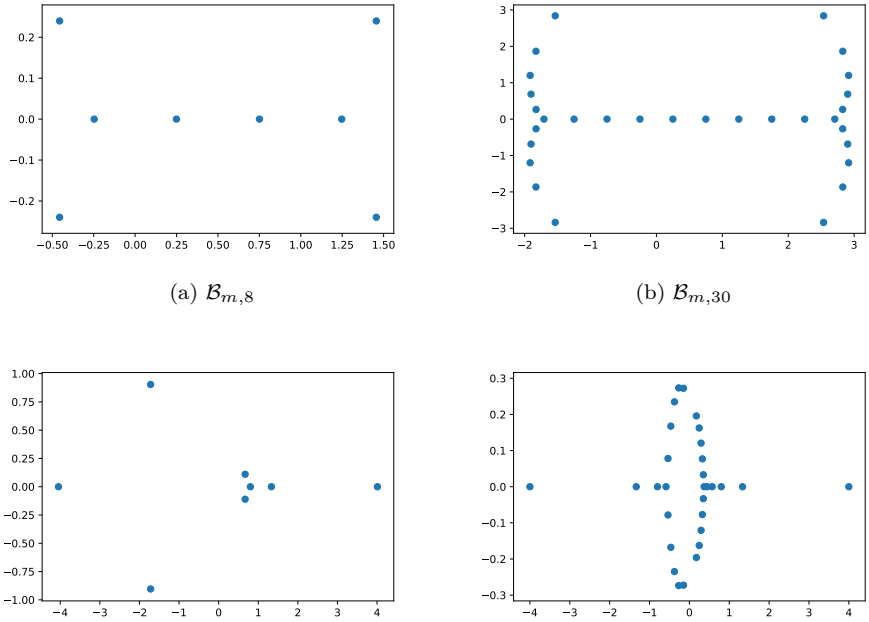
For testing purposes we consider a family of curves given by Bernoulli polynomials

$$\mathcal{B}_{m,n} : y^m = B_n(x) = \sum_{k=0}^{n} \binom{n}{k} b_{n-k} x^k$$

as well as their reciprocals

$$\widetilde{\mathcal{B}}_{m,n} : y^m = x^n B_n\left(\frac{1}{x}\right).$$

The branch points of these curves present interesting patterns which can be respectively considered as good and bad cases from a numerical integration perspective (Figure 11).



(a) $\mathcal{B}_{m,8}$ (b) $\mathcal{B}_{m,30}$

(c) $\widetilde{\mathcal{B}}_{m,8}$ (d) $\widetilde{\mathcal{B}}_{m,30}$

Figure 11: configurations of branch points.

In the case of hyperelliptic curves, we compare our timings with the existing Magma code [25] (see Tables 1 and 2). We obtain a huge speedup which is mostly due to the better integration scheme, but more interesting is the fact that the running time of our algorithm mainly depends on the genus and the precision, while that of Magma depends a lot on the branch points and behaves very badly in terms of the precision.

genus	curve	bits / digits	128 / 38	512 / 154	2000 / 600	4000 / 1200	10000 / 3000
3	$\mathcal{B}_{2,8}$	Arb	5e-3	0.01	0.16	0.48	3.99
		Magma (new)	0.05	0.08	0.44	2.16	25.3
		Magma (old)	0.33	0.44	6.28	421	—
	$\widetilde{\mathcal{B}}_{2,8}$	Arb	5e-3	0.01	0.17	0.54	4.58
		Magma (new)	0.06	0.11	0.67	3.42	40.6
		Magma (old)	0.42	0.45	6.44	457	—
14	$\mathcal{B}_{2,30}$	Arb	0.05	0.22	1.99	8.74	80.9
		Magma (new)	0.55	0.94	4.64	18.7	185.1
		Magma (old)	5.15	10.1	134	9291	—
	$\widetilde{\mathcal{B}}_{2,30}$	Arb	0.05	0.23	2.11	9.31	87.8
		Magma (new)	0.51	1.02	5.40	21.9	227
		Magma (old)	14.8	42.6	370	12099	—
39	$\mathcal{B}_{2,80}$	Arb	0.69	1.64	16.1	70.5	601
		Magma (new)	6.29	9.08	36.4	122	1024

Table 1: timings for hyperelliptic curves, single core Xeon E5 3GHz (in seconds).

genus	curve	bits / digits	128 / 38	512 / 154	2000 / 600	4000 / 1200	10000 / 3000
21	$\mathcal{B}_{7,8}$	Arb	0.06	0.27	4.25	29.5	455
		Magma (new)	0.23	1.06	14.6	83.1	1035
	$\widetilde{\mathcal{B}}_{7,8}$	Arb	0.03	0.19	7.44	58.8	1027
		Magma (new)	0.30	1.64	23.9	132	1613
84	$\mathcal{B}_{25,8}$	Arb	0.09	0.45	8.86	55.6	727
		Magma (new)	0.74	2.60	27.2	135	1529
87	$\mathcal{B}_{7,30}$	Arb	2.05	6.46	43.9	249	3091
		Magma (new)	2.29	10.0	93.8	461	4990
348	$\mathcal{B}_{25,30}$	Arb	2.82	9.57	101	557	6195
		Magma (new)	19.9	41.4	234	1014	9614
946	$\mathcal{B}_{25,80}$	Arb	67.8	182	952	4330	
		Magma (new)	369	585	2132	7474	

Table 2: timings for superelliptic curves, single core Xeon E5 3GHz (in seconds).

10 Outlook

In this paper we presented an approach based on numerical integration for multiprecision computation of period matrices and the Abel-Jacobi map of superelliptic curves given by $m > 1$ and squarefree $f \in \mathbb{C}[x]$.

Integration along a spanning tree and the special geometry of such curves make it possible to compute these objects to high precision performing only a few numerical integrations. The resulting algorithm has an excellent scaling with the genus and works for several thousand digits of precision.

10.1 Reduced small period matrix

For a given curve our algorithm computes a small period matrix τ in the Siegel upper half-space $\mathcal{H}_g$ which is arbitrary in the sense that it depends on the choice of a symplectic basis made during the algorithm.

For applications like the computation of theta functions it is useful to have a small period matrix in the Siegel fundamental domain $\mathcal{F}_g \subset \mathcal{H}_g$ (see [13, §1.3]).

We did not implement any such reduction. The authors of [13] give a theoretical sketch of an algorithm (Algorithm 1.9) that achieves this reduction step, as well as two practical versions (Algorithms 1.12 and 1.14) which work in any genus and have been implemented for $g \leq 3$. It would be interesting to combine this with our implementation.

10.2 Generalizations

We remark that there is no theoretical obstruction to generalizing our approach to more general curves.

10.2.1 Multiple roots

In a first step the algorithm could be extended to all complex superelliptic curves given by $m > 1$ and $f \in \mathbb{C}[x]$, where f can have multiple roots of order at most $m-1$, say $f = \prod_{k=1}^{n}(x - x_k)^{n_k}$. We want to highlight the following issues:

- The differentials are of the form $\frac{\prod_{k=1}^{n}(x-x_k)^{i_k}}{y^j}\mathrm{d}x$ where the exact condition on the holomorphicity is given in [14, Theorem 3]. However, these holomorphic differentials can still be integrated using double-exponential integration as presented in §6.1.

- The local monodromies may no longer be equal or even cyclic, but they are completely (up to conjugacy) determined by the multiplicities n_k. We believe that applying the Tretkoff algorithm [23] to obtain a homology basis and the intersections could be a better approach than generalizing the methods used in Section 5, although this seems possible.

Although several adjustments would have to be made in the analysis and in the code, staying within the superelliptic setting promises a fast and rigorous extension of our algorithm.

Moreover, this generalization would allow to perform any Moebius transform on the model of the curve and to efficiently implement the idea of §8.5.1.

10.2.2 General affine algebraic curves

We also believe that the strategy employed here (numerical integration between branch points combined with information about local intersections) could be adapted to completely general algebraic curves given by $F \in \mathbb{C}[x, y]$.

However, serious issues have to be overcome:

- On the numerical side we no longer have a nice m-th root function, it may be replaced by a combination of Newton's method between branch points (analytic continuation has to be performed on all sheets) and Puiseux series expansion around them.

- On the geometric side the combinatorics of loops and intersections become even more intricate than in the non-separable case 10.2.1. It is not clear whether our strategy based on shifting numbers and local intersection could be generalized. One can instead obtain the local monodromies from analytic continuation and then employ the Tretkoff algorithm [23], as described (for example) in [11].

We did not investigate further: at this point the advantages of superelliptic curves which are utilized by our approach are already lost (simple geometry of branch points and $m-1$ integrals at the cost of one). It is not clear whether this approach would be more efficient than methods that avoid branch points.

References

[1] Milton Abramowitz and Irene A. Stegun. *Handbook of mathematical functions with formulas, graphs, and mathematical tables*, volume 55 of *National Bureau of Standards Applied Mathematics Series*. For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C., 1964.

[2] Andrew R. Booker, Jeroen Sijsling, Andrew V. Sutherland, John Voight, and Dan Yasaki. A database of genus-2 curves over the rational numbers. *LMS Journal of Computation and Mathematics*, 19(A):235–254, 2016.

[3] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[4] Jean-Benoît Bost and Jean-François Mestre. Moyenne arithmético-géométrique et périodes des courbes de genre 1 et 2. *Gaz. Math.*, 1(38):36–64, 1988.

[5] Richard P. Brent and Paul Zimmermann. *Modern computer arithmetic*, volume 18 of *Cambridge Monographs on Applied and Computational Mathematics*. Cambridge University Press, Cambridge, 2011.

[6] M. M. Chawla and M. K. Jain. Error estimates for Gauss quadrature formulas for analytic functions. *Math. Comp.*, 22:82–90, 1968.

[7] Edgar Costa, Nicolas Mascot, Jeroen Sijsling, and John Voight. Rigorous computation of the endomorphism ring of a jacobian. *arXiv preprint arXiv:1705.09248*, 2017.

[8] John E. Cremona and Thotsaphon Thongjunthug. The complex AGM, periods of elliptic curves over $\mathbb{C}$ and complex elliptic logarithms. *J. Number Theory*, 133(8):2813–2841, 2013.

[9] Bernard Deconinck and Mark van Hoeij. Computing Riemann matrices of algebraic curves. *Phys. D*, 152/153:28–46, 2001. Advances in nonlinear mathematics and science.

[10] Jörg Frauendiener and Christian Klein. Computational approach to hyperelliptic riemann surfaces. *Letters in Mathematical Physics*, 105(3):379–400, 2015.

[11] Jörg Frauendiener and Christian Klein. Computational approach to compact Riemann surfaces. *Nonlinearity*, 30(1):138–172, 2017.

[12] F. Johansson. Arb: a C library for ball arithmetic. *ACM Communications in Computer Algebra*, 47(4):166–169, 2013.

[13] Pinar Kilicer, Hugo Labrande, Reynald Lercier, Christophe Ritzenthaler, Jeroen Sijsling, and Marco Streng. Plane quartics over $\mathbb{Q}$ with complex multiplication. *arXiv preprint arXiv:1701.06489*, 2017.

[14] Ja Kyung Koo. On holomorphic differentials of some algebraic function field of one variable over c. *Bulletin of the Australian Mathematical Society*, 43(3):399–405, 1991.

[15] Greg Kuperberg. Kasteleyn cokernels. *Electronic Journal of Combinatorics*, 9, 2002.

[16] Hugo Labrande. *Explicit computation of the Abel-Jacobi map and its inverse.* Theses, Université de Lorraine ; University of Calgary, November 2016.

[17] The LMFDB Collaboration. The L-functions and modular forms database. `http://www.lmfdb.org`, 2013. [Online; accessed 16 September 2013].

[18] Nicolas Mascot. Computing modular Galois representations. *Rend. Circ. Mat. Palermo (2)*, 62(3):451–476, 2013.

[19] Rick Miranda. *Algebraic Curves and Riemann Surfaces (Graduate Studies in Mathematics, Vol 5).* American Mathematical Society, 4 1995.

[20] Pascal Molin. *Intégration numérique et calculs de fonctions L.* PhD thesis, Université de Bordeaux I, 2010.

[21] Pascal Molin and Christian Neurohr. hcperiods: Arb and Magma packages for periods of superelliptic curves. `http://doi.org/10.5281/zenodo.1098275`, July 2017.

[22] Christopher Towse. Weierstrass points on cyclic covers of the projective line. *Transactions of the American Mathematical Society*, 348(8):3355–3378, 1996.

[23] C.L. Tretkoff and M.D. Tretkoff. Combinatorial group theory, riemann surfaces and differential equations. *Contemporary Mathematics*, 33:467–517, 1984.

[24] Paul van Wamelen. Equations for the jacobian of a hyperelliptic curve. *Transactions of the American Mathematical Society*, 350(8):3083–3106, 1998.

[25] Paul B. van Wamelen. Computing with the analytic Jacobian of a genus 2 curve. In *Discovering mathematics with Magma*, volume 19 of *Algorithms Comput. Math.*, pages 117–135. Springer, Berlin, 2006.