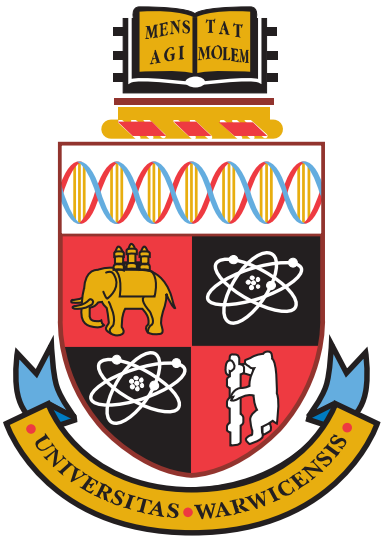


# $S$-integral points on hyperelliptic curves

by

**Homero Renato Gallegos Ruiz**

**Thesis**

Submitted to the University of Warwick

for the degree of

**Doctor of Philosophy**

**Mathematics**

December 2010

THE UNIVERSITY OF WARWICK

# Contents

# List of Tables

# List of Figures

# Acknowledgments

*To the glory of my God and Saviour, Jesus Christ.*
*For from Him and through Him and to Him are all things.*

*Dedicated to Noel, my little son. Perhaps some day he will read this work, and he will know that he has been a great motivation leading to the happy conclusion of this path of personal growth.*

I am grateful to my supervisor Samir Siksek. He is an example of great values in humankind: patience and encouragement. These virtues make him an excellent guide. His support has been instrumental to the accomplishment of this work.

I also thank the financial support of CONACyT, the Mexican Council of Science and Technology (Scholarship Number 160194). Without its support, my studies would not have been made real.

I would also like to thank my wife Martha. She has given me strength in moments of discouragement and weakness. She had the ability to endure times when I was not able to be with my family, and she sacrificed time of her own studies, for the sake of my academic progress. I thank my parents, Limberg and Betty; and my sister Marce; and Marcos, Lulú, Omar and Sofi. They signify the explanation of my presence in this world. Finally, I would like to thank the members of the Church Street Gospel Hall. They have been my true brothers and sisters in the Lord, and they are great examples of the spiritual transformation that God works in the lives of human beings.

## Agradecimientos [1]

*Para la gloria y la honra de mi Dios y Salvador, Jesucristo. Porque de Él, por Él y para Él son todas las cosas*

Para mi supervisor Samir Siksek, muestra de grandes valores del ser humano: paciencia y ánimo, que lo convierten en inmejorable guía. Su apoyo ha sido determinante para la realización de este trabajo.

Para el Consejo Nacional de Ciencia y Tecnología de México (Beca número 160194), sin cuyo respaldo mis estudios no hubieran tenido un lugar en el mundo de las realidades.

Para mi esposa, Martha, que me infundió fuerza en los momentos de desánimo y flaqueza; por su capacidad para entender que en aras del progreso académico tuve que sacrificar parte importante del tiempo de convivencia familiar.

Para mis padres, Limberg y Betty; mi hermana Marce, para Marcos, Lulú, Omar y Sofi, que significan la explicación de mi presencia en este mundo.

Para los miembros de la iglesia Church Street Gospel Hall, verdaderos hermanos en el Señor. Ellos son un gran ejemplo de la transformación espiritual que Dios obra en la vida de los seres humanos.

Para Noel, mi pequeño hijo. Algún día leerá este documento y sabrá que fue un motor cuya fuerza me llevó a concluir venturosamente este camino de crecimiento personal.

[1] Spanish version of the Acknowledgments

# Declarations

I declare that, except where acknowledged, the material contained in this thesis is my own work and it has not been submitted elsewere for the purpose of obtaining an academic degree.

Chapter 2 consists on standard material which is needed in the rest of the work.

The material in Chapter 3 has been accepted for publication in The International Journal of Number Theory.

Homero Renato Gallegos Ruiz.
December 2010.

# Abstract

Let $\mathcal{C} : Y^2 = a_n X^n + \cdots + a_0$ be a hyperelliptic curve with the $a_i$ rational integers, $n \geq 5$, and the polynomial on the right irreducible. Let $J$ be its Jacobian. Let $S$ be a finite set of rational primes. In this thesis we give explicit methods for finding all of the integral and $S$-integral points on $\mathcal{C}$. The work consists of the following parts.

1. We give a completely explicit upper bound for the size of the $S$-integral points on the model $\mathcal{C}$, provided we know at least one rational point on $\mathcal{C}$ and a Mordell–Weil basis for $J(\mathbb{Q})$. There is a refinement of the Mordell–Weil sieve that can then be used to determine all the $S$-integral points on the curve.

2. In the case the curve has genus $2$ and the polynomial defining the curve has real roots only, we reduce the upper bound for the size of the integral points to manageable proportions using linear forms in hyperelliptic logarithms. We then find all of the integral points on $\mathcal{C}$ by a direct search.

3. We give an algorithm for the computation of hyperelliptic logarithms of real points on genus $2$ curves defined by a polynomial having real roots only. This is needed for $2$.

We illustrate the practicality of the method by finding all the integral points on the curve $Y^2 = f(X) = X^5 - 5X^3 - X^2 + 3X + 1$, and all the $S$-integral points on the curve $Y^2 - Y = X^5 - X$ for the set $S$ of the first $22$ primes.

# Chapter 1

# Introduction

Consider the hyperelliptic curve with affine model

$$\mathcal{C} : Y^2 = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0, \tag{1.0.1}$$

where $a_0, \ldots, a_n$ are rational integers, $a_n \neq 0$, $n \geq 5$. Let $S$ be a finite set of rational primes. Siegel's theorem [40] states that (1.0.1) has only finitely many $S$-integral solutions. Siegel's theorem is superseded by Faltings' theorem [20] that states that there are only finitely many rational points on $\mathcal{C}$. Both Siegel's and Faltings' results are ineffective. That is, their proofs do not lead to an algorithm to determine all the rational points.

Using his theory of linear forms in logarithms, Baker [1] was the first to provide an effective result concerning the size of the integral points on $\mathcal{C}$. He showed that any integral point $(X, Y)$ on this affine model satisfies

$$\max(|X|, |Y|) \leq \exp\exp\exp\{(n^{10n} H)^{n^2}\}, \quad H = \max_{i=1,\ldots,n} \{|a_i|\}.$$

Baker's result has been improved and extended to solutions in algebraic integers and $S$-integers by many authors (see [43, 48, 36, 2, 3, 12]). Despite the improvements, the bounds remain astronomical and often involve inexplicit constants.

Recently, Bugeaud et al. [15] gave the first general practical method for explicitly

computing integral points on affine models (1.0.1) of hyperelliptic curves. Their method falls into two steps.

I. They give an upper bound for the size of integral points.

II. They describe a variant of the Mordell–Weil sieve capable of searching up to the bounds found in the first step.

In this thesis we give a method for explicitly computing $S$-integral points on hyperelliptic curves (1.0.1). As in [15], our strategy falls in two steps.

I'. We compute a completely explicit upper bound for the size of $S$-integral points. This step is based in part on the ideas for step (I) above in [15]. The method has to be completely reworked for the $S$-integral setting. We not only extend step (I) to the $S$-integral case, but we also improve on the bounds given in [15] for the size of the integral points. Nevertheless, the bounds are very large, and it is impractical to do a search for $S$-integral points up to the bound. This material also forms a 22-page paper [25] accepted for publication in The International Journal of Number Theory.

II'. We use one of the following methods.

(a) We try to reduce the bound found in Step (I') to manageable proportions, using lattice reduction. We show how the bound can be turned into an upper bound for the size of the coefficients of the linear combinations of the points on the Jacobian corresponding to integral points on the curve. We turn the linear combination in the Mordell–Weil group $J(\mathbb{Q})$ into linear forms in hyperelliptic logarithms. We give an upper bound for the linear forms and we use it to reduce the upper bound for the coefficients of the linear combination to manageable proportions.

(b) We use step (II) above to sieve up to the bounds found in Step (I').

As mentioned earlier, Step (I') has to be completely reworked from Step (I) for the $S$-integral setting.

i. We replace some of the bounds of Bugeaud and Győry [13] for the size of systems of fundamental units and the size of solutions to $S$-unit equations with more recent and sharper bounds due to Győry and Yu [27].

ii. We combine Matveev's bounds for linear forms in logarithms [31] with Yu's bounds for linear forms in $p$-adic logarithms [53] and an idea due to Voutier [49] to get an upper bound for the size of solutions of a particular type of $S$-unit equations.

iii. In [15] the authors use an upper bound for the regulator of a number field based on a theorem of Landau. The theorem of Landau actually bounds the product of the regulator and the class number, which we need to bound in our case.

iv. Our bounds for the size of the $S$-integral solutions on (1.0.1) depend on the class number of some number field. We use an upper bound for the class number due to Lenstra [28].

The improvements on the first step are the following. First, our constants are smaller than those in [15], and do not depend on parameters related to Lehmer's problem. This is due to the improvement on systems of fundamental $S$-units we use. Moreover, though Voutier's idea had been already used to give effective upper bounds for the size of $S$-integral solutions in [12], the bounds were inexplicit. Our bounds are completely explicit and they are based on more recent estimates for linear forms in logarithms than those used in [12].

Step (II')-(a) in its present form can only be used to find integral points on $\mathcal{C}$ when the genus of the curve is $2$, and when the polynomial defining the curve has real roots only. The generalisation of the method to polynomials with complex roots defining genus $2$ curves is work in progress.

Step (II')-(b) is practically unchanged with respect to step (II) above, and we merely summarise what we need for it from [15].

We need the following assumptions for all steps:

a. The knowledge of at least one rational point $P_0$ on $\mathcal{C}$.

b. The knowledge of a Mordell–Weil basis for $J(\mathbb{Q})$ where $J$ is the Jacobian of $\mathcal{C}$.

For the second step we also need to assume that the canonical height $\hat{h} : J(\mathbb{Q}) \to \mathbb{R}$ is explicitly computable and that we have explicit upper and lower bounds for the difference

$$\mu_1 \leq h(D) - \hat{h}(D) \leq \mu_2. \tag{1.0.2}$$

For step (II')-(a) we further require that generators of $J(\mathbb{Q})$ are divisors supported by points on $\mathcal{C}(\mathbb{R})$ only.

The assumption that we know a point on the curve brings simplifications to our method. As remarked in [15], if we do not know any rational point on the curve, it is possible that there are no rational points at all. This can be proved using the techniques of Bruin and Stoll [9, 10, 11].

We have made most of the necessary computations with the computational algebra system `MAGMA` [5]. Some computations have been performed with the Mathematica system [52].

The thesis is arranged as follows. Chapter 2 outlines the existing methods for the computation of the bounds for the height difference, and the computation of the Mordell–Weil group. It consists on standard material, but it is needed to set up notation which will be used throughout the thesis. Chapter 3 is concerned with the computation of the upper bounds for the size of the $S$-integral points on the affine model 1.0.1. It also explains how one can completely determine all the $S$-integral points using the variant of the Mordell–Weil sieve found in [15]. Chapter 5 deals with the reduction of the upper bounds obtained in Chapter 3 for the particular case of integral points on genus $2$ hyperelliptic curves. The method requires the computation of the periods of the curve, and hyperelliptic logarithms of degree $0$ divisors on $\mathcal{C}$ to high precision. In Chapter 4 we

present an algorithm of Bost and Mestre [6] for the computation of the periods, and we work on an extension of it so that we can also compute the hyperelliptic logarithms.

We now briefly describe the available tools for the solution of Diophantine hyperelliptic equations. After Siegel's proof of the finiteness of the number of $S$-integral points on curves of higher genus, effective methods for finding all the $S$-integral points on hyperelliptic curves have been developed. Some of them are not general, and those that are general are often impractical or inexplicit.

1. **Chabauty's method**. Chabauty [17] proved that a curve of genus $g \geq 2$ has a finite number of rational points whenever the rank of the Mordell–Weil group of its Jacobian is strictly less than $g$. His proof often leads to a sharp bound on the number of points on $\mathcal{C}$. If the bound is attained, then one has not only the integral points, but *all* the rational points. This requires knowledge of generators for the Mordell–Weil group or a subgroup of finite index. For notes on the application of this method see [16, Chapter 13] or [32]. The examples we present in this thesis are genus $2$ curves with Mordell–Weil rank $\geq 2$, so Chabauty's method does not apply. There are also some variants of Chabauty's method (as Elliptic Curve Chabauty [7], [8], [23], [24]) that can determine all the rational points on a hyperelliptic curve, but they are also limited to curves of small rank.

2. **Bilu and Hanrot's variant of Baker's method** Bilu and Hanrot [4] have produced a method to solve superelliptic Diophantine equations (i.e. of the form $Y^m = f(X)$ with $m \geq 3$) which computes an upper bound for the size of the integral points. Their method does not involve Thue or unit equations since they compute directly a linear form in logarithms from a careful analysis of some number fields. The upper bound they get is huge, but it is then reduced by an application of the LLL-algorithm. The authors claim that one can adjust the method to the hyperelliptic case, but they do not do it explicitly. The method needs some computations of class groups of number fields of large degree ($\geq 20$) that in many cases in practice are beyond the present abilities of computer algebra.

3. **Baker's method and the Mordell–Weil sieve**. A third method is the one we have mentioned before: Baker's method combined with the variant of the Mordell–Weil sieve [15] to find the integral points. This is the more general method, as it does not depend on the genus, and it does not involve computations of unit groups, but only bounds on the regulator of large degree number fields which are easy to compute. Nevertheless, the computations for the Mordell–Weil sieve can be expensive. Thus, one would like to reduce the upper bound obtained from Baker's method as much as possible, to sieve up to a not so large bound, or not to have to sieve at all.

# Chapter 2

# The Mordell–Weil group

The methods we use for the complete solution to hyperelliptic Diophantine equations depend heavily on computing explicit generators for the Mordell–Weil group $J(\mathbb{Q})$, which is finitely generated by the Mordell–Weil theorem. The purpose of this chapter is to set up the notation on Jacobians that we will use throughout the thesis and gather the standard results on Jacobians we will need. We will also describe what are the existing tools to explicitly compute generators for $J(\mathbb{Q})$. The strategy is mainly inspired by the elliptic case. One needs to explicitly compute the canonical height of a point on the Jacobian. One also needs to compute the rank of the curve. Then one looks for generators of $J(\mathbb{Q})/2J(\mathbb{Q})$. Finally, one extends that set of generators to a complete set of generators for $J(\mathbb{Q})$.

The chapter is arranged as follows. Section 2.1 presents the basic definitions about hyperelliptic curves and Jacobians. Section 2.2 gathers results by Flynn, Smart and Stoll related to the explicit computation of lower and upper bounds for the height difference which lead to the explicit computation of the canonical height. Section 2.3 deals with the computation of the rank of the curve and the $2$-descent. Finally, Section 2.4 explains how one can perform the infinite descent to compute a complete set of generators for $J(\mathbb{Q})$.

## 2.1 Basic definitions and theorems

The following definitions and results are standard and are taken from Chapters 1-3 in [16]. Let $\mathcal{C}$ be a hyperelliptic curve of genus $2$ defined over $\mathbb{Q}$ given by an affine model of the form

$$\mathcal{C}: \quad Y^2 = f(X),$$

where

$$f(X) = f_6X^6 + f_5X^5 + f_4X^4 + f_3X^3 + f_2X^2 + f_1X + f_0,$$

where the $f_i$s are all integers and $f_6$ is not zero and $f(x)$ has no multiple factors. Every genus $2$ hyperelliptic curve over $\mathbb{Q}$ is birationally equivalent over $\mathbb{Q}$ to a curve of this type, which is unique up to a fractional linear transformation in $X$, and an associated transformation in $Y$.

When dealing with the degree $6$ affine model of a hyperelliptic curve one should bear in mind that the corresponding projective model in $\mathbb{P}^2$ has a singularity at infinity. But we think instead on a complete non-singular model, either in a weighted projective space $\mathbb{P}_{X,Y,Z}(1,3,1)$ or the model in $\mathbb{P}^4$ resulting from blowing up the singularity at infinity (see [16, Chapter 1, Section 1]). This means that as a double cover of $\mathbb{P}^1$, the curve $\mathcal{C}$ has two points over $\infty$. They are traditionally named $\infty_+$ and $\infty_-$, according to the sign of $Y/X^3$ along the corresponding branch (see for instance [16, p. 77]). We will also consider affine models given by a degree $5$ polynomial $f$. In this case there is only one point over the point at infinity in $\mathbb{P}^1$ which is traditionally named $\infty$ as well. Hopefully, in the rest of the work it will be clear from the context whether we are talking about the point $\infty \in \mathbb{P}^1$ or the point $\infty \in \mathcal{C}$.

**Definition.** The *Jacobian of* $\mathcal{C}$ is defined as $J(\mathcal{C}) = \mathrm{Pic}^0(\mathcal{C})$, i.e. degree $0$ divisors modulo linear equivalence.

Let $P$ be a point of $\mathcal{C}$, $P = (x, y)$. We say that the point $\bar{P} = (x, -y)$ is the *conjugate* of $P$. A divisor of degree $2$ of the type $P + \bar{P}$ is the intersection of $\mathcal{C}$ with $X = x$. We see then that any two divisors of this type are linearly equivalent.

Denote the corresponding element of $\mathrm{Pic}^2(\mathcal{C})$ by $D$. We will choose $\infty_+ + \infty_-$ as a representative for $D$. Since $D$ is the canonical class, the Riemann Roch Theorem implies that any other element of $\mathrm{Pic}^2(\mathcal{C})$ contains precisely one effective divisor $P+Q$ fixed as a pair by $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ (see [16, Chapter 1, Section 1]). We will identify any such element of $\mathrm{Pic}^2(\mathcal{C})$ with its unique effective divisor. We can identify $\mathrm{Pic}^0(\mathcal{C})$ with $\mathrm{Pic}^2(\mathcal{C})$ via addition by $D$. Doing so identifies $0 \in \mathrm{Pic}^0(\mathcal{C})$ with $D$. We will in general express points on the Jacobian other than $0$ in the form $P+Q-D$, where $P$ and $Q$ are not conjugate under the hyperelliptic involution.

Let $P_0$ be a rational point on $\mathcal{C}$. Sometimes we will want to express points in the Jacobian in the form $P'+Q'-2P_0$. We will do it in the following way. Let $P+Q-D$ be an element in $J(\mathcal{C})$. Consider the divisor $D' = P+Q-D+P_0-\bar{P}_0 \in \mathrm{Pic}^0(\mathcal{C})$. In general, $D'$ will not be linearly equivalent to $0$. Let $P'+Q'$ be the only degree $2$ effective divisor such that $P'+Q'-D$ is linearly equivalent to $D'$. Then the divisor $P'+Q'-2P_0$ is linearly equivalent to $D'+D-2P_0$, which is linearly equivalent to $P+Q-P_0-\bar{P}_0$, which is linearly equivalent to $P+Q-D$.

The Jacobian of the curve $J(\mathcal{C})$ can also be thought of as an algebraic variety whose points correspond to the elements of $\mathrm{Pic}^0(\mathcal{C})$. In [16, Chapter 2] the authors describe explicitly this variety as the intersection of $72$ quadrics in $\mathbb{P}^{15}$ and they also give explicit maps taking divisors of the form $P+Q-D$ to the algebraic variety.

The model of the Jacobian variety in $\mathbb{P}^{15}$ is a large object, difficult to manipulate. There is another variety associated to $J(\mathcal{C})$ that retains much of the information of the Jacobian which is much simpler, the *Kummer surface* $\mathcal{K} = \mathcal{K}(\mathcal{C})$. This is a quartic surface in $\mathbb{P}^3$. We take its definition from [16, Chapter 3]. We define $\mathcal{K}$ as the projective locus in $\mathbb{P}^3$ of the map given by

$$P+Q-D \in J(C) \mapsto (k_1,k_2,k_3,k_4) = (1, x+u, xu, (F_0(x,u)-2yv)/(x-u)^2),$$

where $P=(x,y)$, $Q=(u,v)$, $P \neq Q$, and

$$F_0(x,u) = 2f_0+f_1(x+u)+2f_2xu+f_3xu(x+u)+2f_4(xu)^2+f_5(xu)^2(x+u)+2f_6(xu)^3.$$

The Kummer surface is then given by a quartic equation

$$R(k_1, k_2, k_3)k_4^2 + S(k_1, k_2, k_3)k_4 + T(k_1, k_2, k_3) = 0, \tag{2.1.1}$$

where $R, S$ and $T$ are homogeneous of degree $2, 3$ and $4$ respectively. These polynomials can be found in Chapter 3 of [16]. We can extend the map to pairs of points $P, Q$ that include the points at infinity, and to pairs of the form $P, P$. The values are the following, according to Flynn and Smart [22]. For pairs $P, P$ where $P$ is not one of the points at infinity, $k_1, k_2, k_3$ are as above, and $k_4$ is uniquely determined by Equation (2.1.1). If the pair is of the form $(x, y), \infty_{\pm}$, then $k_1 = 0, k_2 = 1, k_3 = x_1, k_4 = f_5x^2 + 2f_6x_1^3 - (\pm 2y\sqrt{f_6})$. The pair $\infty_+, \infty_-$ is mapped to $(0, 0, 0, 1)$ and if the pair consists of two equal points at infinity, the corresponding point on the Kummer surface is $(0, 0, 1, k_4)$ where $k_4$ can be determined from equation (2.1.1). We remark that the Jacobian variety is a double cover of the Kummer surface (see [16, Chapter 3, Section 8]).

Finally, we state the Mordell–Weil Theorem. The proof for the general theorem on Abelian varieties over number fields can be found in Serre's book [39, Chapter 4].

**Theorem 2.1.1.** *The group of points on $J(\mathcal{C})$ defined over $\mathbb{Q}$ is a finitely generated abelian group.*

## 2.2 Bounds for the height difference

We define a naive height on $\mathcal{K}$ as the restriction of the naive height in $\mathbb{P}^3$: let $(x_0, x_1, x_2, x_3)$ be the homogeneous coordinates of a point in $\mathbb{P}^3(\mathbb{Q})$. Multiplying by a nonzero constant, we can assume that the $x_i$s are all integers having $1$ as their greatest common divisor. We define the (exponential) *naive height of* $(x_0, x_1, x_2, x_3)$ as $\max(|x_0|, |x_1|, |x_2|, |x_3|)$. We will normally consider the *logarithmic naive height*, that is, the logarithm of the naive height.

**Definition.** The *naive height* or *logarithmic height of a point $Q$* on the Jacobian variety

of $\mathcal{C}$ is the logarithmic naive height of the corresponding point on the Kummer surface. We denote the naive height of $Q$ by $h(Q)$.

This is much easier than computing heights directly on $\mathbb{P}^{15}$ where $J(\mathcal{C})$ is embedded. Note as well that the set of points

$$\{P \in J(\mathbb{Q}) : h(P) \leq B\}$$

is finite since the set in $\mathbb{P}^3$ consisting of points of height $\leq B$ is finite and the Jacobian is a double cover of the Kummer surface. Taking advantage of the group law on the Jacobian, one can also define another height, the *canonical height*, by

$$\hat{h}(P) = \lim_{n\to\infty} \frac{1}{n^2} h(nP).$$

For many hyperelliptic curves, the canonical height of a given point $P$ on $J(\mathbb{Q})$ is explicitly computable. Flynn and Smart [22] were the first to give an algorithm for the computation of the canonical height. The algorithm has since been improved, in particular by Stoll [44, 46]. Stoll's algorithm has been implemented in the Computer Algebra system `MAGMA` and it is the one we use.

We explain now how we can find real constants $\mu_1$ and $\mu_2$ bounding the height difference

$$\mu_1 \leq h(Q) - \hat{h}(Q) \leq \mu_2. \tag{2.2.1}$$

The idea behind obtaining such bounds is approximating the distance from a given point to twice the point. Let $P$ be a point on $J(\mathcal{C})$. Denote by $\mathbf{k}_P = (k_1, k_2, k_3, k_4)$ the corresponding point on the Kummer surface. The coordinates of $\mathbf{k}_{2P}$ are given by quartics in terms of the $k_i$s, and we denote them by $(\delta_1, \delta_2, \delta_3, \delta_4)$. The equations for those quartics are given in [21] and they are too large to be reproduced here. Following [22] we define a local error function for every prime $p$, including the infinite prime:

$$\varepsilon_p(\mathbf{k}_P) = \log(\max_{i=1,\ldots,4}\{|\delta_i(\mathbf{k}_P)|_p\}) - 4\log(\max_{i=1,\ldots,4}\{|k_i|_p\}).$$

It can be shown (see [22]) that for all primes of good reduction the error function vanishes. For the remaining primes upper and lower bounds can be computed. We now show how to bound the error function in the infinite case.

**Lemma 2.2.1.** *An upper bound for $\varepsilon_\infty$ is given by*

$$\mu_1^{(\infty)} = \log(\max_{i=1,\dots,4}\left\{\sum \textit{absolute value of the coefficients of } \delta_i\right\}).$$

*Proof.* Multiplying by a constant we can assume that the maximum of the absolute value of the entries of $\mathbf{k}_P$ is one. Then

$$\max_i\{|\delta_i(k_1,k_2,k_3,k_4)|\} \leq \max_{i=1,\dots,4}\left\{\sum \text{absolute value of the coefficients of } \delta_i\right\}.$$

Because of our assumption for $\mathbf{k}$,

$$\varepsilon_\infty = \log(\max_i\{|\delta_i(k_1,k_2,k_3,k_4)|\}).$$

The result follows. □

We could find a sharper bound for $\varepsilon_\infty$, but this one will be enough for our purposes. A lower bound for $\varepsilon_\infty$ can be obtained using numerical techniques such as steepest descent.

Obtaining sharp lower bounds for the finite primes is the subject of [44, 46]. In [22] the authors show that $0$ is always an upper bound for the local error function at the finite primes.

The following theorem gives the desired lower and upper bounds for the height difference. This is Theorem 4 in [22].

**Theorem 2.2.2.** *For every prime $p$, including the infinite prime, let $\mu_1^{(p)}, \mu_2^{(p)}$ be non-negative real constants such that*

$$\mu_1^{(p)} \geq \varepsilon_p(\mathbf{k}_P) \geq -\mu_2^{(p)}$$

*for all $P \in J(\mathbb{Q})$, where all but finitely many of the $\mu_1^{(p)}, \mu_2^{(p)}$ are $0$. Define $\mu_1 = -\frac{1}{3}\sum_p \mu_1^{(p)}$ and $\mu_2 = \frac{1}{3}\sum_p \mu_2^{(p)}$. Then, for all $P \in J(\mathbb{Q})$ we have*

$$\mu_1 \leq h(P) - \hat{h}(P) \leq \mu_2.$$

For the computation of the canonical height and for finding generators of the Mordell–Weil group $J(\mathbb{Q})$ one only needs the upper bound $\mu_2$ for the height difference. MAGMA's package dealing with hyperelliptic curves does not implement the lower bound. Nevertheless, we will use the lower bound $\mu_1$ obtained from Lemma 2.2.1 in Chapter 5 to relate upper bounds for the naive height of the integral points on $\mathcal{C}$ to upper bounds for linear forms in hyperelliptic logarithms. We will also need it in Section 3.8.

*Remark.* The existence of the bounds $\mu_1, \mu_2$ for the height difference implies that the set of points

$$\{P \in J(\mathbb{Q}) : \hat{h}(P) \leq B\}$$

is finite for a given positive real number $B$. Then, the intersection of the image under $\hat{h}$ of $J(\mathbb{Q})$ with the interval $[0, B] \subset \mathbb{R}$ is a finite set. It follows that $\hat{h}(J(\mathbb{Q}))$ is a discrete subset of $\mathbb{R}$

## 2.3 Computing the rank of $J(\mathbb{Q})$ – $2$-descent.

There is no algorithm known so far that provably determines the rank of the Mordell–Weil group $J(\mathbb{Q})$. But many algorithms have been developed to give upper and lower bounds for it ([37, 38, 45]). In many cases the bounds coincide and then one knows the rank. In this section we outline the main ideas behind such bounds.

The proof of the Mordell–Weil theorem looks at the quotient $J(\mathbb{Q})/mJ(\mathbb{Q})$. The finiteness of the quotient implies that $J(\mathbb{Q})$ is finitely generated. Normally, one looks at the case $m = 2$, as the multiplication by $2$ map is available as an isogeny defined over $\mathbb{Q}$ and has low degree. Up to the computation of the torsion, one can deduce the rank of $J(\mathbb{Q})$ from the structure of $J(\mathbb{Q})/2J(\mathbb{Q})$ once the torsion subgroup has been computed. The computation of generators for $J(\mathbb{Q})/2J(\mathbb{Q})$ is known as $2$-*descent*.

Stoll gives an algorithm for the computation of the torsion subgroup $J(\mathbb{Q})_{\text{tors}}$ in [44]. The idea of the algorithm is first computing the group $J(\mathbb{F}_p)$ for some small primes $p$ of good reduction. The order of the rational torsion subgroup must divide the greatest

common divisor $g$ of the orders of the groups $J(\mathbb{F}_p)$. Since the rational torsion subgroup is a finite abelian group, it suffices to compute the $q$-parts for all primes dividing the order of the group. Only primes dividing $g$ can occur. Then, for every prime $q$ dividing $g$ one takes a prime of good reduction $p \neq q$. Then one tries to lift points on $J(\mathbb{F}_p)[q^n]$ to $J(\mathbb{Q})$. One does so lifting them first to $J(\mathbb{Q}_p)$ and finally a computation of heights decides whether the point can indeed be lifted or not.

An upper bound for the rank is obtained from the $2$-Selmer group, as explained in [45]. Once we get an upper bound $r'$ for the rank, we try to search for points on the Jacobian until we get $r'$ independent elements. If that is the case we then know that $r'$ equals the rank of the curve. We can search for points on the Jacobian up to certain height $c$ by looking for points on the Kummer surface with naive logarithmic height at most $c + \mu_2$, as long as $c + \mu_2$ is not too large ($< 10$).

In order to test whether a finite set $W \subset J(\mathbb{Q})/J(\mathbb{Q})_{\text{tors}}$ is a linearly independent set in $J(\mathbb{Q})$ we need the following definition.

**Definition.** The *height pairing on* $J(\mathbb{Q})$ is the bilinear form

$$\langle \cdot, \cdot \rangle : J(\mathbb{Q}) \times J(\mathbb{Q}) \to \mathbb{R}$$

given by

$$\langle P, Q \rangle = \frac{1}{2}(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)).$$

Let $P_1, \ldots, P_n$ be a sequence of points on $J(\mathbb{Q})$. The *height pairing matrix* of the given points is the matrix with entries

$$\langle P_i, P_j \rangle.$$

The bilinearity of the height pairing follows from the standard fact that the canonical height is a positive definite quadratic form on $J(\mathbb{Q})$. The determinant of the height pairing matrix of a sequence of points on $J(\mathbb{Q})$ is $0$ if and only if the points are not an independent set in $J(\mathbb{Q})/J(\mathbb{Q})_{\text{tors}}$. Once we are able to compute explicitly the canonical height, we have a very useful tool to test for linear independence in $J(\mathbb{Q})$ without the knowledge of an explicit basis.

Once we find $r$ linearly independent elements in $J(\mathbb{Q})$ we test if they, together with the torsion points, generate $J(\mathbb{Q})/2J(\mathbb{Q})$. We do it by testing if they are not the double of another point on $J(\mathbb{Q})$. We can test whether a point of infinite order $P$ is not the double of a point $Q \in J(\mathbb{Q})$ using heights. If $P = 2Q$, then $\hat{h}(Q) = 1/4\hat{h}(P)$, as we can see from the definition of $\hat{h}$. We then can look for points $Q$ on $J(\mathbb{Q})$ of canonical height at most $1/4\hat{h}(P)$ and see whether $2Q = P$ or not.

## 2.4 The infinite descent

The procedure that computes a set of generators for the full Mordell–Weil group out of a set of generators for $J(\mathbb{Q})/2J(\mathbb{Q})$ is known as *infinite descent*. There are different ways of performing the infinite descent (see [22, 46]). We will use a simple method due to Zagier [41, Proposition 7.2].

**Theorem 2.4.1** (Zagier)**.** *Let $S_c = \{P \in J(\mathbb{Q}) : \hat{h}(P) \leq c\}$. If $S_c$ contains a full set of representatives for $J(\mathbb{Q})/mJ(\mathbb{Q})$ $(m > 1)$, then $J(\mathbb{Q})$ is generated by $S_c$.*

*Proof.* The proof in [41] also applies in the hyperelliptic case. We repeat it here for completeness.

Let $J_1$ be the subgroup of $J(\mathbb{Q})$ generated by $S_c$. Suppose that $J_1 \neq J(\mathbb{Q})$. Then choose a $Q \in J(\mathbb{Q})$, with $Q \notin J_1$ of minimal height. This is possible, since $\hat{h}(J(\mathbb{Q}))$ is a discrete subset of $\mathbb{R}$ (see last remark in Section 2.2). Since $Q \notin S_c$ we have $\hat{h}(Q) > c$. Choose $P \in S_c$ with $P \equiv Q \pmod{mJ(\mathbb{Q})}$, so $P = Q + mR$ for some $R \in J(\mathbb{Q})$. We note that $R \notin J_1$ because of our assumption on $Q$.

Now note that

$$\begin{aligned}\hat{h}(R) &= \frac{1}{m^2}\hat{h}(P - Q) \leq \frac{2}{m^2}(\hat{h}(P) + \hat{h}(Q)) \\ &\leq \frac{2}{m^2}(c + \hat{h}(Q)) < \frac{4}{m^2}\hat{h}(Q) \\ &\leq \hat{h}(Q),\end{aligned}$$

since $m \geq 2$. Since $R \notin J_1$ this is a contradiction to the minimality of $Q$ and hence proves the proposition. □

Once we know a set of generators for $J(\mathbb{Q})/2J(\mathbb{Q})$, we compute the heights of representatives of every class modulo $2J(\mathbb{Q})$. Let $c$ be the maximum of those heights. Then, the set $S_c$ satisfies the conditions of the theorem and we know it generates the full Mordell–Weil group. If the height of one of the generators is very large, or if the rank is very large, then Zagier's theorem might be impractical, and one would need to use the lattice enlargement procedures and the sieving techniques from [22, 46].

**Example 2.4.2.** Let $\mathcal{C}$ be the genus $2$ curve defined by the equation

$$y^2 = 4x^5 - 4x + 1.$$

This curve is equivalent to that in Theorem 1.1 of [15]. There the authors compute the Mordell–Weil group of the curve, and we check here the computations to illustrate the methods presented in this chapter.

Using `MAGMA` we find some rational points on the curve.

$$\infty,\ (-1,\pm 1),\ (0,\pm 1),\ (1,\pm 1,1),\ (2,\pm 11),$$
$$(3,\pm 31),\ (1/4,\pm 1/16),\ (-15/16,\pm 679/512),\ (30,\pm 9859).$$

`MAGMA`'s command `TorsionSubgroup` reveals that the Mordell–Weil group is torsion free. Using the command `ReducedBasis` we find a set of generators for the subgroup generated by the divisors $P - Q$, where $P, Q$ are in the list we have just found. A list of independent generators for the subgroup is

$$(0,1) - \infty, \quad (1,1) - \infty, \quad (-1,1) - \infty.$$

Hence $J(\mathbb{Q})$ has rank at least $3$. Now we use the command `RankBounds` to see that an upper bound obtained from the information of the $2$-Selmer group of $J(\mathbb{Q})$ is $3$. Then $J(\mathbb{Q})$ has rank $3$. We now want to see that none of the generators is the double of some divisor. We first compute an upper bound for the height difference using the `HeightConstant` command. We find that $\mu_2$ is about $2.17$. We compute the canonical heights of the divisors above with the `Height` command and see that they are respectively about $0.16$, $0.60$ and $0.79$. If the double of a divisor $D$ is one of the divisors above,

then it should have strictly lower height. Using the upper bound for the height difference we look for all points of naive logarithmic height less than $\hat{h}((-1,1))+\mu_2$. We use again the command `ReducedBasis` to obtain independent generators for the group generated by the points found in our search, and we obtain the same generators. Hence, none of the original divisors was of the form $2D$, and they generate $J(\mathbb{Q})/2J(\mathbb{Q})$. Finally, we compute the heights of the representatives of each coset, and apply Zagier's theorem to find a complete set of generators of $J(\mathbb{Q})$. We see that the Mordell–Weil group is generated by the divisors above.

# Chapter 3

# Upper bounds for the size of $S$-integral points on hyperelliptic curves

The material presented here is a slightly expanded version of that in my paper [25], which is to appear in The International Journal of Number Theory.

Consider the hyperelliptic curve with affine model

$$\mathcal{C} : Y^2 = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0, \tag{3.0.1}$$

where $a_0, \ldots, a_n$ are rational integers, $a_n \neq 0$, $n \geq 5$, where the polynomial on the right-hand side is irreducible. Let $S$ be a finite set of rational primes. A rational number $x = p/q$, $p, q \in \mathbb{Z}$, $(p, q) = 1$, is an *$S$-integer* if $q$ is either $1$ or it is divisible by primes in $S$ only. The *size* (or *height*) of $x$, $x \neq 0$ is defined by $\max\{\log|a|, \log|b|\}$. In this chapter we give a method for explicitly computing an upper bound for the size of the $S$-integral points on hyperelliptic curves (3.0.1). Our strategy is based in part on the ideas in [15] (see Chapter 1 for a detailed explanation of the similarities and the differences between the two approaches).

We use a variant of Baker's method to transform the problem of finding the $S$-

integral points on a hyperelliptic curve into a finite set of $S$-unit equations in certain number fields. Since the degree of the fields we will deal with will be often large ($> 20$), the explicit computation of the group of units and the resulting unit equations is beyond the present power of computer algebra. We will then bound the size for the solutions of the unit equations in terms of invariants of the number fields, namely the regulator and the class number. Again, these invariants are hard to compute in the cases we need, but they have been previously bounded in the literature. These bounds are not necessarily sharp and we use them to save ourselves the expense, obtaining large bounds for the size of the $S$-integral points on the curve.

We need the following assumptions:

a. The knowledge of at least one rational point $P_0$ on $\mathcal{C}$.

b. The knowledge of a Mordell–Weil basis for $J(\mathbb{Q})$ where $J$ is the Jacobian of $\mathcal{C}$.

The chapter is arranged as follows. In Section 3.1 we show, after appropriate scaling, that an $S$-integral point $(x, y)$ satisfies $x - \alpha = \kappa\xi^2$ where $\alpha$ is some fixed algebraic integer, $\xi \in \mathbb{Q}(\alpha)$, and $\kappa$ is an algebraic integer belonging to a finite computable set. In Section 3.7 we give bounds for the height of $S$-integral solutions $x$ to an equation of the form $x - \alpha = \kappa\xi^2$ where $\alpha$ and $\kappa$ are fixed algebraic integers. Thus we obtain bounds for the height of $S$-integral points on our affine model (3.0.1). Sections 3.2–3.6 are preparation for Section 3.7: in particular Section 3.2 is concerned with $S$-integers and heights; Section 3.3 collects various results on appropriate choices of systems of fundamental $S$-units; Section 3.4 explains how a theorem of Landau can be used to bound the $S$-regulator of a number field; Section 3.5 is devoted to Matveev's lower bounds for linear forms in logarithms and to Yu's lower bounds for linear forms in $p$-adic logarithms; in Section 3.6 we use an idea due to Voutier to adapt recent estimates for the size of solutions to $S$-unit equations due to Győry and Yu. These estimates are more suited to our purposes and we use them in Section 3.7 to deduce the bounds for the height of $x$ alluded to above from the bounds for solutions of unit equations. Finally,

Section 3.8 explains how the variant of the Mordell–Weil sieve in [15] can be used to effectively sieve up to the bounds obtained in Section 3.6 and thus completely determine the set of $S$-integral points on the curve.

## 3.1 Descent

Consider a (non-empty) finite set of rational primes $S$ and the $S$-integral points on the affine model of the hyperelliptic curve (3.0.1), where the polynomial on the right-hand side is irreducible. By appropriate scaling, one transforms the problem of finding the $S$-integral points on (3.0.1) to that of finding the $S$-integral points on a model of the form

$$ay^2 = x^n + b_{n-1}x^{n-1} + \cdots + b_0, \tag{3.1.1}$$

where $a$ and $b_0, \ldots, b_{n-1}$ are integers, with $a \neq 0$. We will denote the polynomial on the right-hand side by $f$.

Let $\alpha$ be a root of $f$. In a similar way to that in [15] we will show that for every $S$-integral point $(x, y)$ on the model (3.1.1) we have

$$x - \alpha = \kappa\xi^2,$$

where $\kappa, \xi \in K = \mathbb{Q}(\alpha)$ and $\kappa$ is an algebraic integer that comes from a finite computable set. We follow ideas from [15], but we adjust the proofs for the $S$-integral case. In particular, the finite computable set is larger than that in [15] in one case.

We will suppose that the Mordell–Weil group $J(\mathbb{Q})$ of the curve $\mathcal{C}$ is known. The method depends on whether the degree of $f$ is odd or even.

### 3.1.1 The Odd Degree Case

Schaefer [37, Lemma 2.2] proved that when the polynomial $f$ has odd degree, every degree $0$ divisor defined over $\mathbb{Q}$ is linearly equivalent to a divisor of the form $\sum_{i=1}^{m}(P_i - \infty)$, where the set $\{P_1, \ldots, P_m\}$ is stable under the action of the Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$,

and such that all $y(P_i)$ are non-zero. By [15] claim that we can write $x(P_i) = \gamma_i/d_i^2$ where $\gamma_i$ is an algebraic integer and $d_i \in \mathbb{Z}_{\geq 1}$; and that if $P_i$, $P_j$ are conjugate, we can suppose that $d_i = d_j$ and in consequence $\gamma_i$, $\gamma_j$ are conjugate. In this odd degree case we will always choose representatives of the cosets of $J(\mathbb{Q})/2J(\mathbb{Q})$ having this form.

Choose a set of representatives for $J(\mathbb{Q})/2J(\mathbb{Q})$ satisfying the conditions of the previous paragraph. To each representative we associate the algebraic number

$$\kappa = a^{(m \bmod 2)} \prod_{i=1}^{m} (\gamma_i - \alpha d_i^2).$$

**Lemma 3.1.1.** *Let $\mathcal{K}$ be a set of $\kappa$ associated as above to a complete set of coset representatives for $J(\mathbb{Q})/2J(\mathbb{Q})$. Then $\mathcal{K}$ is a finite subset of $\mathcal{O}_K$, the ring of integers of $K$ and if $(x, y)$ is a rational point on the model* (3.1.1) *then $x - \alpha = \kappa\xi^2$ for some $\kappa \in \mathcal{K}$ and $\xi \in K$.*

*Remark.* This is Lemma 3.1 in [15]. The proof there does not require $x$ to be an integer, but only a rational number. Hence the proof is valid for every rational point in the curve. We present the proof here for completeness.

*Proof.* For hyperelliptic curves defined by a polynomial $f$ of odd degree Schaefer [37, Lemma 2.1] proved that the map

$$\theta : J(\mathbb{Q})/2J(\mathbb{Q}) \to K^*/K^{*2}$$

given by

$$\theta\left(\sum_{i=1}^{m}(P_i - \infty)\right) = a^m \prod_{i=1}^{m} (x(P_i) - \alpha) \pmod{K^{*2}}$$

is a well defined homomorphism for coset representatives of the form $\sum(P_i - \infty)$ with $y(P_i) \neq 0$. Since $f$ is irreducible over $\mathbb{Q}$, a rational point $P$ on the model (3.1.1) will necessarily have $x(P) \neq 0$. Then the coset of the divisor $P - \infty$ will be mapped under $\theta$ to $x(P) - \alpha \pmod{K^{*2}}$. Since $\mathcal{K}$ consists of the image of a complete set of representatives for $J(\mathbb{Q})/2J(\mathbb{Q})$ the result follows. □

### 3.1.2 The Even Degree Case

We are assuming the existence of a rational point $P_0$. If $P_0$ is one of the two points at infinity, let $\epsilon_0 = 1$. Otherwise, $y(P_0) \neq 0$ since $f$ is irreducible. Write $x_0 = \gamma_0/d_0^2$ with $\gamma_0 \in \mathbb{Z}$ and $d_0 \in \mathbb{Z}_{\geq 1}$ and let $\epsilon_0 = \gamma_0 - \alpha d_0^2$.

In this even degree case one needs to modify the homomorphism given in the odd degree case. Since we are assuming the existence of a rational point on the curve, we can choose a representative of every coset of $J(\mathbb{Q})/2J(\mathbb{Q})$ having the form $\sum_{i=1}^{m}(P_i - P_0)$ where the set $\{P_1, \ldots, P_m\}$ is stable under the action of the Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, and such that all $y(P_i)$ are non-zero (see Section 5 of [45]). Again, as in [15, Section 3], we can write $x(P_i) = \gamma_i/d_i^2$ where $\gamma_i$ is an algebraic integer and $d_i \in \mathbb{Z}_{\geq 1}$; and if $P_i$, $P_j$ are conjugate, we may suppose that $d_i = d_j$ and in consequence $\gamma_i$, $\gamma_j$ are conjugate. We associate to such a coset representative the algebraic number

$$\epsilon = \epsilon_0^{(m \bmod 2)} \prod_{i=1}^{m} (\gamma_i - \alpha d_i^2).$$

**Lemma 3.1.2.** *Let $\mathcal{E}$ be a set of $\epsilon$ associated as above to a complete set of coset representatives for $J(\mathbb{Q})/2J(\mathbb{Q})$. Let $\Delta$ be the discriminant of the polynomial $f$. For each $\epsilon \in \mathcal{E}$ let $B_\epsilon$ be the set of square-free rational integers supported only by primes dividing $a\Delta \,\mathrm{Norm}_{K/\mathbb{Q}}(\epsilon) \prod_{p \in S} p$. Let $\mathcal{K} = \{\epsilon b : \epsilon \in \mathcal{E}, b \in \mathcal{B}_\epsilon\}$. Then $\mathcal{K}$ is a finite subset of $\mathcal{O}_K$ and if $(x, y)$ is an $S$-integral point on the model* (3.1.1)*, then $x - \alpha = \kappa\xi^2$ for some $\kappa \in \mathcal{K}, \xi \in K$.*

*Proof.* In this even degree case there is also a well defined homomorphism

$$\theta : J(\mathbb{Q})/2J(\mathbb{Q}) \to K^*/\left(\mathbb{Q}^* K^{*2}\right)$$

given by

$$\theta\left(\sum_{i=1}^{m}(P_i - P_0)\right) = a^m \prod_{i=1}^{m}(x(P_i) - \alpha) \pmod{\mathbb{Q}^* K^{*2}}$$

for coset representatives $\sum(P_i - P_0)$ with $y(P_i) \neq 0$ (see [35] and Section 5 of [45]). Let $P = (x, y)$ be an $S$-integral point on the curve. Under $\theta$, the coset of $P - P_0$ is

mapped to $x-\alpha \pmod{\mathbb{Q}^* K^{*2}}$. Then we have that $(x-\alpha)=\epsilon b\xi^2$ for some $\epsilon \in \mathcal{E}$, $\xi \in K^*$ and $b$ a square-free rational integer. Suppose $\wp$ does not divide $a\Delta\prod_{p\in S} p$. Write $f(x)=(x-\alpha)\phi(x)$ where $\phi(x)=\prod_{i=1}^{n-1}(x-\alpha_i)=x^{n-1}+c_1x^{n-2}+\cdots+c_{n-1}$ for some $c_i \in K$. Consider the equality

$$\operatorname{ord}_\wp(ay^2)=\operatorname{ord}_\wp(x-\alpha)+\operatorname{ord}_\wp\phi(x).$$

Assume $\operatorname{ord}_\wp(x-\alpha)$ is odd. Then, it is positive and $x\equiv\alpha \pmod{\wp}$. Hence $\phi(x)\equiv \alpha^{n-1}+c_1\alpha^{n-2}+\cdots+c_{n-1}\equiv 0 \pmod{\wp}$, for $\wp$ divides $ay^2$, but it does not divide $a$, so $\operatorname{ord}_\wp(ay^2)$ is even and $\operatorname{ord}_\wp\phi(x)$ is odd. Since $\alpha^{n-1}+c_1\alpha^{n-2}+\cdots+c_{n-1}=\prod_{i=1}^{n-1}(\alpha-\alpha_i)$, we have that $\wp$ divides $\Delta=\delta_1\delta_2$, where $\delta_1=\prod_{i=1}^{n-1}(\alpha-\alpha_i)^2$ and $\delta_2=\prod_{i<j}(\alpha_i-\alpha_j)^2$. But this is a contradiction and then $\operatorname{ord}_\wp(x-\alpha)$ is even. Since $\wp$ does not divide $a$ we conclude $2 \mid \operatorname{ord}_\wp(b)$. Let $\wp \mid p$ where $p$ is a rational prime not dividing $a\Delta\operatorname{Norm}_{K/\mathbb{Q}}(\epsilon)\prod_{p\in S} p$. Then $p$ is unramified in $K/\mathbb{Q}$ and so $\operatorname{ord}_p(b)=\operatorname{ord}_\wp(b)\equiv 0 \pmod{2}$. This shows that $b\in\mathcal{B}_\epsilon$ and proves the lemma. □

## 3.2 $S$-integers and heights

In this section we state the basic properties of heights of algebraic numbers and we fix some notation that we will use throughout the thesis. Most of these are standard results which can be found in [51, Chapter 3]. Let $K$ be a number field of degree $d$. We denote by $M_K$ the set of all places of $K$ and by $\mathcal{O}_K$ the set of integers of $K$. Denote by $R$ the regulator of $K$. For a place $\upsilon\in M_K$ let $\mathbb{Q}_\upsilon, K_\upsilon$ be the completions at $\upsilon$ of $\mathbb{Q}$ and $K$ respectively.

For $\upsilon\in M_K$, we let $|\cdot|_\upsilon$ be the usual normalised valuation corresponding to $\upsilon$; in particular if $\upsilon$ is non-Archimedean and $p$ is the rational prime below $\upsilon$ then $|p|_\upsilon=p^{-1}$. Thus if $L/K$ is a field extension, and $\omega$ a place of $L$ above $\upsilon$ then $|\alpha|_\omega=|\alpha|_\upsilon$, for all $\alpha\in K$.

We denote by $d_\upsilon$ the local degree $[K_\upsilon:\mathbb{Q}_\upsilon]$. Define

$$\|\alpha\|_\upsilon=|\alpha|_\upsilon^{d_\upsilon}.$$

Hence for $\alpha \in K^*$, the product formula states that

$$\prod_{v \in M_K} \|\alpha\|_v = 1.$$

In particular, if $v$ is Archimedean, corresponding to a real or complex embedding $\sigma$ of $K$ then

$$|\alpha|_v = |\sigma(\alpha)| \qquad \text{and} \qquad \|\alpha\|_v = \begin{cases} |\sigma(\alpha)| & \text{if } \sigma \text{ is real} \\ |\sigma(\alpha)|^2 & \text{if } \sigma \text{ is complex.} \end{cases}$$

If $v$ is finite and $\mathfrak{p}$ is a prime ideal corresponding to $v$, then for $\alpha \in K \backslash \{0\}$ we have

$$\|\alpha\|_v = N(\mathfrak{p})^{-\operatorname{ord}_{\mathfrak{p}}(\alpha)}.$$

For $\alpha \in K$, the (absolute) logarithmic height $\mathrm{h}(\alpha)$ is given by

$$\mathrm{h}(\alpha) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} d_v \log \max\{1, |\alpha|_v\} = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} \log \max\{1, \|\alpha\|_v\}. \tag{3.2.1}$$

The absolute logarithmic height of $\alpha$ is independent of the field $K$ containing $\alpha$. Note that in the case $K = \mathbb{Q}$ this definition of height agrees with the definition of size given at the beginning of this chapter.

Let $S$ be a finite set of places of $K$ including all the infinite places. Set $s = |S|$ (we exclude the case $s = 1$). We define the *ring of $S$-integers of $K$* as

$$\mathcal{O}_S = \{\alpha \in K : |\alpha|_v \leq 1, v \notin S\},$$

and the group of $S$-units as the group of units of $\mathcal{O}_S$,

$$\mathcal{O}_S^* = \{\alpha \in K : |\alpha|_v = 1, v \notin S\}.$$

The unit theorem of Dirichlet and Chevalley [30, Chapter V] states that the group $\mathcal{O}_S^*$ is a free abelian group of rank $s - 1$. A set of generators for $\mathcal{O}_S^*$ is known as a *system of fundamental $S$-units in $K$*. For example, let $K = \mathbb{Q}$ and $S = \{\infty, 2, 3\}$. (By abuse of notation we write $p$ instead of the place corresponding to the $p$-adic valuation.) Then

the ring of integers of $K$ is the usual ring of integers $\mathbb{Z}$ and the ring of $S$-integers of $K$ is

$$\{\pm 2^i 3^j n : i, j, n \in \mathbb{Z}\}.$$

In this case the group of units of $K$ is $\{\pm 1\}$ and the group of $S$-units of $K$ is

$$\{\pm 2^i 3^j : i, j \in \mathbb{Z}\},$$

which is free abelian of rank $2$.

We now define the $S$-regulator and the $S$-norm of a fractional ideal, as in [13]. Let $\{\varepsilon_1, \dots \varepsilon_{s-1}\}$ be a system of fundamental $S$-units in $K$. Consider the matrix $(\log|\varepsilon_i|_{v_j})$ where $j$ runs over $s-1$ places of $K$. The absolute value of the determinant of the matrix is called the *$S$-regulator of $K$*. When the set $S$ is the set of infinite places of $K$ this coincides with the usual definition of regulator. The product formula implies that the definition is independent of the choice of places $v_1, \dots, v_{s-1}$, for the $(s-1) \times s$ matrix $B = (\log|\varepsilon_i|_{v_j})$ where $j$ runs over all the places of $S$ has the property that its columns add up to $0$. Hence the absolute value of the determinant of the matrix obtained by deleting one of the columns is independent of the choice of column. The definition is also independent of the system of fundamental units $\{\varepsilon_1, \dots \varepsilon_{s-1}\}$ as the $S$-regulator is, up to a constant, the volume of a fundamental domain of the lattice spanned by the vectors $L(\varepsilon_i) = (\log|\varepsilon_i|_{v_j}) \in \mathbb{R}^s$ contained in the $s$-dimensional subspace of vectors whose entries add up to $0$, and this lattice is the same for every choice of a system of fundamental $S$-units.

If $\alpha \in K$ is a nonzero algebraic integer, the fractional ideal generated by $\alpha$ can be uniquely written in the form $\mathfrak{a}_1 \cdot \mathfrak{a}_2$, where $\mathfrak{a}_1$ is composed of primes outside $S$ and $\mathfrak{a}_2$ is composed of primes contained in $S$. We define the *$S$-norm of $\alpha$* as $N(\mathfrak{a}_1)$ and we denote it by $N_S(\alpha)$. Note that $N_S(\alpha)$ is a positive integer for every $\alpha \in \mathcal{O}_S \backslash \{0\}$.

**Lemma 3.2.1.** *Let $K$ be a number field. For any nonzero algebraic number $\alpha \in K$, we have $\mathrm{h}(\alpha^{-1}) = \mathrm{h}(\alpha)$. For algebraic numbers $\alpha_1, \dots, \alpha_n \in K$, we have*

$$\mathrm{h}(\alpha_1 \alpha_2 \cdots \alpha_n) \leq \mathrm{h}(\alpha_1) + \cdots + \mathrm{h}(\alpha_n), \quad \mathrm{h}(\alpha_1 + \cdots + \alpha_n) \leq \log n + \mathrm{h}(\alpha_1) + \cdots + \mathrm{h}(\alpha_n),$$

*and for any place* $v \in M_K$

$$\log\|\alpha\|_v \leq [K:\mathbb{Q}]\,\mathrm{h}(\alpha).$$

*Proof.* The first equality is an immediate consequence of the definition of absolute logarithmic height and the product formula. For the second estimate note that for non-negative $x_1, \ldots, x_n$

$$\max\{1, x_1 x_2 \cdots x_n\} \leq \max\{1, x_1\} \cdots \max\{1, x_n\}.$$

We also have

$$\max\{1, x_1 + \cdots + x_n\} \leq n \max\{1, x_1\} \cdots \max\{1, x_n\},$$

which implies the third estimate. Finally, the last inequality is also an immediate consequence of the definition of absolute logarithmic height. □

**Lemma 3.2.2.** *Let* $K$ *be a number field of degree* $d$ *and* $S$ *a finite set of places of* $K$ *including the infinite places. Denote by* $s$ *the cardinality of* $S$*. Let* $\varepsilon \in K^*$ *be a* $S$*-unit. Let* $\eta \in M_K$ *be a place of* $K$ *making* $\|\varepsilon\|_\eta$ *minimal. Then*

$$\mathrm{h}(\varepsilon) \leq -\frac{s}{d}\log\|\varepsilon\|_\eta.$$

*Proof.* Note $\|\varepsilon\|_v = 1$ for all $v \notin S$ so we can choose $\eta \in S$. Then $0 < \|\varepsilon\|_\eta \leq 1$. Now,

$$\begin{aligned}\mathrm{h}(\varepsilon) = \mathrm{h}(\varepsilon^{-1}) &= \frac{1}{d}\sum_{v\in M_K} \max\{\log\|\varepsilon^{-1}\|_v, 0\} \\ &\leq \frac{1}{d}\sum_{v\in S} \log\|\varepsilon^{-1}\|_\eta = -\frac{s}{d}\log\|\varepsilon\|_\eta,\end{aligned}$$

and we have now proved the lemma. □

**Lemma 3.2.3.** *Let* $K$ *be a number field of degree* $d$ *and* $S$ *a finite set of places of* $K$ *including the infinite places. Let* $\varepsilon$ *be a* $S$*-unit. Then*

$$\sum_{v\in S} |\log\|\varepsilon\|_v| = 2d\,\mathrm{h}(\varepsilon).$$

*Proof.* Recall that $\|\varepsilon\|_v = 1$ for all places $v \notin S$. Now

$$\begin{aligned}\sum_{v\in M_K} |\log\|\varepsilon\|_v| &= \sum_{\substack{v\in M_K\\ \|\varepsilon\|_v\le 1}} |\log\|\varepsilon\|_v| + \sum_{\substack{v\in M_K\\ \|\varepsilon\|_v\ge 1}} |\log\|\varepsilon\|_v| \\ &= \sum_{\substack{v\in M_K\\ \|\varepsilon^{-1}\|_v\ge 1}} \log\|\varepsilon^{-1}\|_v + \sum_{\substack{v\in M_K\\ \|\varepsilon\|_v\ge 1}} \log\|\varepsilon\|_v \\ &= \sum_{v\in M_K} \max\{0, \log\|\varepsilon^{-1}\|_v\} + \max\{0, \log\|\varepsilon\|_v\} \\ &= d(\mathrm{h}(\varepsilon^{-1}) + \mathrm{h}(\varepsilon)) = 2d\,\mathrm{h}(\varepsilon).\end{aligned}$$

□

The following Lemma is due to Voutier [50, Corollary 2].

**Lemma 3.2.4.** *Let $K$ be a number field of degree $d$ and let $\alpha \in K$ be a nonzero algebraic number which is not a root of unity. Then*

$$d\,\mathrm{h}(\alpha) \ge \begin{cases} \log 2 & d = 1, \\ 2/(\log(3d))^3 & d \ge 2. \end{cases}$$

## 3.3 Systems of fundamental units

For a number field of large degree ($\ge 10$) it is extremely time consuming to explicitly describe the group of units and the group of $S$-units. But we can find bounds for the size of the units in a fundamental system of units in terms of the $S$-regulator. The following Lemma, which is due to Bugeaud and Győry [13, 14] and Győry and Yu [27, Lemma 2] gives the bounds for the size of units we will use in the rest of this work.

We first fix some notation for the whole section. Let $K$ be a number field of degree $d$, $S$ a finite set consisting of $s$ places of $K$ including the set $S_\infty$ of infinite places. We denote by $R_S$ the $S$-regulator of $K$. For a positive real number $a$ we set $\log^*(a) = \max\{1, \log a\}$.

**Lemma 3.3.1.** *Define the constants*

$$c_1(s,d) = \frac{((s-1)!)^2}{2^{s-2}d^{s-1}},$$

$$c_2(s,d) = 29e\sqrt{s-2}\, c_1(s,d) d^{s-1} \log^*(d)$$

$$c_3(s,d) = \frac{((s-1)!)^2}{2^{s-1}} \begin{cases} 2/\log 2 & \text{if } d = 1, \\ (\log(3d))^3 & \text{if } d \geq 2. \end{cases}$$

*There exists a fundamental system of $S$-units $\{\varepsilon_1, \ldots, \varepsilon_{s-1}\}$ in $K$ with the following properties:*

*i.* $\prod_{i=1}^{s-1} \mathrm{h}(\varepsilon_i) \leq c_1(s,d) R_S$,

*ii.* $\max_{i=1,\ldots,s-1} \mathrm{h}(\varepsilon_i) \leq c_2(s,d) R_S$ *if* $s \geq 3$,

*iii. Write $\mathcal{M}$ for the $(s-1) \times (s-1)$-matrix $(\log \|\varepsilon_i\|_{v_j})$ where $v_j$ runs over $s-1$ of the places in $S$ and $1 \leq i \leq s-1$. Then the absolute values of the entries of $\mathcal{M}^{-1}$ are bounded above by $c_3(s,d)$.*

Later on we will need to bound linear forms in logarithms, and we will use the following lemma [27, Lemma 5].

**Lemma 3.3.2.** *Let $\{\varepsilon_1, \ldots, \varepsilon_{s-1}\}$ be a system of fundamental $S$-units in $K$ as in Lemma 3.3.1. For $s \geq 3$ define the constant*

$$c_4(s,d) = d\pi^{s-2} c_2(s,d).$$

*Then*

$$\prod_{i=1}^{s-1} \max(d\,\mathrm{h}(\varepsilon_i), \pi) \leq \begin{cases} \max(R_S, \pi) & \text{if } s = 2, \\ c_4(s,d) R_S & \text{if } s \geq 3. \end{cases}$$

The following Lemma is an improvement on [15, Lemma 6.2].

**Lemma 3.3.3.** *Let $\{\varepsilon_1, \ldots, \varepsilon_{s-1}\}$ be a system of fundamental $S$-units in $K$ as in Lemma 3.3.1. Define the constant $c_5 = c_5(s,d) = 2dc_3(s,d)$. Suppose $\varepsilon = \zeta \varepsilon_1^{b_1} \ldots \varepsilon_{s-1}^{b_{s-1}}$, where $\zeta$ is a root of unity in $K$. Then*

$$\max\{|b_1|, \ldots, |b_{s-1}|\} \leq c_5(s,d)\, \mathrm{h}(\varepsilon).$$

*Proof.* Note that for any place $v$ in $S$,

$$\log\|\varepsilon\|_v = \sum b_i \log\|\varepsilon_i\|_v.$$

From part (iii) of Lemma 3.3.1 we have that $|b_i| \leq c_3(s,d)\sum_v|\log\|\varepsilon\|_v|$, where the sum runs over all but one of the places in $S$. Now

$$\sum_{\substack{s-1 \text{ places} \\ \text{of } S}} |\log\|\varepsilon\|_v| \leq \sum_{v\in M_K} |\log\|\varepsilon\|_v| = 2d\,\mathrm{h}(\varepsilon),$$

where the last equality follows from Lemma 3.2.3. The proof is now complete. □

The following result is an special case of Lemma 3 of [27].

**Lemma 3.3.4.** *Let $\alpha \in K$ be a nonzero $S$-integer. Let $h$ be the class number of $K$ and $r$ the unit rank of $K$. Denote by $R$ the regulator of $K$ and by $t$ the number of finite places in $S$. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ be the prime ideals corresponding to the finite places in $S$. Set $Q = N(\mathfrak{p}_1 \cdots \mathfrak{p}_t)$ if $t > 0$, $Q = 1$ if $t = 0$. Then there is a $S$-unit $\varepsilon$ such that*

$$\mathrm{h}(\varepsilon\alpha) \leq \frac{1}{d}(\log N_S(\alpha) + h\log Q) + c_6 R.$$

*where*

$$c_6(r,d) = \begin{cases} 0, & r = 0, \\ 1/d & r = 1 \\ 29er!r\sqrt{r-1}\log d & r \geq 2 \end{cases}$$

## 3.4 Upper bounds for the regulator and the class number

Later on we need to give upper bounds for the $S$-regulators of complicated number fields of high degree. We can bound the $S$-regulator of a number field in terms of its regulator and the class number as in the following lemma due to Bugeaud and Győry, which is Lemma 3 of [13].

**Lemma 3.4.1.** *Let $K$ be a number field of degree $d$ with regulator $R$ and class number $h$. Let $S$ be a finite set of places of $K$ including all infinite places and at least one finite place. Let $R_S$ be the $S$-regulator of $K$. Denote by $t$ the number of finite places in $S$ and by $P$ the largest prime below the finite places in $S$. Then*

$$R_S \leq Rh(d \log^* P)^t.$$

**Definition.** Let $K$ be a number field and let $\{b_1, \ldots, b_n\}$ be an integral basis for the ring of integers $\mathcal{O}_K$. Denote the embeddings of $K$ in $\mathbb{C}$ by $\sigma_1, \ldots, \sigma_n$. The *absolute discriminant of* $K$ is the square of the determinant of the matrix $\sigma_i(b_j)$.

It is a standard fact that the absolute discriminant of a number field does not depend on the choice of basis $\{b_1, \ldots, b_n\}$.

We can bound the product $Rh$ numerically. Our bound is based on bounds of Landau [29].

**Lemma 3.4.2.** *Let $K$ be a number field with degree $d = u + 2v$ where $u$ and $v$ are respectively the numbers of real and complex embeddings. Denote the absolute discriminant of $K$ by $D$ and the regulator by $R$, and the number of roots of unity in $K$ by $w$. Suppose, moreover, that $L$ is a real number such that $D \leq L$. Let*

$$a = 2^{-v}\, \pi^{-d/2}\, \sqrt{L}.$$

*Define the function $f_K(L, s)$ by*

$$f_K(L, s) = 2^{-u}\, w\, a^s \left(\Gamma(s/2)\right)^u \left(\Gamma(s)\right)^v s^{d+1}\, (s-1)^{1-d},$$

*and let $B_K(L) = \min\{f_K(L, 2 - t/1000) \ : t = 0, 1, \ldots, 999\}$. Then $Rh < B_K(L)$.*

*Proof.* This is Lemma 5.1 in [15]. We note that Landau [29, proof of Hilfssatz 1] established the inequality $Rh < f_K(D_K, s)$ for all $s > 1$. (In the proof of [15, Lemma 5.1] only a bound on $R$ was needed and then the result of Landau is only quoted there as $R < f_K(D_K, s)$.) Since the function $f_K$ is increasing with respect to the first parameter the result follows. □

We will also need a bound for the class number of a given number field. We shall use the following bound due to Lenstra [28, Theorem 6.5].

**Lemma 3.4.3.** *Let $K$ be a number field of degree $d = u + 2v$ where $u$ and $v$ are respectively the numbers of real and complex embeddings. Let $h$ be the class number of $K$. Denote the absolute discriminant of $K$ by $D$. Suppose that $L$ is a real number such that $D \leq L$. Let $a = (2/\pi)^v \sqrt{L}$. Then*

$$h \leq a \cdot \frac{(d - 1 + \log a)^{d-1}}{(d-1)!}.$$

## 3.5 Linear forms in logarithms

Let $L$ be a number field of degree $d$ and consider a "linear form"

$$\Lambda := \alpha_1^{b_1} \cdots \alpha_n^{b_n} - 1, \tag{3.5.1}$$

where $\alpha_1, \ldots, \alpha_n \in L^*$ are $n \geq 2$ nonzero elements of $L$ and $b_1, \ldots, b_n$ are rational integers. In section 3.6 a unit equation will be transformed into a linear form in logarithms. This form will be written in terms of the $S$-units in a fundamental system of $S$-units. As we have mentioned before, for number fields of large degree ($\geq 20$) the explicit computation of the group of units is beyond the present capabilities of computer algebra. We will then use lower bounds for the linear forms in terms of the height of the units.

Set

$$B^* = \max\{|b_1|, \ldots, |b_n|\}$$

and

$$A_i \geq \max(d\,\mathrm{h}(\alpha_i), \pi), \quad i = 1, \ldots, n.$$

The following lemma is a version of Matveev's bound for linear forms in logarithms [31], due to Győry and Yu [27, Proposition 4].

**Lemma 3.5.1.** *Suppose $\Lambda \neq 0$, $b_n = \pm 1$ and let $B$ be a real number satisfying*

$$B \geq \max\{B^*, 2e \max(n\pi/\sqrt{2}, A_1, \ldots, A_{n-1})A_n\}.$$

*Then*

$$\log|\Lambda| > -c_7(n,d)A_1\cdots A_n\log(B/(\sqrt{2}A_n)),$$

*where*

$$c_7(n,d) = \min\{1.451(30\sqrt{2})^{n+4}(n+1)^{5.5}, \pi 2^{6.5n+27}\}d^2\log(ed).$$

We consider again the linear form (3.5.1). Let $B, B_n$ be real numbers such that

$$B \geq B^*, \quad B \geq B_n \geq |b_n|. \tag{3.5.2}$$

Let $p$ be a rational prime and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_L$ lying over $p$. Denote by $e_\mathfrak{p}$ the ramification index of $\mathfrak{p}$. We denote by $N(\mathfrak{p})$ the norm of the ideal $\mathfrak{p}$. Define the constants

$$c_8(n,d) = (16ed)^{2(n+1)}n^{3/2}\log(2nd)\log(2d),$$
$$c_9(n,d) = (2d)^{2n+1}\log(2d)\log^3(3d),$$

The following bound for linear forms in $p$-adic logarithms is due to Yu [53].

**Lemma 3.5.2.** *Assume that* $\operatorname{ord}_p b_n \leq \operatorname{ord}_p b_j$ *for* $j = 1,\ldots,n$*, and for* $j = 1,\ldots,n$ *set*

$$h'_j = \max\{\mathrm{h}(\alpha_j), 1/(16e^2d^2)\}.$$

*If* $\Lambda \neq 0$*, then for any real number* $\delta$ *with* $0 < \delta \leq 1/2$ *we have*

$$\operatorname{ord}_\mathfrak{p}\Lambda < c_8(n,d)e_\mathfrak{p}^n\frac{N(\mathfrak{p})}{(\log N(\mathfrak{p}))^2}\max\left\{h'_1\cdots h'_n\log M, \frac{\delta B}{B_n c_9(n,d)}\right\},$$

*where*

$$M = (B_n/\delta)2e^{(n+1)(6n+5)}d^{3n}\log(2d)N(\mathfrak{p})^{n+1}h'_1\cdots h'_{n-1}.$$

## 3.6 Upper bounds for the size of the solutions to $S$-unit equations

We now prove an explicit version of Lemma 4 of [12]. We will follow ideas from the proof of Theorem 1 of [27]. Instead of obtaining an estimate in terms of the regulator of

a large field, we get one in terms of the product of the regulators of two of its subfields. This often results in a significant improvement of the upper bound for the height. This idea is due to Voutier [49]. Recall the notation $\log^*(a) = \max\{1, \log a\}$.

**Proposition 3.6.1.** *Let $L$ be a number field of degree $d$, which contains $K_1, K_2$ as subfields of degree $d_1, d_2$, respectively. Let $S$ (resp. $S_1$, $S_2$) be a finite set of places of $L$ (resp. $K_1$, $K_2$) containing the set of infinite places. Denote by $s$ (resp. $s_1$, $s_2$) the number of places in $S$ (resp. $S_1$, $S_2$) and assume both $s_1$ and $s_2$ are $\geq 3$. Denote by $P$ the largest norm of the prime ideals corresponding to the finite places in $S$, with the convention that $P = 1$ if $S$ does not contain finite places. Assume that $\mathcal{O}_{S_1}^*$ and $\mathcal{O}_{S_2}^*$ are both contained in $\mathcal{O}_S^*$. Denote by $R_i$ the $S_i$-regulator of $K_i$ for $i = 1, 2$. Suppose that $\nu_1, \nu_2, \nu_3$ are non-zero elements of $L$ with height $\leq H$, where $H$ is a constant $\geq \max(1, \pi/d)$ and consider the unit equation*

$$\nu_1\varepsilon_1 + \nu_2\varepsilon_2 + \nu_3\varepsilon_3 = 0 \tag{3.6.1}$$

*where $\varepsilon_1$ is a $S_1$-unit of $K_1$, $\varepsilon_2$ a $S_2$-unit of $K_2$ and $\varepsilon_3$ a $S$-unit of $L$. Define the constants*

$$\begin{aligned}
c_{10} &= 2H(s+1) + 4sHc_4(s_1,d_1)c_4(s_2,d_2)c_7(s_1+s_2-1,d)R_1R_2\times \\
&\qquad \log(\sqrt{2}e\max\{(s_1+s_2-2)\pi/\sqrt{2}, c_2(s_1,d_1)R_1, c_2(s_2,d_2)R_2)\}), \\
c_{11} &= 4sHc_4(s_1,d_1)c_4(s_2,d_2)c_7(s_1+s_2-1,d)R_1R_2, \\
c_{12} &= 2H(s+1) + c_{11}\log\left(\frac{\max\{c_5(s_1,d_1), c_5(s_2,d_2), 1)\}}{2\sqrt{2}dH}\right), \\
c_{13} &= \log 2 + 2H + 4(s_1+s_2-2)Hc_1(s_1,d_1)c_1(s_2,d_2)c_9(s_1+s_2-1,d)\times \\
&\quad R_1R_2\max\{c_2(s_1,d_1)R_1, c_2(s_2,d_2)R_2\}, \\
c_{14} &= \frac{2Hd^{s_1+s_2-2}P}{\log(2)\log^* P}c_1(s_1,d_1)c_1(s_2,d_2)c_8(s_1+s_2-1,d)R_1R_2, \\
c_{15} &= 2H(s+1)+ \\
&\qquad c_{14}\log\left(\frac{\max\{c_5(s_1,d_1), c_5(s_2,d_2), 1)\}e^{(s_1+s_2)(6(s_1+s_2)-1)}d^{3(s_1+s_2-1)}\log(2d)P^{s_1+s_2}}{Hc_9(s_1+s_2-1,d)}\right).
\end{aligned}$$

*Then*

$$\mathrm{h}\left(\frac{\nu_1\varepsilon_1}{\nu_3\varepsilon_3}\right) \le \max\{c_{10}, c_{12} + c_{11}\log(\max\{\mathrm{h}(\varepsilon_1), \mathrm{h}(\varepsilon_2), 1\}), c_{13}, \\ c_{15} + c_{14}\log(\max\{\mathrm{h}(\varepsilon_1), \mathrm{h}(\varepsilon_2), 1\})\}$$

*Proof.* Let $\{\mu_1, \ldots, \mu_{s_1-1}\}$ and $\{\rho_1, \ldots, \rho_{s_2-1}\}$ be respectively systems of fundamental $S_i$-units for $K_1$ and $K_2$ as in Lemma 3.3.1; in particular we know

$$\prod_{j=1}^{s_1-1} \mathrm{h}(\mu_j) \le c_1(s_1, d_1)R_1, \qquad \prod_{j=1}^{s_2-1} \mathrm{h}(\rho_j) \le c_1(s_2, d_2)R_2. \tag{3.6.2}$$

We can write

$$\varepsilon_1 = \zeta_1\mu_1^{b_1}\cdots\mu_{s_1-1}^{b_{s_1-1}}, \quad \varepsilon_2 = \zeta_2\rho_1^{f_1}\cdots\rho_{s_2-1}^{f_{s_2-1}},$$

where $\zeta_1$ and $\zeta_2$ are roots of unity and $b_1, \ldots, b_{s_1-1}$, and $f_1, \ldots, f_{s_2-1}$ are rational integers. Set

$$B_1 = \max\{|b_1|, \ldots, |b_{s_1-1}|\}, \quad B_2 = \max\{|f_1|, \ldots, |f_{s_2-1}|\}$$

We deduce from Lemma 3.3.3 that

$$B_1 \le c_5(s_1, d_1)\,\mathrm{h}(\varepsilon_1), \qquad B_2 \le c_5(s_2, d_2)\,\mathrm{h}(\varepsilon_2),$$

and hence

$$B := \max\{c_5(s_1, d_1), c_5(s_2, d_2), 1)\}\max\{\mathrm{h}(\varepsilon_1), \mathrm{h}(\varepsilon_2), 1\} \ge \max\{B_1, B_2\}. \tag{3.6.3}$$

Set $\alpha_0 = -\zeta_2\nu_2/(\zeta_1\nu_1)$ and $b_0 = 1$. By (3.6.1) we have

$$\frac{\nu_3\varepsilon_3}{\nu_1\varepsilon_1} = \alpha_0^{b_0}\mu_1^{-b_1}\cdots\mu_{s_1-1}^{-b_{s_1-1}}\rho_1^{f_1}\cdots\rho_{s_2-1}^{f_{s_2-1}} - 1. \tag{3.6.4}$$

Now choose the place $\upsilon$ of $L$ such that $\|\varepsilon_3/\varepsilon_1\|_\upsilon$ is minimal. From Lemma 3.2.2 we deduce that

$$\mathrm{h}(\varepsilon_3/\varepsilon_1) \le -\frac{s}{d}\log\left(\|\varepsilon_3/\varepsilon_1\|_\upsilon\right). \tag{3.6.5}$$

We will compute a lower bound for the linear form (3.6.4) using the techniques from Section 3.5. Observe that

$$\|\varepsilon_3/\varepsilon_1\|_v = \frac{\|\nu_3\varepsilon_3/(\nu_1\varepsilon_1)\|_v}{\|\nu_3/\nu_1\|_v}.$$

Combining this with Lemma 3.2.1 and (3.6.5) we get

$$\mathrm{h}\left(\frac{\nu_3\varepsilon_3}{\nu_1\varepsilon_1}\right) \leq 2H(s+1) - \frac{s}{d}\log\left\|\frac{\nu_3\varepsilon_3}{\nu_1\varepsilon_1}\right\|_v, \tag{3.6.6}$$

and hence a lower bound for $\log\|\nu_3\varepsilon_3/(\nu_1\varepsilon_1)\|_v$ will give an upper bound for $\mathrm{h}(\nu_3\varepsilon_3/(\nu_1\varepsilon_1))$. Assume first that $v$ is infinite. Set

$$\begin{aligned} A_0 &= 2dH \geq \max(d\,\mathrm{h}(\alpha_0), \pi), \\ A_i &= \begin{cases} \max(d\,\mathrm{h}(\mu_i), \pi), & i = 1, \ldots, s_1 - 1, \\ \max(d\,\mathrm{h}(\rho_{i-(s_1-1)}), \pi), & i = s_1, \ldots, s_1 + s_2 - 2. \end{cases} \end{aligned} \tag{3.6.7}$$

Let $n = s_1 + s_2 - 1$. Since we assumed $s_1$ and $s_2$ to be $\geq 3$, we observe that from Lemma 3.3.2

$$\prod_{i=1}^{n-1} A_i \leq c_4(s_1, d_1)c_4(s_2, d_2)R_1R_2, \tag{3.6.8}$$

and

$$\max_{1\leq i\leq n-1} A_i \leq \max\{c_2(s_1, d_1)R_1, c_2(s_2, d_2)R_2, \pi\}. \tag{3.6.9}$$

We distinguish two cases. First assume that

$$B \leq 2e\max((s_1 + s_2 - 2)\pi/\sqrt{2}, A_1, \ldots, A_{s_1+s_2-2})A_0.$$

From Lemma 3.5.1 and equations (3.6.8) and (3.6.9) we have

$$\begin{aligned} \log\left\|\frac{\nu_3\varepsilon_3}{\nu_1\varepsilon_1}\right\|_v > &- 2d_v dHc_4(s_1, d_1)c_4(s_2, d_2)c_7(n, d)R_1R_2\times \\ &\log(\sqrt{2}e\max\{(s_1 + s_2 - 2)\pi/\sqrt{2}, c_2(s_1, d_1)R_1, c_2(s_2, d_2)R_2)\}. \end{aligned} \tag{3.6.10}$$

Next assume that $B > 2e\max((s_1+s_2-2)\pi/\sqrt{2}, A_1, \dots, A_{s_1+s_2-2})A_0$. Then, using again Lemma 3.5.1 and (3.6.8) we get the following bound.

$$\begin{aligned}\log\left\|\frac{\nu_3\varepsilon_3}{\nu_1\varepsilon_1}\right\|_v > -2d_v dHc_4(s_1,d_1)c_4(s_2,d_2)c_7(n,d)R_1R_2\times \\ \log(B/(2\sqrt{2}dH)).\end{aligned} \tag{3.6.11}$$

Now assume $v$ is finite. Let $\mathfrak{p}$ be a corresponding prime ideal to $v$. Then

$$\log\left\|\frac{\nu_3\varepsilon_3}{\nu_1\varepsilon_1}\right\|_v = -\operatorname{ord}_{\mathfrak{p}}(\alpha_0^{b_0}\mu_1^{-b_1}\cdots\mu_{s_1-1}^{-b_{s_1-1}}\rho_1^{f_1}\cdots\rho_{s_2-1}^{f_{s_2-1}}-1)\log N(\mathfrak{p}). \tag{3.6.12}$$

Again, we distinguish two cases. First assume that

$$B < 4c_9(n,d)H\,\mathrm{h}(\mu_1)\cdots\mathrm{h}(\mu_{s_1-1})\,\mathrm{h}(\rho_1)\cdots\mathrm{h}(\rho_{s_2-1}).$$

In this case we will directly compute an upper bound for $\mathrm{h}(\nu_3\varepsilon_3/(\nu_1\varepsilon_1))$. From (3.6.4) and Lemma 3.3.1 we deduce that

$$\mathrm{h}\left(\frac{\nu_3\varepsilon_3}{\nu_1\varepsilon_1}\right) \le \log 2 + 2H + B(n-1)\max\{c_2(s_1,d_1)R_1, c_2(s_2,d_2)R_2\}.$$

Then, from our assumption for $B$ and (3.6.2) we get

$$\begin{aligned}\mathrm{h}\left(\frac{\nu_3\varepsilon_3}{\nu_1\varepsilon_1}\right) \le \log 2 + 2H + 4(n-1)Hc_1(s_1,d_1)c_1(s_2,d_2)c_9(n,d)\times \\ R_1R_2\max\{c_2(s_1,d_1)R_1, c_2(s_2,d_2)R_2\}.\end{aligned} \tag{3.6.13}$$

We next assume

$$B \ge 4c_9(n,d)H\,\mathrm{h}(\mu_1)\cdots\mathrm{h}(\mu_{s_1-1})\,\mathrm{h}(\rho_1)\cdots\mathrm{h}(\rho_{s_2-1}).$$

Since $2H \ge 1$ we have $h_0' = \max\{\mathrm{h}(\alpha_0), 1/(16e^2d^2)\} \le 2H$. Moreover, using Lemma 3.2.4, for $i = 1, \dots, s_1-1$ and $j = 1, \dots, s_2-1$ we have

$$h_i' = \max\{\mathrm{h}(\mu_i), (16e^2d^2)^{-1}\} = \mathrm{h}(\mu_i),$$

and

$$h_{j+s_1-1}' = \max\{\mathrm{h}(\rho_j), (16e^2d^2)^{-1}\} = \mathrm{h}(\rho_j).$$

Choose now

$$\delta = 2c_9(n,d)H\,\mathrm{h}(\mu_1)\cdots\mathrm{h}(\mu_{s_1-1})\,\mathrm{h}(\rho_1)\cdots\mathrm{h}(\rho_{s_2-1})/B.$$

It is clear from our assumption for $B$ that $\delta \leq 1/2$. We apply Lemma 3.5.2 to (3.6.4) to obtain the following bound:

$$\log\left\|\frac{\nu_3\varepsilon_3}{\nu_1\varepsilon_1}\right\|_v > -c_8(n,d)d^n\frac{N(\mathfrak{p})}{\log N(\mathfrak{p})}2H\prod_{i=1}^{s_1-1}\mathrm{h}(\mu_i)\prod_{j=1}^{s_2-1}\mathrm{h}(\rho_j)\max\{\log M_0,1\},$$

where

$$M_0 = Be^{(n+1)(6n+5)}d^{3n}\log(2d)N(\mathfrak{p})^{n+1}/(Hc_9(n,d)).$$

We observe that $N(\mathfrak{p})/\log N(\mathfrak{p}) \leq (1/\log 2)P/\log^* P$. Hence, using (3.6.2) and the last inequality we have

$$\log\left\|\frac{\nu_3\varepsilon_3}{\nu_1\varepsilon_1}\right\|_v > -\frac{2Hd^nP}{\log 2\log^* P}c_1(s_1,d_1)c_1(s_2,d_2)c_8(n,d)R_1R_2\log M, \qquad (3.6.14)$$

where

$$M = Be^{(n+1)(6n+5)}d^{3n}\log(2d)P^{n+1}/(Hc_9(n,d)).$$

The lower bounds for $\log\|\nu_3\varepsilon_3/(\nu_1\varepsilon_1)\|_v$ given in Equations (3.6.10), (3.6.11) and (3.6.14) together with equation (3.6.6), and (3.6.13) complete the proof of the Proposition. □

## 3.7 Upper bounds for the size of $S$-integral points on hyperelliptic curves

We can now give an explicit bound for the size of $S$-integral points on the hyperelliptic curve given by the affine model (3.1.1). This is an extension of Theorem 9.2 of [15] and we follow the proof there, adding the needed details for the $S$-integral case. We include the bounds for unit equations given in the previous section that are different from those on [15]. First we will fix some notation. Let $S$ be a finite set of rational primes of cardinality $s$. For a number field $K$, we will denote by $S_K$ the set of places of $K$ over the primes in $S$, together with the infinite places.

**Theorem 3.7.1.** *Let $S$ be a finite set of rational primes of cardinality $s$. Let $P$ be the largest prime in $S$, with the convention that $P = 1$ if $S$ is empty. Let $\alpha$ be an algebraic integer of degree at least $3$, and let $\kappa$ be an integer belonging to $K = \mathbb{Q}(\alpha)$. Let $\alpha_1, \alpha_2, \alpha_3$ be different conjugates of $\alpha$ and let $\kappa_1, \kappa_2, \kappa_3$ be the corresponding conjugates of $\kappa$. Let*

$$K_1 = \mathbb{Q}(\alpha_1, \alpha_2, \sqrt{\kappa_1\kappa_2}), \quad K_2 = \mathbb{Q}(\alpha_1, \alpha_3, \sqrt{\kappa_1\kappa_3}), \quad K_3 = \mathbb{Q}(\alpha_2, \alpha_3, \sqrt{\kappa_2\kappa_3}),$$

*and*

$$L = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \sqrt{\kappa_1\kappa_2}, \sqrt{\kappa_1\kappa_3}).$$

*Let $d_1, d_2, d_3$ and $r_1, r_2, r_3$ be the degrees and the unit ranks of $K_1, K_2, K_3$ respectively. Let $d$ be the degree of $L$. Let $R$ be an upper bound for the regulators of $K_1, K_2, K_3$ and $R_S$ an upper bound for the respective $S_{K_i}$-regulators of $K_1, K_2, K_3$. Let $s_i$ be the number of places in $S_{K_i}$. Let $h$ be an upper bound for the class numbers of the $K_i$. Let*

$$\begin{aligned}
c_j^* &= \max_{i=1,2} c_j(s_i, d_i), \quad j = 1, \ldots, 5,\\
c_6^* &= \max_{i=1,2,3} c_6(r_i, d_i),\\
N &= \max_{1\le i,j\le 3} \left|\mathrm{Norm}_{\mathbb{Q}(\alpha_i,\alpha_j)/\mathbb{Q}}(\kappa_i(\alpha_i - \alpha_j))\right|^2,\\
H^* &= \max\left\{\frac{\log N}{\min_{i=1,2,3} d_i} + h\left(\sum_{p\in S}\log p\right) + c_6^* R + \mathrm{h}(\kappa), 1, \pi/d\right\}.\\
c_{10}^* &= 2H^* + 2H^* d(s+1)(1 + 2(c_4^*)^2 c_7(s_1+s_2-1, d)R_S^2\times\\
&\qquad \log(\sqrt{2}e\max\{(s_1+s_2-2)\pi/\sqrt{2}, c_2^* R_S\}),\\
c_{11}^* &= 4d(s+1)H^*(c_4^*)^2 c_7(s_1+s_2-1, d)R_S^2\\
c_{12}^* &= 2H^* + 2H^*(d(s+1)) + c_{11}^* \log\left(\frac{\max\{c_5^*, 1\}}{2\sqrt{2}dH^*}\right),\\
c_{13}^* &= \log 2 + 2H^* + 4(s_1+s_2-2)H^*\,(c_1^*)^2\, c_2^* c_9(s_1+s_2-1, d)R_S^3
\end{aligned}$$

$$c_{14}^* = \frac{2H^* d^{s_1+s_2-2} P^d}{\log(2)\log^*(P^d)} (c_1^*)^2 \, c_8(s_1+s_2,d) R_S^2$$

$$c_{15}^* = 2H^* + 2H^* d(s+1) +$$
$$c_{14}^* \log\left( \frac{\max\{c_5^*,1\} e^{(s_1+s_2)(6(s_1+s_2)-1)} d^{3(s_1+s_2-1)} \log(2d) P^{d(s_1+s_2)}}{H^* c_9(s_1+s_2-1,d)} \right).$$

*If $x \in \mathbb{Q}\backslash\{0\}$ is a $S$-integer satisfying $x-\alpha = \kappa\xi^2$ for some $\xi \in K$ then*

$$\begin{aligned} \mathrm{h}(x) \le{}& 20\log 2 + 13\,\mathrm{h}(\kappa) + 19\,\mathrm{h}(\alpha) + H^* + \\ & 8\max\{c_{10}^*/2, c_{13}^*/2, c_{12}^* + c_{11}^* \log c_{11}^*, c_{15}^* + c_{14}^* \log c_{14}^*\}. \end{aligned} \tag{3.7.1}$$

*In the particular case when $S$ is empty, we have*

$$\mathrm{h}(x) \le 20\log 2 + 13\,\mathrm{h}(\kappa) + 19\,\mathrm{h}(\alpha) + H^* + 8\max\{c_{10}^*/2, c_{12}^* + c_{11}^* \log c_{11}^*\}.$$

*Proof.* For $a \in K$ and $i = 1,2,3$, we will write $a_i$ for the corresponding conjugates of $a$. Conjugating the relation $x-\alpha = \kappa\xi^2$ appropriately and taking differences we obtain

$$\alpha_1 - \alpha_2 = \kappa_2\xi_2^2 - \kappa_1\xi_1^2, \quad \alpha_3 - \alpha_1 = \kappa_1\xi_1^2 - \kappa_3\xi_3^2, \quad \alpha_2 - \alpha_3 = \kappa_3\xi_3^2 - \kappa_2\xi_2^2.$$

Let

$$\tau_1 = \kappa_1\xi_1, \qquad \tau_2 = \sqrt{\kappa_1\kappa_2}\xi_2, \qquad \tau_3 = \sqrt{\kappa_1\kappa_3}\xi_3.$$

Observe that

$$\kappa_1(\alpha_1-\alpha_2) = \tau_2^2 - \tau_1^2, \quad \kappa_1(\alpha_3-\alpha_1) = \tau_1^2 - \tau_3^2, \quad \kappa_1(\alpha_2-\alpha_3) = \tau_3^2 - \tau_2^2,$$

and

$$\tau_2 \pm \tau_1 \in K_1, \quad \tau_1 \pm \tau_3 \in K_2, \quad \tau_3 \pm \tau_2 \in \sqrt{\kappa_1/\kappa_2} K_3.$$

The equation $\tau_2^2 = \kappa_1(x-\alpha_2)$ shows that $\tau_2$ is a $S_{K_1}$-integer, and so are $\tau_2+\tau_1$ and $\tau_2-\tau_1$. Write $\nu' = \tau_2 - \tau_1$. Since $(\tau_2-\tau_1)(\tau_2+\tau_1) = \kappa_1(\alpha_1-\alpha_2)$ we have

$$N_{S_{K_1}}(\nu') \le N_{S_{K_1}}(\kappa_1(\alpha_1-\alpha_2)).$$

By Lemma 3.3.4 there is a $S_{K_1}$ unit $\varepsilon$ of $K_1$ such that

$$\mathrm{h}(\nu'\varepsilon) \le c_6(r_1,d_1)R + \frac{\log N_{S_{K_1}}(\kappa_1(\alpha_1-\alpha_2))}{[K_1:\mathbb{Q}]} + h\left(\sum_{p\in S}\log p\right).$$

Write $\nu_1 = \nu'\varepsilon$ and $\varepsilon_1 = \varepsilon^{-1}$. Hence we have expressed $\tau_2 - \tau_1$ in the form $\nu_1\varepsilon_1$ where $\varepsilon_1$ is a $S_{K_1}$-unit and $\mathrm{h}(\nu_1) \leq H^*$. We can repeat the same process on $\tau_2+\tau_1$. Similarly, the equation $\tau_3^2 = \kappa_1(x - \alpha_3)$ shows that $\tau_3$, $\tau_1 + \tau_3$ and $\tau_1 - \tau_3$ are $S_{K_2}$-integers, and we can repeat the process to write now $\tau_1 \pm \tau_3$ in the form $\nu_2\varepsilon_2$ where $\varepsilon_2$ is a $S_{K_2}$-unit and $\mathrm{h}(\nu_2) \leq H^*$.

We now want to express $\tau_2 \pm \tau_3$ in a similar way. Define $\nu'' = \sqrt{\kappa_2/\kappa_1}(\tau_2 - \tau_3)$. Note $\nu'' = \kappa_2\xi_2 - \sqrt{\kappa_2\kappa_3}\xi_3$ is a $S_{K_3}$-integer of $K_3$. Similarly, $\sqrt{\kappa_2/\kappa_1}(\tau_2 + \tau_3)$ is a $S_{K_3}$-integer of $K_3$ and

$$\nu''\sqrt{\kappa_2/\kappa_1}(\tau_2 + \tau_3) = \kappa_2(\alpha_2 - \alpha_3).$$

Hence, $\mathrm{Norm}_{S_{K_3}}(\nu'') \leq N$. Using again Lemma 3.3.4 there is a $S_{K_3}$-unit $\varepsilon_3$ such that $\nu'' = \nu'\varepsilon$ and

$$\mathrm{h}(\nu') \leq c_6(r_3, d_3)R + \frac{\log N_{S_{K_3}}(\kappa_2(\alpha_2 - \alpha_3))}{[K_1 : \mathbb{Q}]} + h\left(\sum_{p\in S} \log p\right).$$

Let $\nu = \sqrt{\kappa_1/\kappa_2}\nu'$. Thus $\tau_2 - \tau_3 = \nu\varepsilon$ where $\mathrm{h}(\nu) \leq \mathrm{h}(\nu') + \mathrm{h}(\kappa) \leq H^*$. We will apply Proposition 3.6.1 to the unit equation

$$(\tau_1 - \tau_2) + (\tau_3 - \tau_1) + (\tau_2 - \tau_3) = 0,$$

which is indeed of the form $\nu_1\varepsilon_1 + \nu_2\varepsilon_2 + \nu_3\varepsilon_3 = 0$ where $\varepsilon_1$ is a $S_{K_1}$-unit of $K_1$, $\varepsilon_2$ is a $S_{K_2}$-unit of $K_2$ and we consider $\varepsilon_3$ as a $S_L$-unit of $L$. Observe that, since $\sum_{v|p} d_v = d$, then there are at most $d$ places in $S_L$ over a prime in $S$ and hence $S$ has at most $d(s+1)$ elements. We obtain

$$\mathrm{h}\left(\frac{\tau_1 - \tau_2}{\tau_2 - \tau_3}\right) \leq \max\begin{cases} c_{10}^*, \\ c_{13}^*, \\ c_{12}^* + c_{11}^* \log(\max\{\mathrm{h}(\varepsilon_1), \mathrm{h}(\varepsilon_2), 1\}), \\ c_{15}^* + c_{14}^* \log(\max\{\mathrm{h}(\varepsilon_1), \mathrm{h}(\varepsilon_2), 1\}). \end{cases}$$

To ease notation we write $A_1 + A_2 \log(\max\{\mathrm{h}(\varepsilon_1), \mathrm{h}(\varepsilon_2), 1\})$ for the expression that attains the maximum in the last inequality, where we take $A_2$ to be $0$ if the maximum is attained in one of the first two cases. Note that

$$\mathrm{h}(\varepsilon_i) \leq \mathrm{h}(\nu_i \varepsilon_i) + \mathrm{h}(\nu_1) \leq \mathrm{h}(\nu_i \varepsilon_i) + H^*,$$

since $\varepsilon_i = \nu_i \varepsilon_i / \nu_i$. We derive as in [15] that

$$\mathrm{h}(\tau_i \pm \tau_j) \leq 2 \log 2 + 3\,\mathrm{h}(\kappa) + \mathrm{h}(\alpha) + \mathrm{h}(x).$$

Hence,

$$\mathrm{h}\left(\frac{\tau_1 - \tau_2}{\tau_2 - \tau_3}\right) \leq A_1 + A_2 \log(A_3 + \mathrm{h}(x)), \tag{3.7.2}$$

where $A_3 = H^* + 2 \log 2 + 3\,\mathrm{h}(\kappa) + \mathrm{h}(\alpha)$. We also apply Proposition 3.6.1 to the unit equation

$$-(\tau_1 + \tau_2) + (\tau_3 + \tau_1) + (\tau_2 - \tau_3) = 0,$$

to obtain precisely the same bound for $\mathrm{h}\left(\frac{\tau_1 + \tau_2}{\tau_2 - \tau_3}\right)$. Using the identity

$$\left(\frac{\tau_1 - \tau_2}{\tau_2 - \tau_3}\right) \cdot \left(\frac{\tau_1 + \tau_2}{\tau_2 - \tau_3}\right) = \frac{\kappa_1(\alpha_2 - \alpha_1)}{(\tau_2 - \tau_3)^2},$$

we obtain that

$$\mathrm{h}(\tau_2 - \tau_3) \leq \frac{\log 2 + \mathrm{h}(\kappa)}{2} + \mathrm{h}(\alpha) + A_1 + A_2 \log(A_3 + \mathrm{h}(x)).$$

We derive as in [15] that

$$\mathrm{h}(x) \leq 7 \log 2 + 5\,\mathrm{h}(\alpha) + 3\,\mathrm{h}(\kappa) + 4\,\mathrm{h}(\tau_2 - \tau_3).$$

Thus

$$\mathrm{h}(x) \leq 9 \log 2 + 9\,\mathrm{h}(\alpha) + 5\,\mathrm{h}(\kappa) + 4A_1 + 4A_2 \log(A_3 + \mathrm{h}(x)).$$

If $A_2 = 0$ we obtain (3.7.1) directly. Otherwise, using Lemma 9.1 of [15] we complete the proof of the theorem. □

We use Theorem 3.7.1 in conjunction with Lemmas 3.1.1 and 3.1.2 to obtain an upper bound for the size of all $S$-integral points on a hyperelliptic curve with model (3.1.1).

*Remark.* We use here the notation of Section 3.1. In the even degree case, the set $\mathcal{K}$ is the union of the sets $\epsilon\mathcal{B}_\epsilon$, where $\epsilon \in \mathcal{E}$. The set $\mathcal{B}_\epsilon$ consists of square free rational integers supported by primes dividing $a\Delta \operatorname{Norm}_{K/\mathbb{Q}}(\epsilon)\prod_{p\in S} p$. Hence, the fields $K_1, K_2, K_3$ and $L$ defined in the statement of the previous theorem are the same for all $\kappa \in \epsilon\mathcal{B}_\epsilon$. In order to get the desired upper bound for the size of all $S$-integral points we only need to compute the bound for the $\kappa \in \epsilon\mathcal{B}_\epsilon$ that maximises $\mathrm{h}(\kappa)$ and $\operatorname{Norm}_{\mathbb{Q}(\alpha_i,\alpha_j)/\mathbb{Q}}(\kappa_i(\alpha_i-\alpha_j))$, namely $\kappa = b\epsilon$ where $b$ is the largest square-free rational integer dividing $a\Delta \operatorname{Norm}_{K/\mathbb{Q}}(\epsilon)\prod_{p\in S} p$. Thus, though in the even degree case the set $\mathcal{K}$ is much bigger than in the odd degree case, the computation of the upper bound for the size of the $S$-integral points is essentially not more complicated than that in the odd degree case.

**Example 3.7.2.** This is a continuation of Example 2.4.2. Let $\mathcal{C}$ be the curve defined by

$$Y^2 = 4X^5 - 4X + 1,$$

and let $S$ be the set of the first $22$ primes. We transform the equation into

$$\mathcal{C} \quad : \quad 2y^2 = x^5 - 16x + 8, \tag{3.7.3}$$

via the change of variables $y = 2Y$ and $x = 2X$ which preserves $S$-integrality. The curve $\mathcal{C}$ given by the model (3.7.3) is the same curve as the one in the proof of Theorem 1.1 of [15]. The authors compute an upper bound for the size of the integral points on the curve. We will here compute a bound for the $S$-integral points. Denote by $J$ the Jacobian of $\mathcal{C}$. We had seen in Example 2.4.2 that $J(\mathbb{Q})$ is free of rank $3$. A set of generators for $J(\mathbb{Q})$ is given by

$$D_1 = (0,2) - \infty, \qquad D_2 = (2,2) - \infty, \qquad D_3 = (-2,2) - \infty.$$

Let $f(x) = x^5 - 16x + 8$. Let $\alpha$ be a root of $f$. We choose for coset representatives of $J(\mathbb{Q})/2J(\mathbb{Q})$ the linear combinations $\sum_{i=1}^{3} n_i D_i$ with $n_i \in \{0, 1\}$. For a given set of primes $S$ we have that any $S$-integral point of (3.7.3) (in fact, any rational point) satisfies

$$x - \alpha = \kappa \xi^2,$$

where $\kappa \in \mathcal{K}$ and $\mathcal{K}$ is constructed as in Lemma 3.1.1. Next, we compute the bounds for $\mathrm{h}(x)$ given by Theorem 3.7.1 for every $\kappa \in \mathcal{K}$. We implemented our bounds in `MAGMA` [5]. As remarked in [15], the Galois group of $f$ is $S_5$, which implies that the fields $K_1, K_2, K_3$ corresponding to a particular $\kappa$ are isomorphic. We tabulate the bounds for each $\kappa \in \mathcal{K}$ for the set $S$ of primes up to 79 in Table 3.1. Thus, if $(x, y)$ is an $S$-integral

Table 3.1: Bounds for the height of $S$-integral points on (3.7.3)

| coset of $J(\mathbb{Q})/2J(\mathbb{Q})$ | $\kappa$ | $S_{K_i}$-unit rank of $K_i$ | bound $R$ for $S_{K_i}$-regulator of $K_i$ | bound for $\mathrm{h}(x)$ |
|---|---|---|---|---|
| $0$ | $1$ | $154$ | $8.5 \times 10^{301}$ | $7.8 \times 10^{4025}$ |
| $D_1$ | $-2\alpha$ | $266$ | $1.6 \times 10^{603}$ | $1.6 \times 10^{8421}$ |
| $D_2$ | $4 - 2\alpha$ | $258$ | $4.2 \times 10^{576}$ | $1.9 \times 10^{8160}$ |
| $D_3$ | $-4 - 2\alpha$ | $262$ | $1.0 \times 10^{596}$ | $4.7 \times 10^{8301}$ |
| $D_1 + D_2$ | $-2\alpha + \alpha^2$ | $257$ | $1.7 \times 10^{581}$ | $1.3 \times 10^{8135}$ |
| $D_1 + D_3$ | $2\alpha + \alpha^2$ | $264$ | $7.1 \times 10^{591}$ | $5.6 \times 10^{8352}$ |
| $D_2 + D_3$ | $-4 + \alpha^2$ | $264$ | $3.1 \times 10^{600}$ | $1.2 \times 10^{8364}$ |
| $D_1 + D_2 + D_3$ | $8\alpha - 2\alpha^3$ | $266$ | $2.2 \times 10^{596}$ | $1.5 \times 10^{8415}$ |

point of (3.7.3) we have

$$\mathrm{h}(x) \leq 1.6 \times 10^{8421}.$$

We have also computed the bounds in the case when $S$ is the empty set, in other words, a bound for the size of the integral points on (3.7.3). We get $\mathrm{h}(x) \leq 4.4 \times 10^{428}$. The bound in [15] is $5.1 \times 10^{565}$. Recalling the definition of size given at the beginning of this chapter, this means that an $S$-integral point $P = (x, y)$ on the curve, with $x = p/q$, $p, q \in \mathbb{Z}$ and $(p, q) = 1$ will have

$$\max\{|p|, |q|\} \leq \exp(1.6 \times 10^{8421}).$$

If the point $P$ is an integral point on the curve, then

$$|x| \leq \exp(4.4 \times 10^{428})$$

which gives a significant improvement on the bound given in [15].

**Example 3.7.3.** Let $\mathcal{C}$ be the genus $2$ curve defined by the equation

$$y^2 = f(x) = x^6 + x + 2. \tag{3.7.4}$$

Let $S = \{2, 3, 5\}$. Using `MAGMA` we find some rational points on the curve:

$$\infty_+,\ \infty_-,\ (1, -2),\ (1, 2),\ (-2, -8),\ (-2, 8).$$

The Mordell–Weil group of the curve is free of rank $2$, so Chabauty's method to find the $S$-integral points on the curve does not apply in this case.

A basis for the Mordell–Weil group is given by

$$D_1 = \infty_+ - \infty_-, \quad D_2 = (1, 2) - \infty_-.$$

We will now compute the set $\mathcal{K}$ as in Lemma 3.1.2. We choose as representatives for $J(\mathbb{Q})/2J(\mathbb{Q})$ the divisors $0, D_1, D_2$, and $D_1 - D_2$, which is linearly equivalent to $(1, -2) - \infty_-$. Take $P_0 = \infty_-$. We then choose $\epsilon_0 = 1$, and we can easily see that the $\epsilon$ we associate to $0$ and $D_1$ is $1$, whereas we associate $1 - \alpha$ to $D_2$, and $D_1 - D_2$, where $\alpha$ is a root of $f$. The discriminant $\Delta$ of the polynomial $f$ is $-1489867$, which is prime. Let $K = \mathbb{Q}(\alpha)$. We have that $\mathrm{Norm}_{K/\mathbb{Q}}(1 - \alpha) = 4$. Following the notation of Lemma 3.1.2, the set $\mathcal{B}_1$ consists of the square-free rational integers supported by the prime $1489867$ and the primes in $S$. The set $\mathcal{B}_{1-\alpha}$ consists of the square-free rational integers supported by the primes $2, 1489867$, and the primes in $S$. Finally, the set $\mathcal{K}$ consists of the set $\mathcal{B}_1$ together with the set $(1 - \alpha)\mathcal{B}_{1-\alpha}$.

According to the remark following Theorem 3.7.1, we only need to compute the upper bounds given by $\kappa_1 = 2 \cdot 3 \cdot 5 \cdot 1489867$ and $\kappa_2 = 2 \cdot 3 \cdot 5 \cdot 1489867(1 - \alpha)$. Using `MAGMA` we find that an upper bound for the size of the $S$-integral points on the curve $C$ is $5.57 \times 10^{2218}$.

## 3.8 The Mordell–Weil sieve

We have given explicit upper bounds for the size of the $S$-integral points of a hyperelliptic curve. As we saw in the examples, the bounds are astronomical, and we cannot expect to search for all points below that bound. One usually looks for points of small size and tries to prove the points found are all the $S$-integral points on the curve. In this section we use a powerful variant of the Mordell–Weil sieve [15, Sections 10–12] to show that any rational point on a curve is either a known rational point or a point with very large height. If the unknown rational points have a height larger than the upper bound obtained for the size of the $S$-integral points, then we have found all the $S$-integral points.

We now summarize the method described in [15]. Let $\mathcal{C}/\mathbb{Q}$ be a smooth projective curve (not necessarily hyperelliptic) of genus $g \geq 2$ and let $J$ be its Jacobian. As indicated in the introduction, we assume the knowledge of some rational point on $\mathcal{C}$. Let $P_0$ be a fixed rational point on $\mathcal{C}$ and let $\jmath$ be the corresponding Abel–Jacobi map:

$$\jmath : \mathcal{C} \to J, \quad P \mapsto [P - P_0].$$

Let $W$ be the image in $J$ of the known rational points on $\mathcal{C}$. Let $r$ be the rank of $J(\mathbb{Q})$ and $D_1, \ldots, D_r$ generators for the free part of $J(\mathbb{Q})$. Let

$$\phi : \mathbb{Z}^r \to J(\mathbb{Q}), \quad \phi(a_1, ..., a_r) = \sum a_i D_i,$$

so that the image of $\phi$ is simply the free part of $J(\mathbb{Q})$. The variant of the Mordell-Weil sieve as explained in [15] is a strategy for obtaining a very long decreasing sequence of lattices in $\mathbb{Z}^r$:

$$L_0 \supsetneq L_1 \supsetneq L_2 \cdots \supsetneq L_k = L \tag{3.8.1}$$

such that

$$\jmath(\mathcal{C}(\mathbb{Q})) \subset W + \phi(L_j)$$

for $j = 1, \ldots, k$. It consists of two steps. The first is finding a large integer $B$ such that

$$\jmath(\mathcal{C}(\mathbb{Q})) \subset W + \phi(B\mathbb{Z}^r).$$

Set $L_0 = B\mathbb{Z}^r$. The second step requires running through many primes $q$ of good reduction for $\mathcal{C}$. Reducing modulo $q$, the authors get under certain conditions an explicit sequence of sublattices with the required properties. We remark that many of the primes will not give any new information, or will make the computations very slow. Eventually we expect to get a lattice $L$ such that $\jmath(\mathcal{C}(\mathbb{Q})) \subset W + \phi(L)$. Since explicit generators for the lattice can be computed, we can compute as well a positive integer $B_1$ such that $L \subseteq B_1\mathbb{Z}^r$. If the generators of the lattice are large enough, this integer will be considerably larger than $B$. We can restart the application of the second strategy using this new integer and consider now the primes that did not give new information in the previous round. Many of these primes will now give new information and we will get a smaller lattice $L'$ satisfying the required conditions. In our computations this has resulted in a quicker way of finding a lattice with very large generators compared to only carrying on with larger and larger primes $q$ of good reduction.

The following lemma [15, Lemma 12.1] gives a lower bound for the size of rational points whose image does not belong to the set $W$.

**Lemma 3.8.1.** *Let $W$ be a finite subset of $J(\mathbb{Q})$, and let $L$ be a sublattice of $\mathbb{Z}^r$. Suppose that $\jmath(\mathcal{C}(\mathbb{Q})) \subset W + \phi(L)$. Let $\mu_1$ be a lower bound for $h - \hat{h}$ as in* (2.2.1)*. Let*

$$\mu_2 = \max\left\{\sqrt{\hat{h}(w)} \ : \ w \in W\right\}.$$

*Let $M$ be the height-pairing matrix for the Mordell–Weil basis $D_1, \ldots, D_r$ and let $\lambda_1, \ldots, \lambda_r$ be its eigenvalues. Let*

$$\mu_3 = \min\left\{\sqrt{\lambda_j} \ : \ j = 1, \ldots, r\right\}.$$

*Let $m(L)$ be the Euclidean norm of the shortest non-zero vector of $L$, and suppose that $\mu_3 m(L) \geq \mu_2$. Then, for any $P \in \mathcal{C}(\mathbb{Q})$, either $\jmath(P) \in W$ or*

$$h(\jmath(P)) \geq (\mu_3 m(L) - \mu_2)^2 - \mu_1.$$

**Example 3.8.2.** This is a continuation of Example 3.7.2. Consider the genus $2$ curve $Y^2 - Y = X^5 - X$. This curve is the same as in Theorem 1.1 in [15]. Let $S$ be the set

of the first $22$ primes. We transform the equation $Y^2 - Y = X^5 - X$ into

$$\mathcal{C} \quad : \quad 2y^2 = x^5 - 16x + 8, \tag{3.8.2}$$

via the change of variables $y = 4Y - 2$ and $x = 2X$ which preserves $S$-integrality. The curve $\mathcal{C}$ is the same considered in Example 3.7.2. In that example we proved that if $(x, y)$ is an $S$-integral point of (3.7.3) we have

$$\mathrm{h}(x) \leq 1.6 \times 10^{8421}.$$

We also computed a set of generators for $J(\mathbb{Q})$. It is given by

$$D_1 = (0, 2) - \infty, \qquad D_2 = (2, 2) - \infty, \qquad D_3 = (-2, 2) - \infty.$$

The set of known rational points on $\mathcal{C}$ consists of the following 17 points:

$$\infty,\ (-2, \pm 2),\ (0, \pm 2),\ (2, \pm 2),\ (4, \pm 22),\ (6, \pm 62),$$
$$(1/2, \pm 1/8),\ (-15/8, \pm 697/256),\ (60, \pm 19718).$$

We now apply the implementation of the Mordell–Weil sieve explained in this chapter. Let $W$ denote the image of this set in $J(\mathbb{Q})$. From [15] we know that $\jmath(\mathcal{C}(\mathbb{Q})) \subseteq W + BJ(\mathbb{Q})$ where

$$B = 444932978061474820647297268617994065251575448327430679656821404800 0.$$

We are now ready to start the implementation of the variant of the Mordell–Weil sieve explained in the present section. We apply Lemma 11.1 in [15] successively to primes of good reduction that satisfy the conditions of the lemma and Criteria (I)–(IV) in [15, p. 878]. Once we have tried with all the first $50000$ primes in $\mathbb{N}$, we obtain a lattice $L_1$ of approximate index $7.6 \times 10^{2534}$. This lattice satisfies

$$L_1 \subset B_1 \mathbb{Z}^3,$$

where

$$B_1 = 5186741896925513071830083009825556124942917192193989646274007029699373573973400334073122166989734932220032461464914836423781724500387155455257408447361695982490888926739368195706524280686958842758289131220782597477643207682612837102714721726154880000.$$

We start again with this $B_1$ instead of $B$ and we now sieve using the primes which did not satisfied the criteria in the first application. We go on using the first $50000$ primes, and after three more repetitions replacing the values of $B$, we find a lattice $L$ in $\mathbb{Z}^3$ of approximate index $5.7 \times 10^{13161}$ with $\jmath(\mathcal{C}(\mathbb{Q})) \subset W + \phi(L)$. Let $\mu_1, \mu_2, \mu_3$ be as in the notation of Lemma 3.8.1. Using `MAGMA` we find $\mu_1 = 2.167, \mu_2 = 2.612, \mu_3 = 0.378$ (to 3 decimal places). The shortest nonzero vector of $L$ has Euclidean length approximately $1.06 \times 10^{4387}$. Lemma 3.8.1 implies that if $P$ is not one of the known rational points on $\mathcal{C}$, then

$$h(\jmath(P)) \geq 1.6 \times 10^{8773}.$$

Write $P = (x, y)$. Then $h(\jmath(P)) = \mathrm{h}(2x^2) \leq \log 2 + 2\,\mathrm{h}(x)$ and

$$\mathrm{h}(x) \geq 8.02 \times 10^{8772}.$$

This contradicts the bounds given in Table 3.1 for $\mathrm{h}(x)$ for the set of $S$-integral points where $S$ is the set of the first 22 primes and shows that the only $S$-integral points on the curve $Y^2 - Y = X^5 - X$ are

$$(-1, 0),\ (-1, 1),\ (0, 0),\ (0, 1),\ (1, 0),\ (1, 1),\ (2, -5),\ (2, 6),$$
$$(3, -15),\ (3, 16),\ (1/64, 15/32),\ (1/64, 17/32),\ (-15/4096, -185/1024),$$
$$(-15/4096, 1209/1024),\ (30, -4929),\ (30, 4930).$$

The reader can find the MAGMA programs for verifying the above computations at:

http://www.warwick.ac.uk/staff/H.R.Gallegos-Ruiz/programs/sintegral/

*Remark.* The variant of the Mordell–Weil sieve used in this section works in a general setting. But it is computationally expensive, in particular it is memory and time-consuming. The computations for the example presented above took about 17 days in a workstation equipped with 120 GB in RAM and four 2.4 GHz Quad-Core AMD Opteron processors.

# Chapter 4

# Periods of genus $2$ curves defined over the reals

Let $f$ be a degree $5$ or $6$ polynomial defined over $\mathbb{R}$ with real roots only, all different. In the next chapter, we will need to compute numerically integrals of the form

$$\int_{x_1}^{x_2} \frac{S(t)dt}{\sqrt{|f(t)|}},$$

for $x_1, x_2 \in \mathbb{R}$, where $S(t) = s_1 t + s_2$ is a degree $1$ polynomial with real coefficients. In this chapter we explain how one can compute such integrals. We first remark that when either $x_1$ or $x_2$ is one of the roots of $f$ the usual numerical methods of integration take too long when one tries to compute the integral to hundreds or thousands of decimal places. Therefore we need to use another method, as we will need such high precision in the next chapter.

In an expository article Bost and Mestre [6] present a version of an algorithm due to Richelot for the numerical computation of the integrals

$$\int_a^{a'} \frac{S(t)dt}{\sqrt{|f(t)|}}, \int_b^{b'} \frac{S(t)dt}{\sqrt{|f(t)|}}, \text{ and } \int_c^{c'} \frac{S(t)dt}{\sqrt{|f(t)|}}, \tag{4.0.1}$$

with $a < a' < b < b' < c < c'$, $f(t) = (t-a)(t-a')(t-b)(t-b')(t-c)(t-c')$ and $S$ is a polynomial with real coefficients of degree $\leq 1$. The algorithm is based on a modified version of the Arithmetic-Geometric Mean (AGM).

The AGM of two positive real numbers $a, b$ is defined as the limit of the recurrently defined sequences

$$a_{n+1} = \frac{a_n + b_n}{2}, \quad b_{n+1} = \sqrt{a_n b_n},$$

where $a_0 = a$ and $b_0 = b$. The sequences $a_n$, $b_n$ have a common limit, so the AGM is well defined. A good exposition on the AGM can be found in [18]. A very important property of the AGM is that the convergence of the sequences $a_n, b_n$ is quadratic, which roughly means that the precision of the $n$-th iteration with respect to the limit is doubled at the following iteration. The AGM had been used before to compute elliptic integrals (that is, when the degree of $f$ is either 3 or 4). Bost and Mestre explain how one can define an 'arithmetic-geometric mean' of six real numbers, and how it is related to the integrals (4.0.1). More precisely, given six different real numbers $a < a' < b < b' < c < c'$ they define six sequences $a_n$, $a'_n$, $b_n$, $b'_n$, $c_n$, $c'_n$ which converge quadratically. The sequences $a_n$ and $a'_n$ (resp. $b_n$, $b'_n$, resp. $c_n$, $c'_n$) have a common limit $\alpha$ (resp. $\beta$, resp. $\gamma$). The main result is that the integrals in (4.0.1) are respectively given by

$$\pi T \frac{S(a)}{(b-a)(c-a)} \quad \pi T \frac{S(b)}{(b-a)(c-b)}, \quad \pi T \frac{S(c)}{(c-a)(c-b)}.$$

where $T$ is the limit of a recurrently defined sequence $t_n$ which depends on $a < a' < b < b' < c < c'$. The precise statements can be found in the following sections.

In [6, Appendice A3] the authors give a list of exercises that lead to an elementary proof of the correctness of their algorithm. They do not give solutions to the exercises, nor a proof of the correctness of the algorithm. It is for this reason that in the present Chapter we will show its correctness. We will also present a modified version of it that will allow us to compute the integrals (4.1.1) for general $x_1, x_2$. The idea behind the modified version is keeping track of the correspondence (see section 4.2 for the definition of correspondence) between the hyperelliptic curves

$$y^2 = (x-a)(x-a')(x-b)(x-b')(x-c)(x-c') = f(x)$$

and

$$y^2 = (x-a_1)(x-a'_1)(x-b_1)(x-b'_1)(x-c_1)(x-c'_1) = f_1(x).$$

Under the correspondences, every point on the first curve corresponds to two points on the second curve. Say $(x_1, \sqrt{f(x_1)})$ corresponds to $(z_1, w_1), (z_2, w_2)$ and $(x_2, \sqrt{f(x_2)})$ corresponds to $(z_3, w_3), (z_4, w_4)$. Then one can compute a direct relation between the integrals (4.1.1)

$$\int_{z_1}^{z_3} \frac{S(t)\ dt}{\sqrt{|f_1(t)|}} \quad \text{and} \quad \int_{z_2}^{z_4} \frac{S(t)\ dt}{\sqrt{|f_1(t)|}}.$$

The chapter is arranged as follows. In Section 4.1 we show how the integrals (4.1.1) can be computed from integrals of that form, but with the following restrictions: $f$ is precisely of degree $6$ and $x_1$ is a root of $f$. In Section 4.2 we first show the correctness of Bost and Mestre's algorithm and we present the modified version of it alluded to above. Finally, in Section 4.3 we present the algorithms in concise form.

## 4.1 Reduction of the problem

We will show that in order to compute the desired integrals for general $f, S, x_1, x_2$, it is enough to compute integrals of the form

$$\int_{x_1}^{x_2} \frac{S(t)dt}{\sqrt{|f(t)|}}, \tag{4.1.1}$$

where $S$ is of degree $1$, $f$ is monic of degree $6$ with real roots only, $x_1$ is one of the roots of $f$, and $f$ is negative along $(x_1, x_2)$.

Assume first that $f$ has degree $5$. Let $x_0 \in \mathbb{R}$ with $x_0$ not a root of $f$. Denote the roots of $f$ by $a_1 < a_2 < a_3 < a_4 < a_5$, and let $f_5$ be the leading coefficient of $f$. Consider the change of variables

$$t' = \frac{1}{t - x_0}.$$

For a nonzero real number $x$ write $\operatorname{sgn}(x)$ for the sign of $x$. Then, if $x_0 < x_1$ or $x_0 > x_2$

$$\int_{x_1}^{x_2} \frac{S(t)dt}{\sqrt{|f(t)|}} = \frac{-1}{\sqrt{|f_5 f(x_0)|}} \int_{x_1'}^{x_2'} \frac{s_1 + t' S(x_0)}{\sqrt{|t' \prod (t' - a_i')|}} \operatorname{sgn}(t') dt'.$$

Note that $\operatorname{sgn}(t)$ does not change along $[x_1, x_2]$ in this case. Now, if $x_1 \leq x_0 \leq x_2$

$$\int_{x_1}^{x_2} \frac{S(t)dt}{\sqrt{|f(t)|}} = \frac{-1}{\sqrt{|f_5 f(x_0)|}} \int_{-\infty}^{x_1'} \frac{s_1 + t'S(x_0)}{\sqrt{|t' \prod (t' - a_i')|}} dt' + \frac{1}{\sqrt{|f_5 f(x_0)|}} \int_{x_2'}^{\infty} \frac{s_1 + t'S(x_0)}{\sqrt{|t' \prod (t' - a_i')|}} dt'. \quad (4.1.2)$$

In the next chapter we will simultaneously compute many integrals of the present kind, and we will choose only one change of variables to do them all. For our convenience, in this degree five case, the point $x_0$ will be chosen in between $a_1$ and $a_2$. Then all of the inequalities considered before involving $x_1, x_2$ and $x_0$ will be present in practice.

The degree $5$ case has then been reduced to the degree $6$ case. From now on we will assume that $f$ has exactly degree $6$.

Now denote the roots of $f$ by $a < a' < b < b' < c < c'$, and let $f_6$ be the leading coefficient of $f$. Note that

$$\int_{x_1}^{x_2} \frac{S(t)dt}{\sqrt{|f(t)|}} = \int_{a}^{x_2} \frac{S(t)dt}{\sqrt{|f(t)|}} - \int_{a}^{x_1} \frac{S(t)dt}{\sqrt{|f(t)|}}$$

and

$$\int_{x_1}^{x_2} \frac{S(t)dt}{\sqrt{|f(t)|}} = \frac{1}{|f_6|} \int_{x_1}^{x_2} \frac{S(t)dt}{\sqrt{|(t-a)(t-a')(t-b)(t-b')(t-c)(t-c')|}}.$$

Then it suffices to compute integrals of the form

$$\int_{a}^{x} \frac{S(t)dt}{\sqrt{|f(t)|}},$$

with $f$ monic. If $x \geq a$, denote by $x_0$ the largest root of $f$ with $x_0 \leq x$. Then

$$\int_{a}^{x} \frac{S(t)dt}{\sqrt{|f(t)|}} = \int_{a}^{x_0} \frac{S(t)dt}{\sqrt{|f(t)|}} + \int_{x_0}^{x} \frac{S(t)dt}{\sqrt{|f(t)|}}.$$

Therefore, we only need to compute the integrals

$$\int_{x_1}^{x_2} \frac{S(t)dt}{\sqrt{|f(t)|}},$$

where $x_1$ and $x_2$ are two consecutive roots of $f$, and also integrals of the form

$$\int_{x}^{a} \frac{S(t)dt}{\sqrt{|f(t)|}} \text{ and } \int_{x_0}^{x} \frac{S(t)dt}{\sqrt{|f(t)|}},$$

where, in the first case $x < a$, and in the second case $x \geq a$ and there are no roots of $f$ in the interval $(x_0, x)$.

We will now assume that $f$ is monic. As we mentioned before, there is no loss of generality in doing this. In this case, $f(t)$ is positive along the intervals $(-\infty, a)$, $(a', b)$, $(b', c)$ and $(c', \infty)$, and negative along the intervals $(a, a'), (b, b')$ and $(c, c')$. We will make a further simplification of the problem. Let $x_1 < x_2$ be real numbers such that $f$ is non-negative along $[x_1, x_2]$. Let $x_0 \in \mathbb{R}$ with $f(x_0) < 0$. We introduce the change of variables

$$s = g(t) = \frac{1}{t - x_0}.$$

Let $\tilde{f}$ be the polynomial

$$\tilde{f}(s) = (s - g(a))(s - g(a'))(s - g(b))(s - g(b'))(s - g(c))(s - g(c')).$$

Then

$$\int_{x_1}^{x_2} \frac{S(t)dt}{\sqrt{|f(t)|}} = \frac{-1}{\sqrt{-f(x_0)}} \int_{1/(x_1 - x_0)}^{1/(x_2 - x_0)} \frac{s_1 + sS(x_0)}{\sqrt{-\tilde{f}(s)}} \operatorname{sgn}(s) ds.$$

The sign of $s$ does not change in the interval $[1/(x_2 - x_0), 1/(x_1 - x_0)]$, and $\tilde{f}$ is negative along $[1/(x_2 - x_0), 1/(x_1 - x_0)]$. Moreover, there are no roots of $\tilde{f}$ in the interval $(1/(x_2 - x_0), 1/(x_1 - x_0))$. We have thus reduced the problem of computing the integrals

$$\int_a^x \frac{S(t)dt}{\sqrt{|f(t)|}}, \quad \int_{x_0}^x \frac{S(t)dt}{\sqrt{|f(t)|}}$$

with $x < a$ in the first case, and $x_0 = a', b'$ or $c'$ and $f(t)$ positive along $(x_0, x)$ to the computation of integrals of the form

$$\int_a^x \frac{S(t)dt}{\sqrt{|f(t)|}}, \int_b^x \frac{S(t)dt}{\sqrt{|f(t)|}}, \text{ and } \int_c^x \frac{S(t)dt}{\sqrt{|f(t)|}},$$

where $x$ lies in $[a, a'], [b, b']$ or $[c, c']$ respectively.

## 4.2 Bost and Mestre's algorithm

In this section we solve some of the exercises in [6, Appendice A3] which lead to an elementary proof of the correctness of Bost and Mestre's algorithm. We describe the algorithm, we show why it works, and we extend it to the computation of the integrals

$$\int_a^x \frac{S(t)dt}{\sqrt{|f(t)|}}, \int_b^x \frac{S(t)dt}{\sqrt{|f(t)|}}, \text{ and } \int_c^x \frac{S(t)dt}{\sqrt{|f(t)|}},$$

where $x$ lies in $[a, a']$, $[b, b']$ or $[c, c']$ respectively.

Let $P, Q \in \mathbb{R}[X]$ be polynomials with real coefficients. We denote by $[P, Q]$ the polynomial $P'Q - PQ'$. The following properties follow easily from the definition:

- $[P, P] = 0$;
- $[P, Q] = -[Q, P]$;
- $[\lambda P, Q] = \lambda[P, Q] = [P, \lambda Q]$ for $\lambda \in \mathbb{R}$;
- $[P_1 + P_2, Q] = [P_1, Q] + [P_2, Q]$, for $P_1, P_2 \in \mathbb{R}[X]$.

The following lemmas are solutions to some of the exercises alluded to above. We will indicate in brackets the number of the corresponding exercise in [6, Appendice A3].

**Lemma 4.2.1** (*I*–1–a)**.** *Let $P \neq 0$ be a fixed polynomial of degree $n$ in $\mathbb{R}[X]$. Then $[P, Q] = 0$ if and only if $Q = \lambda P$ for some $\lambda \in \mathbb{R}$.*

*Proof.* The 'if' statement is a consequence of the properties previously mentioned. We use induction on the degree $n$ of $P$. If $n = 0, 1$ the result is clear. Let $Q \neq 0$ be a degree $m$ polynomial such that $[P, Q] = 0$. Let $p_n$ be the leading coefficient of $P$ and $q_m$ the leading coefficient of $Q$. Then $0 = [P, Q] = (m - n)p_n q_m X^{n+m} + \sum_{i=0}^{n+m-1} a_i X^i$, with $a_i \in \mathbb{R}$. Since $p_n q_m \neq 0$, then $m = n$. Since $[P, Q] = 0$, then $[P - p_n/q_m Q, Q] = 0$. But $P - p_n/q_m Q$ has degree $< n$. Then $P - p_n/q_m Q = 0$. Choosing $\lambda = p_n/q_m$ completes the proof. □

*Remark.* If $P$ has degree $\leq 1$, then the degree of $[P,Q]$ is at most the degree of $Q$, as $P'$ has degree $< 1$. If $P, Q$ both have degree $2$, then $[P,Q]$ has degree $2$ as well, for if $p_2, q_2$ are the leading coefficients of $P$ and $Q$, respectively, then $[P,Q] = (2-2)p_2q_2X^3 + a_2X^2 + a_1X + a_0$ for some real numbers $a_0, a_1, a_2$.

**Lemma 4.2.2** (*I*–2–a)**.** *Let $P, Q \in \mathbb{R}[X]$ be degree $2$ polynomials. If $P$ and $Q$ have a common root, that root is a double root of $[P,Q]$.*

*Proof.* Write $P = (X-a)f(X)$ and $Q(X) = (X-a)g(X)$ for some $a \in \mathbb{R}$ and some degree $1$ polynomials $f, g$. Then $P'(X) = (X-a)f'(X) + f(X)$ and $Q'(X) = (X-a)g'(X) + g(X)$. Then $[P,Q] = (X-a)^2f'(X)g(X) + (X-a)f(x)g(x) - (X-a)^2f(X)g'(X) - (X-a)f(X)g(X) = (X-a)^2h(X)$, for some polynomial $h(X)$. Then $a$ is a double root of $[P,Q]$. □

**Lemma 4.2.3** (*I*–2–b)**.** *Let $P(X) = (X-x)(X-x')$. Let $Q$ be a degree $2$ polynomial with $[P,Q] \neq 0$. The discriminant of $[P,Q]$ is $4Q(x)Q(x')$*

*Proof.* Write $Q(X) = a(X-y)(X-y')$. Then $P'(X) = 2X - (x+x')$ and $Q'(X) = a(2X - (y+y'))$. So

$$\begin{aligned}[P,Q](X) =& [2a(x+x'-y-y') - a(x+x'-y-y')]X^2 \\ &+ [2a(yy' - xx') + (a-a)(x+x')(y+y')]X \\ &+ a[xx'(y+y') - yy'(x+x')].\end{aligned}$$

Then, the discriminant of $[P,Q]$ is $4a^2(yy'-xx')^2 - 4a^2(x+x'-y-y')(xx'(y+y') - yy'(x+x'))$. Now, $Q(x) = a(x-y)(x-y')$ and $Q(x') = a(x'-y)(x'-y')$. Expanding the product $Q(x)Q(x')$ and comparing it to the expansion of the discriminant of $[P,Q]$ we see that the discriminant equals $4Q(x)Q(x') = 4a^2(x-y)(x-y')(x'-y)(x'-y')$. □

*Remark.* Note that since $P$ and $Q$ are defined over $\mathbb{R}$, $Q(\bar{x}) = \overline{Q(x)}$. Hence the discriminant of $[P,Q]$ is equal to $4\|Q(x)\|^2 \geq 0$ if $P$ has complex roots. In this case $[P,Q]$ has real roots.

**Lemma 4.2.4** (*I*–3)**.** *Let $P, Q \in \mathbb{R}[X]$ be two degree $2$ polynomials. Suppose that $P$ (resp. $Q$) has two different real roots $a < a'$ (resp. $b < b'$), and that $a' < b$. Then $[P, Q]$ has two different real roots $w, w'$ with $a < w < a' < b < w' < b'$.*

*Proof.* Note that the roots of $[P, Q], [\lambda P, Q]$ and $[P, \lambda Q]$ are the same. We can then suppose $P$ and $Q$ are monic and hence $P(X) = (X - a)(X - a')$ and $Q(X) = (X - b)(X - b')$. From Lemma 4.2.3, the discriminant of $[P, Q]$ equals

$$4Q(a)Q(a') = 4(a - b)(a - b')(a' - b)(a' - b').$$

Since $a < a' < b < b'$ all the factors in the product are nonzero, and they are all negative. Then, the discriminant of $[P, Q]$ is positive, and $[P, Q]$ has two different real roots $w < w'$.

Now, we compute the values of $[P, Q]$ at $a, a', b, b'$. From the definition of $[P, Q]$ we see $[P, Q](a) = (a - a')Q(a) = (a - a')(a - b)(a - b')$ and $[P, Q](a') = (a' - a)Q(a') = (a' - a)(a' - b)(a' - b')$. Then $[P, Q](a) < 0 < [P, Q](a')$ and hence, one of the roots of $[P, Q]$ must lie in the interval $(a, a')$. Recalling that $[P, Q] = -[Q, P]$ and using a similar argument, we see that $[P, Q](b) > 0 > [P, Q](b')$. Then the other root lies on the interval $(b, b')$ and $a < w < a' < b < w' < b'$. □

Let $P, Q, R \in \mathbb{R}[X]$ be degree $2$ polynomials. We denote by $\Delta(P, Q, R)$ the determinant of $P, Q, R$ with respect to the basis $1, X, X^2$. We will associate to a triple $(P, Q, R)$ of degree $2$ polynomials the triple $(U, V, W)$ defined by

$$U = [Q, R], \quad V = [R, P], \quad W = [P, Q].$$

We will say that $(U, V, W)$ is the *associated triple to* $(P, Q, R)$.

**Lemma 4.2.5** (*II*–$1$ and $2$)**.** *For every triple $(P, Q, R)$ of degree $2$ polynomials in $\mathbb{R}[X]$, we have, for every pair of real numbers $(x, z)$:*

$$P(x)U(z) + Q(x)V(z) + R(x)W(z) + (x - z)^2\Delta(P, Q, R) = 0,$$

*where $(U, V, W)$ is the associated triple to $(P, Q, R)$.*

*Proof.* Consider the matrix

$$A = \begin{pmatrix} P(z) & P'(z) & P(x) \\ Q(z) & Q'(z) & Q(x) \\ R(z) & R'(z) & R(x) \end{pmatrix}.$$

Note that the determinant of $A$ is $-P(x)U(z) - Q(x)V(z) - R(x)W(z)$. We will show that it also equals $(x-z)^2\Delta(P,Q,R)$. Expand $P(x), Q(x)$ and $R(x)$ in Taylor expansion around $z$,

$$\begin{aligned} P(x) &= P(z) + (z-x)P'(z) + (x-z)^2P''(z)/2, \\ Q(x) &= Q(z) + (z-x)Q'(z) + (x-z)^2Q''(z)/2, \\ R(x) &= R(z) + (z-x)R'(z) + (x-z)^2R''(z)/2. \end{aligned}$$

Using elementary column operations we can reduce the last column of $A$ to

$$\frac{1}{2}\begin{pmatrix} (x-z)^2P''(z) \\ (x-z)^2Q''(z) \\ (x-z)^2R''(z) \end{pmatrix}.$$

Write $P = p_0 + p_1X + p_2X^2$, $Q = q_0 + q_1X + q_2X^2$ and $R = r_0 + r_1X + r_2X^2$. Then $P' = 2p_2X + p_1$ and $P'' = 2p_2$, and similar expressions hold for $Q$ and $R$. Using elementary column operations we see that the determinant of $A$ is

$$(x-z)^2\begin{vmatrix} p_0 & p_1 & p_2 \\ q_0 & q_1 & q_2 \\ r_0 & r_1 & r_2 \end{vmatrix}$$

which equals $(x-z)^2\Delta(P,Q,R)$. Since this matrix has the same discriminant as $A$ we have proved the result. □

**Lemma 4.2.6** (*II*–3)**.** *Let $P, Q, R \in \mathbb{R}[X]$ be three degree $2$ polynomials, and let $(U,V,W)$ be the associated triple to $(P,Q,R)$. Then*

$$\Delta(U,V,W) = -2\Delta(P,Q,R)^2$$

*and*

$$[U, V] = -2R\Delta(P, Q, R),$$
$$[V, W] = -2P\Delta(P, Q, R),$$
$$[W, U] = -2Q\Delta(P, Q, R).$$

*Proof.* Let $A$ be the matrix

$$\begin{pmatrix} P(x) & P'(x) & P''(x) \\ Q(x) & Q'(x) & Q''(x) \\ R(x) & R'(x) & R''(x) \end{pmatrix}.$$

Note that as in the proof of the previous lemma, using elementary column operations we can see that the determinant of $A$ equals $2\Delta(P, Q, R)$. Now we compute the first and second derivatives of $U = [Q, R]$. We obtain

$$U' = (Q'R - QR')' = Q''R - QR'',$$

and

$$U'' = Q''R' - Q'R'',$$

since $Q''' = R''' = 0$ for they are degree 2 polynomials. We get similar expressions for $V', V'', W'$ and $W''$. We can now compute $[U, V]$ in terms of $P, Q, R$ using the definition of $[U, V]$ and the derivatives we have just computed. We obtain $[U, V] = -R\det(A) = -2R\Delta(P, Q, R)$. Repeating the same argument proves the corresponding result for $[V, W]$ and $[W, U]$. We now use the relation from Lemma 4.2.5 with $U, V, W$ instead of $P, Q, R$ to obtain

$$-2\Delta(P, Q, R)(P(x)U(z) + Q(x)V(z) + R(x)W(x)) + (x - z)^2\Delta(U, V, W) = 0,$$

for all $x, z \in \mathbb{R}$. Since $(P(x)U(z) + Q(x)V(z) + R(x)W(x) = -(x - z)^2\Delta(P, Q, R)$ for all $x, z$, setting $x = 1, z = 0$ we have

$$\Delta(U, V, W) = -2\Delta(P, Q, R)^2$$

□

Let $P, Q, R \in \mathbb{R}[X]$ be three degree $2$ monic polynomials, and let $(U, V, W)$ be the associated triple to $(P, Q, R)$. Assume that $P$ (resp. $Q$, resp. $R$) has two real roots $a, a'$ (resp. $b, b'$, resp. $c, c'$) such that $a < a' < b < b' < c < c'$. It follows from Lemma 4.2.4 that $U$ (resp. $V$, resp. $W$) has two different real roots that we denote by $u, u'$ (with $b < u < b' < c < u' < c'$) (resp. $v, v'$, with $a < v < a' < c < v' < c'$, resp. $w, w'$, with $a < w < a' < b < w' < b'$).

*Remark.* In this setting $\Delta(P, Q, R) \neq 0$. We have proved that

$$[U, V] = -2R\Delta(P, Q, R).$$

Recall that, since $U, V$ are nonzero, $[U, V] = 0$ if and only if $U = \lambda V$ for some nonzero real number $\lambda$. But then $U$ and $V$ would have the same roots. The location of the roots $u, u', v, v'$ given before shows that this is not the case. Note as well that the roots of $U$ are different to the roots of $V$, as if they had a common root, then this root would be a double root of $[U, V] = -2R\Delta(P, Q, R)$. But $R$ is assumed to have different roots. It follows that the six roots of $UVW$ are all different.

We now express explicitly the polynomials $U, V, W$ and the value $\Delta(P, Q, R)$ in terms of $a, a', b, b', c, c'$. Set

$$\begin{aligned} A_1 &= -a - a', & B_1 &= -b - b', & C_1 &= -c - c', \\ A_2 &= aa', & B_2 &= bb', & C_2 &= cc'. \end{aligned}$$

Then,

$$\begin{aligned} P(x) &= (x - a)(x - a') = x^2 + A_1 x + A_2, \\ Q(x) &= (x - b)(x - b') = x^2 + B_1 x + B_2, \\ R(x) &= (x - c)(x - c') = x^2 + C_1 x + C_2. \end{aligned}$$

The determinant $\Delta(P, Q, R)$ is then given by

$$\Delta(P, Q, R) = aa'(c + c' - b - b') + bb'(a + a' - c - c') + cc'(b + b' - a - a'),$$

and

$$U(x) = [Q,R](x) = (b+b'-c-c')x^2 + 2(cc'-bb')x + bb'(c+c') - cc'(b+b'),$$
$$V(x) = [R,P](x) = (c+c'-a-a')x^2 + 2(aa'-cc')x + cc'(a+a') - aa'(c+c'),$$
$$W(x) = [P,Q](x) = (a+a'-b-b')x^2 + 2(bb'-aa')x + aa'(b+b') - bb'(a+a').$$

Lemma 4.2.3 states that the discriminant of $W$ equals

$$4Q(a)Q(a') = 4(a-b)(a-b')(a'-b)(a'-b').$$

Similarly, the discriminant of $U$ and $V$ are given respectively by

$$4(c-b)(c-b')(c'-b)(c'-b') \quad \text{and} \quad 4(c-a)(c-a')(c'-a)(c'-a').$$

We then have the following identities

$$u = \frac{bb'-cc'-\sqrt{(c-b)(c-b')(c'-b)(c'-b')}}{b+b'-c-c'},$$
$$u' = \frac{bb'-cc'+\sqrt{(c-b)(c-b')(c'-b)(c'-b')}}{b+b'-c-c'},$$
$$v = \frac{cc'-aa'-\sqrt{(c-a)(c-a')(c'-a)(c'-a')}}{c+c'-a-a'},$$
$$v' = \frac{cc'-aa'+\sqrt{(c-a)(c-a')(c'-a)(c'-a')}}{c+c'-a-a'},$$
$$w = \frac{aa'-bb'-\sqrt{(a-b)(a-b')(a'-b)(a'-b')}}{(a+a'-b-b')},$$
$$w' = \frac{aa'-bb'+\sqrt{(a-b)(a-b')(a'-b)(a'-b')}}{(a+a'-b-b')}.$$

**Lemma 4.2.7** (*III*–3)**.** *The roots $u, u'$ of $U$, $v, v'$ of $V$, and $w, w'$ of $W$ satisfy the following inequalities*

$$a < v < w < a' < b < w' < u < b' < c < u' < v' < c'.$$

*Proof.* The discriminant of $[(X-v)(X-v'),(X-w)(X-w')]$ is positive, as $[V,W] = -2P\Delta(P,Q,R)$ and $P$ has two different real roots. From Lemma 4.2.3 we see that

$$(v+v'-w-w')^2(a-a')^2 = 4(v-w)(v-w')(v'-w)(v'-w'),$$

since the expression on the left equals the discriminant of $[(X-v)(X-v'),(X-w)(X-w')]$, for $v+v'-w-w'$ is the leading coefficient of $[(X-v)(X-v'),(X-w)(X-w')]$, and $a, a'$ are its roots. Note that $v-w'<0$ and that $v'-w$ and $v'-w'$ are both positive, as $a<v, w<a'<b<w'<b'<c<v'<c$. Then we must have $v-w<0$, or equivalently, $v<w$. Repeating the argument with $[U,V]$ and $[W,U]$ completes the proof. □

Put $F_1(x,z)=P(x)U(z)+Q(x)V(z)$, $F_2(x,z)=Q(x)V(z)+R(x)W(z)$ and $F_3(x,z)=P(x)U(z)+R(x)W(z)$.

**Lemma 4.2.8** (*III–4*). *As polynomials in $z$, $F_1$, $F_2$, $F_3$ are precisely of degree $2$ for $x\in[a,a']$, $x\in[b,b']$, and $x\in[c,c']$ respectively. Moreover, in the same intervals for $x$, $F_1, F_2$ and $F_3$ have positive discriminant as polynomials in $z$.*

*Proof.* Write

$$F_1(x,z)=\phi_0(x)z^2+\phi_1(x)z+\phi_2(x),$$

where $\phi_0,\phi_1,\phi_2$ are polynomials in $x$ of degree $\leq 2$. We will compute the sign of $\phi_0(a')$ and $\phi_0(b)$. Note that $F(a',z)=Q(a)V(z)$. Recall that the leading coefficient of $V$ is $c+c'-a-a'$. Now, $Q(a')>0$ since $Q$ is monic and the roots of $Q$ are both $>a'$. Then, the leading coefficient of $F(a',z)$ as a polynomial in $z$, $\phi_0(a')$, is positive. Similarly, looking at $F(b,z)$ we get $\phi_0(b)<0$. Then $\phi_0$ has a root $x_0$ with $a'<x_0<b$.

Using the identity from Lemma 4.2.5 we see that $F(x,z)=-R(x)W(z)-(x-z)^2\Delta(P,Q,R)$. Note that $0=F(a,v)=-R(a)W(v)-(a-v)^2\Delta(P,Q,R)$. Since $R(a)>0$ and $W(v)<0$ we have $-R(a)W(v)>0$. Then $\Delta(P,Q,R)>0$. Looking now at $F(c',z)=-(c'-z)^2\Delta(P,Q,R)$, we see that $\phi_0(c')<0$. Since the leading coefficient of $W$ is $a+a'-b-b'<0$ and $R(x)>0$ for all $x>c'$, we see that for large enough $x$, $-R(x)W(z)-(x-z)^2\Delta(P,Q,R)$ has a positive leading coefficient as a polynomial in $z$. Then for $x>c'$ large enough $\phi_0(x)>0$ and thus $\phi_0$ has a root $x_1>c'$. In summary, the degree $2$ polynomial $\phi_0$ takes positive values for $x\in[a,a']$ and

then $F_1$ is precisely of degree $2$ as claimed. The same argument adjusted accordingly shows the corresponding statements for $F_2$ and $F_3$.

Now, the discriminant of $F_1$ equals $\phi_1^2 - 4\phi_0\phi_2$. It is a polynomial of degree at most $4$. If $\phi_0(x) \neq 0$, then the discriminant vanishes if and only if $F_1$ has a double root $\delta$ as a polynomial in $z$. Lemma 4.2.5 implies that $c, c'$ are roots of $\phi_1^2 - 4\phi_0\phi_2$. Dividing $\phi_1^2 - 4\phi_0\phi_2$ by $R(x)$ we get $4g_1g_2$ where $g_1 = x(c(b+b'-a-a') + aa' - bb') + c(aa' - bb') + bb'(a+a') - aa'(b+b')$ and $g_2 = x(c'(b+b'-a-a') + aa' - bb') + c'(aa' - bb') + bb'(a+a') - aa'(b+b')$. We can see that none of the roots of $\phi_1^2 - 4\phi_0\phi_2$ lie in the interval $[a, a']$, as if $x_0$ is a root of the discriminant and $\delta \in \mathbb{R}$ is such that

$$P(x_0)U(z) + Q(x_0)V(z) = \phi_0(x_0)(z-\delta)^2,$$

for all $z \in \mathbb{R}$, then $P(x_0)$ and $Q(x_0)$ must have the same sign, for $U$ is negative and $V$ is positive along $(-\infty, v)$. However, $P(z)$ and $Q(z)$ have opposite signs along $(a, a')$. Moreover, since $F_1(a) = Q(a)W(z)$ and $Q(a) \neq 0$, $F_1(a)$ has two different roots, and then $\phi_1^2 - 4\phi_0\phi_2$ is positive at $x = a$. Hence it is positive along all of $[a, a']$. The same analysis adjusted accordingly proves the statements for $F_2$ and $F_3$. □

It follows from the Implicit Function Theorem that there are two different functions $z_1$ and $z_2$ defined on $[a, a'] \cup [b, b'] \cup [c, c']$ to $\mathbb{R}$, continuous on $[a, a'] \cup [b, b'] \cup [c, c']$, $C^\infty$ on $(a, a') \cup (b, b') \cup (c, c')$, with $z_1(x) < z_2(x)$ and such that

$$F_1(x, z_1(x)) = F_1(x, z_2(x)) = 0,$$

for all $x \in [a, a']$,

$$F_2(x, z_1(x)) = F_2(x, z_2(x)) = 0,$$

for all $x \in [b, b']$, and

$$F_3(x, z_1(x)) = F_3(x, z_2(x)) = 0,$$

for all $x \in [c, c']$. Define functions $y_1$, $y_2$ on $(a, a') \cup (b, b') \cup (c, c')$ by

$$y_i(x) = \begin{cases} \frac{P(x)U(z_i(x))(x-z_i(x))}{\sqrt{|P(x)Q(x)R(x)|}}, & x \in (a, a') \\ \frac{Q(x)V(z_i(x))(x-z_i(x))}{\sqrt{|P(x)Q(x)R(x)|}}, & x \in (b, b') \\ \frac{R(x)W(z_i(x))(x-z_i(x))}{\sqrt{|P(x)Q(x)R(x)|}}, & x \in (c, c'). \end{cases}$$

**Lemma 4.2.9** (*III*–6–a)**.** *For* $x \in (a, a') \cup (b, b') \cup (c, c')$ *and for* $i = 1, 2$

$$y_i^2 = \frac{|U(z_i(x))V(z_i(x))W(z_i(x))|}{|\Delta(P, Q, R)|}.$$

*Proof.* We prove the identity for $x \in (a, a')$. The proof for the other intervals is similar. For $i = 1, 2$

$$y_i^2(x) = \frac{P^2(x)U^2(z_i(x))(x - z_i(x))^2}{|P(x)Q(x)R(x)|},$$

From Lemma 4.2.5 and the definition of $z_i(x)$ we see that

$$0 = P(x)U(z_i(x)) + Q(x)V(z_i(x)) = R(x)W(z_i(x)) + (x - z_i(x))^2\Delta(P, Q, R).$$

Then

$$P(x)U(z_i(x)) = -Q(x)V(z_i(x))$$

and

$$(x - z_i(x))^2 = -R(x)W(z_i(x))/\Delta(P, Q, R).$$

We then have

$$\begin{aligned} y_i^2(x) &= \frac{P(x)Q(x)R(x)}{|P(x)Q(x)R(x)|} \cdot \frac{U(z_i(x))V(z_i(x))W(z_i(x))}{\Delta(P, Q, R)} \\ &= \frac{|U(z_i(x))V(z_i(x))W(z_i(x))|}{|\Delta(P, Q, R)|}. \end{aligned}$$

□

We now study the functions $z_1, z_2, y_1, y_2$ along $(a, a'), (b, b')$ and $(c, c')$.

**Lemma 4.2.10** (*III*–3–a)**.** *We have* $z_1(a) = v = z_1(a')$, $z_2(a) = v' = z_2(a')$, $z_1(b) = w = z_1(b')$, $z_2(b) = w' = z_2(b')$, $z_1(c) = u = z_1(c')$ *and* $z_2(c) = u' = z_2(c')$. *Moreover,*

$$z_1([a,a']) = [v,w],\ z_2([a,a']) \subset (u',v'],\ z_1([b,b']) \subset (v,w],$$
$$z_2([b,b']) = [w',u],\ z_1([c,c']) \subset (w',u],\ z_2([c,c']) = [u',v'],$$

*and* $z_1(x) = w$ *for* $x \in (a,a')$ *if and only if* $x = w$, $z_2(x) = u$ *for* $x \in (b,b')$ *if only if* $x = u$, $z_2(x) = v'$ *for* $x \in (c,c')$ *if and only if* $x = v'$. *We also have*

$$y_1(x) \begin{cases} \leq 0 & a \leq x \leq w \\ \geq 0 & w \leq x \leq a', \end{cases} \qquad y_2(x) \leq 0, \quad x \in [a,a']$$

$$y_2(x) \begin{cases} \leq 0 & b \leq x \leq u \\ \geq 0 & u \leq x \leq b', \end{cases} \qquad y_1(x) \geq 0, \quad x \in [b,b']$$

$$y_2(x) \begin{cases} \leq 0 & c \leq x \leq v' \\ \geq 0 & v' \leq x \leq c', \end{cases} \qquad y_1(x) \geq 0, \quad x \in [c,c']$$

*Proof.* Note that $0 = F_1(a, z_i(a)) = Q(a)V(z_i(a))$. Since $Q(a) \neq 0$ it follows that $V(z_i(a)) = 0$, that is $z_1(a) = v$, $z_2(a) = v'$. Similarly, $z_1(a') = v$, $z_2(a') = v'$. Since $a < v < a'$, there is a point $x \in (a,a')$ such that $z_1(x) = x$. Then $F(x, z_1(x)) = 0 = R(x)W(z_1(x))$, but $R(x) \neq 0$. Thus $z_1(x)$ must be equal to $w$ and there is only a point in $(a,a')$ satisfying $z_1(x) = x$. Similarly, if $z_1(x) = w$ we have that $x = z_1(x) = w$ for $F(x, z_1(x)) = (x - z_1(x))^2 \Delta(P,Q,R)$. In particular, $z_1(x)$ attains its maximum at $w$. At this point we have that $y_1(x) = 0$. We will now show that $z_1(x) \geq v$ for $x \in (a,a')$. Since $F(x, z_1(x)) = P(x)U(z_1(x)) + Q(x)V(z_1(x)) = 0$, and $P$ is negative and $Q$ is positive along $(a,a')$, then $U(z_1(x))$ and $V(z_1(x))$ cannot have opposite signs. But for $z < v$ we have $V(z) > 0$ and $U(z) < 0$. The same argument shows that $z_2(x) \leq v'$.

Now, on $(a,a')$ we have $P(x) < 0$, and since $z_1(x) \in [v,w]$, we have that $U(z_1(x)) < 0$. Then $y_1(x)$ is negative along $(a,w)$ and positive along $(w,a')$. Note now that there is no point $x \in (a,a')$ with $z_2(x) = u'$, for if $z_2(x) = u'$ then $F(x, z_2(x)) =$

$Q(x)V(z_2(x)) = 0$, but since $V(u') \neq 0$ we would have $Q(x) = 0$. But the roots of $x$ are $> a'$. Then $z_2(x) > u'$ for all $x \in [a, a']$. In particular, $x - z_2(x) < 0$ and $U(z_2(x)) < 0$ for all $x \in (a, a')$. Then $y_2(x) < 0$ for all $x \in (a, a')$.

The corresponding statements for $[b, b']$ and $[c, c']$ are proved in a similar way.

□

We have not been able to prove the following result (Exercise *III*–6–b). Nevertheless, when we have needed it, we have proved the identity in specific cases using symbolic computations with Mathematica [52].

**Lemma 4.2.11** (*III*–6–b)**.** *Let $S(X) \in \mathbb{R}[X]$ be a polynomial of degree at most $1$. Then, for all $x \in [a, a'] \cup [b, b'] \cup [c, c']$*

$$S(z_1(x))\frac{z_1'(x)}{y_1(x)} + S(z_2(x))\frac{z_2'(x)}{y_2(x)} = -\frac{S(x)}{\sqrt{|P(x)Q(x)R(x)|}}.$$

Let $x_0 \in [a, a']$. The previous Lemma implies that

$$\int_a^{x_0} \frac{S(x)dx}{\sqrt{|P(x)Q(x)R(x)|}} = -\int_a^{x_0} \frac{S(z_1(x))z_1'(x)dx}{y_1(x)} - \int_a^{x_0} \frac{S(z_2(x))z_2'(x)dx}{y_2(x)}.$$

Write $\Delta = \Delta(P, Q, R)$. Since $y_2(x) < 0$ for all $x \in (a, a')$ we can use the substitution formula on the second integral to obtain

$$\int_a^{x_0} \frac{S(z_2(x))z_2'(x)dx}{y_2(x)} = \sqrt{|\Delta|}\int_{z_2(x_0)}^{v'} \frac{S(x)dx}{\sqrt{|U(x)V(x)W(x)|}},$$

as $\Delta y_2(x)^2 = |U(z_2(x))V(z_2(x))W(z_2(x))|$. Now $y_1(w) = 0$, so we need to take care of that when using the substitution formula for the integral

$$\int_a^{x_0} \frac{S(z_1(x))z_1'(x)dx}{y_1(x)}.$$

Note that

$$\int_a^{x_0} \frac{S(z_1(x))z_1'(x)dx}{y_1(x)} = \int_a^{w} \frac{S(z_1(x))z_1'(x)dx}{y_1(x)} + \int_w^{x_0} \frac{S(z_1(x))z_1'(x)dx}{y_1(x)}.$$

Recall that $y_1(x)$ is negative along $(a, w)$ and positive along $(w, a')$. Recall as well that $y_1(x)^2 = |U(z_1(x))V(z_1(x))W(z_1(x))|$. Then,

$$\int_a^{w} \frac{S(z_1(x))z_1'(x)dx}{y_1(x)} = -\sqrt{|\Delta|}\int_v^{w} \frac{S(x)dx}{\sqrt{|U(x)V(x)W(x)|}},$$

and

$$\int_w^{x_0} \frac{S(z_1(x))z_1'(x)dx}{y_1(x)} = (-1)^{\varepsilon}\sqrt{|\Delta|}\int_w^{z_1(x_0)} \frac{S(x)dx}{\sqrt{|U(x)V(x)W(x)|}},$$

where we choose $\varepsilon = 0, 1$ according to the sign of $y_1$ along the interval of integration. In the same way we can compute identities for $x \in [b, b'] \cup [c, c']$. It is now easy to check that for $x_0 \in [a, w]$

$$\begin{aligned}\int_a^{x_0} \frac{S(x)dx}{\sqrt{|(PQR)(x)|}} &= \sqrt{\Delta}\left(\int_v^{z_1^a(x_0)} \frac{S(x)dx}{\sqrt{|(UVW)(x)|}} - \int_{z_2^a(x_0)}^{v'} \frac{S(x)dx}{\sqrt{|(UVW)(x)|}}\right)\\ &= \sqrt{\Delta}\left(\int_v^{z_1^a(x_0)} \frac{S(x)dx}{\sqrt{|(UVW)(x)|}} - \int_{u'}^{v'} \frac{S(x)dx}{\sqrt{|(UVW)(x)|}}\right.\\ &\qquad \left. + \int_{u'}^{z_2^a(x_0)} \frac{S(x)dx}{\sqrt{|(UVW)(x)|}}\right).\end{aligned} \tag{4.2.1}$$

and for $x_0 \in [w, a']$,

$$\begin{aligned}\int_a^{x_0} \frac{S(x)dx}{\sqrt{|(PQR)(x)|}} &= \sqrt{\Delta}\left(\int_v^{w} \frac{S(x)dx}{\sqrt{|(UVW)(x)|}} + \int_{z_1^a(x_0)}^{w} \frac{S(x)dx}{\sqrt{|(UVW)(x)|}}\right.\\ &\qquad \left. - \int_{z_2^a(x_0)}^{v'} \frac{S(x)dx}{\sqrt{|(UVW)(x)|}}\right)\\ &= \sqrt{\Delta}\left(2\int_v^{w} \frac{S(x)dx}{\sqrt{|(UVW)(x)|}} - \int_v^{z_1^a(x_0)} \frac{S(x)dx}{\sqrt{|(UVW)(x)|}}\right.\\ &\qquad \left. - \int_{u'}^{v'} \frac{S(x)dx}{\sqrt{|(UVW)(x)|}} + \int_{u'}^{z_2^a(x_0)} \frac{S(x)dx}{\sqrt{|(UVW)(x)|}}\right).\end{aligned} \tag{4.2.2}$$

For $x_0 \in [b, u]$

$$\begin{aligned}\int_b^{x_0} \frac{S(x)dx}{\sqrt{|(PQR)(x)|}} &= \sqrt{\Delta}\left(\int_{w'}^{z_2^b(x_0)} \frac{S(x)dx}{\sqrt{|(UVW)(x)|}} + \int_{z_1^b(x_0)}^{w} \frac{S(x)dx}{\sqrt{|(UVW)(x)|}}\right)\\ &= \sqrt{\Delta}\left(\int_{w'}^{z_2^b(x_0)} \frac{S(x)dx}{\sqrt{|(UVW)(x)|}} + \int_v^{w} \frac{S(x)dx}{\sqrt{|(UVW)(x)|}}\right.\\ &\qquad \left. - \int_v^{z_1^b(x_0)} \frac{S(x)dx}{\sqrt{|(UVW)(x)|}}\right),\end{aligned} \tag{4.2.3}$$

and for $x_0 \in [u, b']$

$$\begin{aligned}\int_b^{x_0} \frac{S(x)dx}{\sqrt{|(PQR)(x)|}} &= \sqrt{\Delta}\left(\int_{w'}^{u} \frac{S(x)dx}{\sqrt{|(UVW)(x)|}} + \int_{z_2^b(x_0)}^{u} \frac{S(x)dx}{\sqrt{|(UVW)(x)|}} \right.\\ &\qquad \left. + \int_{z_1^b(x_0)}^{w} \frac{S(x)dx}{\sqrt{|(UVW)(x)|}}\right)\\ &= \sqrt{\Delta}\left(2\int_{w'}^{u} \frac{S(x)dx}{\sqrt{|(UVW)(x)|}} - \int_{w'}^{z_2^b(x_0)} \frac{S(x)dx}{\sqrt{|(UVW)(x)|}} \right.\\ &\qquad \left. + \int_{v}^{w} \frac{S(x)dx}{\sqrt{|(UVW)(x)|}} - \int_{v}^{z_1^b(x_0)} \frac{S(x)dx}{\sqrt{|(UVW)(x)|}}\right).\end{aligned} \tag{4.2.4}$$

For $x_0 \in [c, v']$

$$\begin{aligned}\int_c^{x_0} \frac{S(x)dx}{\sqrt{|(PQR)(x)|}} &= \sqrt{\Delta}\left(\int_{u'}^{z_2^c(x_0)} \frac{S(x)dx}{\sqrt{|(UVW)(x)|}} + \int_{z_1^c(x_0)}^{u} \frac{S(x)dx}{\sqrt{|(UVW)(x)|}}\right)\\ &= \sqrt{\Delta}\left(\int_{u'}^{z_2^c(x_0)} \frac{S(x)dx}{\sqrt{|(UVW)(x)|}} + \int_{w'}^{u} \frac{S(x)dx}{\sqrt{|(UVW)(x)|}} \right.\\ &\qquad \left. - \int_{w'}^{z_1^c(x_0)} \frac{S(x)dx}{\sqrt{|(UVW)(x)|}}\right),\end{aligned} \tag{4.2.5}$$

and for $x_0 \in [v', c]$

$$\begin{aligned}\int_c^{x_0} \frac{S(x)dx}{\sqrt{|(PQR)(x)|}} &= \sqrt{\Delta}\left(\int_{u'}^{v'} \frac{S(x)dx}{\sqrt{|(UVW)(x)|}} + \int_{z_2^c(x_0)}^{v'} \frac{S(x)dx}{\sqrt{|(UVW)(x)|}} \right.\\ &\qquad \left. + \int_{z_2^c(x_0)}^{v'} \frac{S(x)dx}{\sqrt{|(UVW)(x)|}}\right).\\ &= \sqrt{\Delta}\left(2\int_{u'}^{v'} \frac{S(x)dx}{\sqrt{|(UVW)(x)|}} - \int_{u'}^{z_2^c(x_0)} \frac{S(x)dx}{\sqrt{|(UVW)(x)|}} \right.\\ &\qquad \left. + \int_{w'}^{u} \frac{S(x)dx}{\sqrt{|(UVW)(x)|}} - \int_{w'}^{z_1^c(x_0)} \frac{S(x)dx}{\sqrt{|(UVW)(x)|}}\right).\end{aligned} \tag{4.2.6}$$

The final expressions in the previous identities are formed by either integrals along

intervals whose endpoints are two consecutive roots of $UVW$, or integrals

$$\int_{x_1}^{x} \frac{S(x)dx}{\sqrt{|(UVW)(x)|}},$$

where $x_1$ is a root of $UVW$. Those identities will help us to compute the integrals to high precision recursively and more easily. We note that when $x = a', b'$ and $c'$ we have respectively

$$\int_a^{a'} \frac{S(t)dt}{\sqrt{|f(t)|}} = 2\sqrt{|\Delta|} \int_v^w \frac{S(t)dt}{\sqrt{|\tilde{f}(t)|}}, \tag{4.2.7}$$

$$\int_b^{b'} \frac{S(t)dt}{\sqrt{|f(t)|}} = 2\sqrt{|\Delta|} \int_{w'}^u \frac{S(t)dt}{\sqrt{|\tilde{f}(t)|}}, \tag{4.2.8}$$

$$\int_c^{c'} \frac{S(t)dt}{\sqrt{|f(t)|}} = 2\sqrt{|\Delta|} \int_{u'}^v \frac{S(t)dt}{\sqrt{|\tilde{f}(t)|}}. \tag{4.2.9}$$

(Exercise *III*–7.)

We are now ready to explain the idea behind the algorithm for the computation of

$$\int_a^{a'} \frac{S(t)dt}{\sqrt{|f(t)|}} \tag{4.2.10}$$

We follow Section 3 of [6]. The integrals of the form (4.2.10) can be thought as integrals of the holomorphic differentials $S(x)dx/y$ of the hyperelliptic curve given by the equation $y^2 = f(x)$. Now, let $f \in \mathbb{R}[x]$ be a degree $6$ monic polynomial with real roots only. Denote the roots of $f$ by $a < a' < b < b' < c < c'$. Let $P = (x-a)(x-a')$, $Q = (x-b)(x-b')$ and $R = (x-c)(x-c')$. Let $(U, V, W)$ be the associated triple to $(P, Q, R)$. We have shown that the polynomial $\tilde{f} = U(x)V(x)W(x)$ has six different roots $v < w < w' < u < u' < v'$, where $u, u'$ are the roots of $U$, $v, v'$ the roots of $V$, and $w, w'$ the roots of $W$. Consider the genus $2$ hyperelliptic curves $\mathcal{C}$ and $\mathcal{C}'$ given by the equations $y^2 = f(x)$ and $\Delta y'^2 = \tilde{f}(x')$, where $\Delta = \Delta(P, Q, R)$. We take the following definition from Chapter 2, Section 5 of [26].

**Definition.** A *correspondence* of degree $d$ between two curves $C$ and $C'$ defined over $\mathbb{C}$ associates to every point $p \in C$ a divisor $T(p)$ of degree $d$ on $C'$, varying holomor-

phically with $p$. It can be given by its *curve of correspondence*

$$D = \{(p, q) : q \in T(p)\} \subset C \times C';$$

conversely, given any curve $D \subset C \times C'$, we can define an associated correspondence by

$$T(p) = i_p^*(D) \in \mathrm{Div}(C'),$$

where $i_p : C' \to C \times C'$ is defined by $q \mapsto (p, q)$.

There are three correspondences of degree $2$ between $\mathcal{C}$ and $\mathcal{C}'$ defined by the following curves: let $Z_1$, $Z_2$, $Z_3$ be the curves over $\mathcal{C} \times \mathcal{C}'$ given by the equations

$$Z_1 : \begin{cases} P(x)U(x') + Q(x)V(x') = 0, \\ yy' = P(x)U(x')(x - x'), \end{cases}$$

$$Z_2 : \begin{cases} Q(x)V(x') + R(x)W(x') = 0, \\ yy' = Q(x)V(x')(x - x'), \end{cases}$$

$$Z_3 : \begin{cases} P(x)U(x') + R(x)W(x') = 0, \\ yy' = W(x)R(x')(x - x'), \end{cases}$$

What we have done before when solving the exercises is computing explicitly for $(x, y) \in \mathcal{C}$ with $x \in [a, a']$ the corresponding degree $2$ divisor $(z_1(x), iy_1(x)) + (z_2(x), iy_2(x))$ on $\mathcal{C}'$ under the correspondence defined by $Z_1$, and we have done accordingly for points $(x, y) \in \mathcal{C}$ with $x \in [b, b']$ and $[c, c']$ and the curves $Z_2$ and $Z_3$. These correspondences define linear maps $\delta_{Z_i} : \Omega^1(\mathcal{C}') \to \Omega^1(\mathcal{C})$ as follows: let $p_{1,i}$, $p_{2,i}$ be the restrictions to $Z_i$ of the projections of $\mathcal{C} \times \mathcal{C}'$ to $\mathcal{C}$ and $\mathcal{C}'$; the map $p_{2,i}$ defines an "inverse image" $p_{2,i}^* : \Omega_1(\mathcal{C}') \to \Omega^1(Z_i)$ , and the map $p_{1,i}$ defines a "trace" map $p_{1,i*} : \Omega^1(Z_i) \to \Omega_1(\mathcal{C})$. We define $\delta_{Z_i} = p_{1,i*} \circ p_{2,i}^*$. Lemma 4.2.11 implies that

$$\delta_{Z_i}\left(S(x')\frac{dx'}{y'}\right) = S(x)\frac{dx}{y}.$$

We did a careful study of the action of the correspondences $Z_i$ on the cycles of $C$ associated to the intervals $(a, a'), (b, b'), (c, c')$ when we compared the integrals along

$\mathcal{C}$ to the integrals along $\mathcal{C}'$ just after Lemma 4.2.11. In particular, when proving (4.2.7) what we were doing was showing that the cycle associated to $(a, a')$ (resp. $(b, b'), (c, c')$) corresponds to two cycles: a contractible cycle and twice the cycle associated to $(v, w)$ (resp. $(w', u), (u', v')$).

We will now see that repeating the construction with $U, V$ and $W$ instead of $P, Q, R$ will lead to the value of the desired integrals to high precision. Let $a_1 < a'_1 < b_1 < b'_1 < c_1 < c'_1$ be six real numbers. Set

$$P_1(X) = (X - a_1)(X - a'_1), Q_1(X) = (X - b_1)(X - b'_1), R_1(X) = (X - c_1)(X - c'_1).$$

If $(U_1, V_1, W_1)$ is the associated triple to $(P_1, Q_1, R_1)$, we have previously seen that the six roots of $U_1V_1W_1$ are all real. Order them in increasing order $a_2 < a'_2 < b_2 < b'_2 < c_2 < c'_2$ and set $P_2(X) = (X - a_2)(X - a'_2), Q_2(X) = (X - b_2)(X - b'_2), R_2(X) = (X - c_2)(X - c'_2)$.

We define in this way six sequences of polynomials $P_n, Q_n, R_n, U_n, V_n, W_n$ and six sequences of real numbers $(a_n), (a'_n)(b_n), (b'_n), (c_n), (c'_n)$ recurrently defined for $n \geq 2$ by the relations

$$P_n(X) = (X - a_n)(X - a'_n), Q_n(X) = (X - b_n)(X - b'_n), R_n(X) = (X - c_n)(X - c'_n),$$

where $a_n < a'_n < b_n < b'_n < c_n < c'_n$ are the roots of $U_{n-1}V_{n-1}W_{n-1}$, and $(U_{n-1}, V_{n-1}, W_{n-1})$ is the associated triple to $P_{n-1}Q_{n-1}R_{n-1}$.

**Lemma 4.2.12** (*IV*–1)**.** *The sequences* $(a_n)$ *and* $(a'_n)$ *(resp.* $(b_n)$ *and* $(b'_n)$*, resp.* $(c_n)$ *and* $(c'_n)$*) have a common limit. Moreover, there is a constant* $M$ *such that for all* $n \geq 1$*,*

$$a'_{n+1} - a_{n+1} < M(a'_n - a_n)^2,$$
$$b'_{n+1} - b_{n+1} < M(b'_n - b_n)^2,$$
$$c'_{n+1} - c_{n+1} < M(c'_n - c_n)^2.$$

*Proof.* It is clear from Lemma 4.2.7 that we have

$$a_1 < a_n < a_{n+1} < a'_{n+1} < a'_n < a_1,$$

and that similar relations hold for $(b_n), (b'_n), (c_n)$ and $(c'_n)$. This shows that the sequences converge respectively to $a, a', b, b', c, c'$, say, and that the limits satisfy

$$a \leq a' < b \leq b' < c \leq c'.$$

We will prove that $a = a'$. The proof that $b = b'$ and $c = c'$ follows the same lines. Recall that the discriminant of $W_n = [P_n, Q_n]$ is given by $4Q_n(a_n)Q_n(a_n) = 4(b_n - a_n)(b'_n - a_n)(b_n - a'_n)(b'_n - a'_n)$. Now, since the roots of $W_n$ are $a'_{n+1}$ and $b_{n+1}$ (Lemma 4.2.7), the discriminant also equals $(a_n + a'_n - b_n - b'_n)^2(a'_{n+1} - b_{n+1})^2$, for $a_n + a'_n - b_n - b'_n$ is the leading coefficient of $W_n$. Taking limits we see that

$$(a + a' - b - b')^2(a' - b)^2 = 4(b - a)(b' - a)(b - a')(b' - a').$$

Note that

$$b' - a \geq b - a > 0 \quad \text{and} \quad b' - a' \geq b - a' > 0.$$

Then

$$(b' - a)(b' - a')(b - a)(b - a') \geq (b - a)^2(b - a')^2, \tag{4.2.11}$$

and if $a < a'$ we get a strict inequality. Similarly,

$$(b' - a)(b' - a')(b - a)(b - a') \geq (b' - a')^2(b - a')^2, \tag{4.2.12}$$

where again, $a \neq a'$ implies a strict inequality. Finally, we also have

$$(b' - a)(b' - a')(b - a)(b - a') \geq (b' - a')(b - a)(b - a')^2. \tag{4.2.13}$$

If $a < a'$, adding (4.2.11) plus (4.2.12) plus twice (4.2.13) we then get that

$$4(b' - a)(b' - a')(b - a)(b - a') > (b - a')^2(b' - a' + b - a)^2,$$

which is a contradiction. Therefore $a = a'$. We now prove the existence of the constant $M$. Using the identity $[V_n, W_n] = -P_n\Delta(P_n, Q_n, R_n)$, and the corresponding identities

for $[U_n, V_n]$ and $[W_n, U_n]$, computing discriminants we see that

$$a'_{n+1} - a_{n+1} = \frac{(c'_{n+1} - b_{n+1} - a'_{n+1} + a_{n+1})^2 (a'_n - a_n)^2}{4(b_{n+1} - a_{n+1})(c'_{n+1} - a'_{n+1})(c'_{n+1} - b_{n+1})},$$
$$b'_{n+1} - b_{n+1} = \frac{(c_{n+1} - a'_{n+1} + b'_{n+1} - b_{n+1})^2 (b'_n - b_n)^2}{4(b'_{n+1} - a'_{n+1})(c_{n+1} - a'_{n+1})(c'_{n+1} - b_{n+1})},$$
$$c'_{n+1} - c_{n+1} = \frac{(b'_{n+1} - a_{n+1} - c'_{n+1} + c_{n+1})^2 (c'_n - c_n)^2}{4(b_{n+1} - a_{n+1})(c'_{n+1} - a'_{n+1})(c'_{n+1} - b_{n+1})},$$

and then

$$a'_{n+1} - a_{n+1} < \frac{(c'_1 - b_1 + a'_1 - a_1)^2 (a'_n - a_n)^2}{4(b_1 - a'_1)(c_1 - a'_1)(c_1 - b'_1)},$$
$$b'_{n+1} - b_{n+1} < \frac{(c'_1 - a_1 + b'_1 - b_1)^2 (b'_n - b_n)^2}{4(b_1 - a'_1)(c_1 - a'_1)(c_1 - b'_1)},$$
$$c'_{n+1} - c_{n+1} < \frac{(b'_1 - a_1 + c'_1 - c_1)^2 (c'_n - c_n)^2}{4(b_1 - a'_1)(c_1 - a'_1)(c_1 - b'_1)}.$$

If we set

$$M = \frac{(c'_1 - a_1 + \max\{a'_1 - a_1, b'_1 - b_1, c'_1 - c_1\})^2}{4(b_1 - a'_1)(c_1 - a'_1)(c_1 - b'_1)},$$

we arrive to the required inequalities. □

*Remark.* The previous lemma states that the convergence of the sequences $a_n$, $b_n$, $c_n$ is quadratic. Note that if $a'_n - a_n \leq 10^{-k}$, for some positive integer $k$, then $a'_{n+1} - a_{n+1}$ is about $10^{-2k}$. That is, each step in the construction of the sequence 'doubles' precision. This is very good for practical purposes, as we can find the limit $a$ to thousands of decimal digits of precision in a few iterations.

Write as in the proof of the previous lemma $a = \lim(a_n)$, $b = \lim(b_n)$ and $c = \lim(c_n)$. Let $\Delta_n = \Delta(P_n, Q_n, R_n)$ and

$$t_n = \frac{2\sqrt{\Delta_n}}{\sqrt{(b_n + b'_n - c_n - c'_n)(c_n + c'_n - a_n - a'_n)(a_n + a'_n - b_n - b'_n)}}.$$

(The factors in the denominator are, up to sign, the leading coefficients of $P_n, Q_n, R_n$.) Let $S \in \mathbb{R}[X]$ be a polynomial of degree at most $1$. Put

$$I_n = \int_{a_n}^{a'_n} \frac{S(t)dt}{\sqrt{|P_n(t)Q_n(t)R_n(t)|}}.$$

**Lemma 4.2.13** (*IV*–2 and 3)**.** *The sequences* $(I_n)$ *and* $(\prod_{i=1}^{n} t_i)$ *converge. The limit of* $(I_n)$ *is*

$$I = \frac{\pi S(a)}{(b-a)(c-a)}.$$

*Moreover,* $I_1 = TI$*, where* $T$ *is the limit of* $(\prod_{i=1}^{n} t_i)$*.*

*Proof.* Let $n$ be a positive integer. We introduce the change of variables

$$t = a_n + (a'_n - a_n)\sin^2(t'), \quad t' \in [0, \pi/2], \tag{4.2.14}$$

to obtain

$$I_n = 2\int_0^{\pi/2} \frac{S(a_n \cos^2 t' + a'_n \sin^2 t')dt'}{\sqrt{\prod_{i=1}^{4}(A_{n,i}\cos^2 t' + A'_{n,i}\sin^2 t')}},$$

where

$$\begin{aligned} A_{n,1} &= b_n - a_n, & A'_{n,1} &= b_n - a'_n, \\ A_{n,2} &= b'_n - a_n, & A'_{n,2} &= b'_n - a'_n, \\ A_{n,3} &= c_n - a_n, & A'_{n,3} &= c_n - a'_n, \\ A_{n,4} &= c'_n - a_n & A'_{n,4} &= c'_n - a'_n. \end{aligned}$$

Using the relations $A'_{n,i} < A_{n,i}$, $A_{n,i} < A_{n,i+1}$ and $A'_{n,i} < A'_{n,i+1}$ we see that

$$(b_n - a'_n)(c_n - a'_n) < \sqrt{\prod_{i=1}^{4}(A_{n,i}\cos^2 t' + A'_{n,i}\sin^2 t')} < (b'_n - a_n)(c'_n - a_n).$$

Note now that $a_n < a_n \cos^2 t' + a'_n \sin^2 t' < a'_n$. It is now clear that from our bounds we can construct two sequences $H_n$ and $J_n$ with $H_n < I_n < J_n$ and that the sequences converge to the common limit

$$I = \frac{\pi S(a)}{(b-a)(c-a)}.$$

Now choose $S$ to be the constant polynomial $1$. Then the integrals $I_n$ corresponding to $S$ are nonzero. From equation (4.2.7) we see that $t_n = I_n/I_{n+1}$. Then

$$I_1 = t_1 I_2 = t_1 t_2 I_3 = \cdots = T_n I_{n+1}.$$

Since $I_n$ converges, $T_n$ converges as well. The last statement of the Lemma follows and the proof is now complete. □

Using the correspondences given by the curves $Z_2, Z_3$ we can show in the same way that

$$\int_{b_1}^{b_1'} \frac{S(t)dt}{\sqrt{|P_1(t)Q_1(t)R_1(t)|}} = \pi T \frac{S(b)}{(b-a)(c-b)}$$

and

$$\int_{c_1}^{c_1'} \frac{S(t)dt}{\sqrt{|P_1(t)Q_1(t)R_1(t)|}} = \pi T \frac{S(c)}{(c-a)(c-b)}.$$

Lemma 4.2.13 implies that the algorithm given in Appendix A2 of [6] is correct and that it terminates. We will reproduce it in the next section for completeness. We will now make the necessary modifications of the algorithm so that we can compute the integrals

$$\int_{x_1}^{x_2} \frac{S(t)dt}{\sqrt{|P_1(t)Q_1(t)R_1(t)|}},$$

where $x_1 = a_1, b_1$ or $c_1$ and $x_2 \in (a_1, a_1'), (b_1, b_1')$, or $(c_1, c_1')$. Assume for simplicity that $x_1 = a_1$ and $a_1 < x_2 < a_1'$. We will now write $x$ instead of $x_2$. In the proof of Lemma 4.2.13 we introduced the change of variables (4.2.14). Under the change of variables for $n = 1$ we obtain

$$\int_{a_1}^{x} \frac{S(t)dt}{\sqrt{|P_1(t)Q_1(t)R_1(t)|}}, = 2\int_0^{x'} \frac{S(a_1\cos^2 t' + a_1'\sin^2 t')dt}{\sqrt{\prod_{i=1}^4 (A_{1,i}\cos^2 t' + A_{1,i}'\sin^2 t')}},$$

where $x' = \arcsin\sqrt{\frac{x-a_1}{a_1'-a_1}}$. As in the proof of the lemma, we can bound the integral as follows:

$$2\frac{x'\min\{S(a_1), S(a_1')\}}{(b_1'-a_1)(c_1'-a_1)} \leq \int_{a_1}^{x} \frac{S(t)dt}{\sqrt{|P_1(t)Q_1(t)R_1(t)|}} \leq 2\frac{x'\max\{S(a_1), S(a_1')\}}{(b_1-a_1')(c_1-a_1')}.$$

In the same way we can find explicit upper and lower bounds for the integrals

$$\int_{a_n}^{x} \frac{S(t)dt}{\sqrt{|P_n(t)Q_n(t)R_n(t)|}},$$

with $x \in (a_n, a_n')$, and the other cases where the integral is from $b_n$ to $x \in (b_n, b_n')$ or from $c_n$ to $x \in (c_n, c_n')$.

We start then with one point $x \in (a_1, a_1')$. Under the correspondence given by the curve $Z_1$ we find two points $x_{1,1}, x_{1,2}$ with $a_2 < x_{1,1} < a_2'$ and $c_2 < x_{1,2} < c_2'$. We will use equations (4.2.1)-(4.2.6) in order to represent the integral we want to compute in terms of the integral of $\frac{S(t)dt}{\sqrt{|P_2(t)Q_2(t)R_2(t)|}}$ along $(a_2, a_2')$, $(b_2, b_2')$, $(c_2, c_2')$, $(a_2, x_1)$ and $(c_2, x_2)$. Since there are many cases to be considered, we will choose only one to show how the algorithm will work. The other cases are handled similarly. Suppose that $a_2' < x < a_1'$. Then,

$$\int_{a_1}^{x} \frac{S(t)dt}{\sqrt{|P_1(t)Q_1(t)R_1(t)|}} = \sqrt{\Delta_1}\left(2\int_{a_2}^{a_2'} \frac{S(t)dt}{\sqrt{|(U_1V_1W_1)(t)|}} - \int_{a_2}^{x_{1,1}} \frac{S(t)dt}{\sqrt{|(U_1V_1W_1)(t)|}} - \int_{c_2}^{c_2'} \frac{S(t)dt}{\sqrt{|(U_1V_1W_1)(t)|}} + \int_{c_2}^{x_{1,2}} \frac{S(t)dt}{\sqrt{|(U_1V_1W_1)(t)|}}\right).$$

Now, from equation (4.2.7) we see that the first integral on the right equals

$$\int_{a_1}^{a_1'} \frac{S(t)dt}{\sqrt{|P_1(t)Q_1(t)R_1(t)|}}$$

and the third equals

$$\frac{1}{2}\int_{c_1}^{c_1'} \frac{S(t)dt}{\sqrt{|P_1(t)Q_1(t)R_1(t)|}}.$$

Moreover,

$$\frac{\sqrt{\Delta_1}}{\sqrt{|(U_1V_1W_1)(t)|}} = \frac{t_1}{2} \cdot \frac{1}{\sqrt{|P_2(t)Q_2(t)R_2(t)|}}.$$

We can then find upper and lower bounds for every integral on the right as we mentioned before, and then taking care of the signs, we can compute a lower and upper bound for their sum, obtaining a bound for the original integral we want to estimate. If the difference between the two bounds is not small enough, we repeat the process to the integrals

$$\frac{t_1}{2}\int_{a_2}^{x_{1,1}} \frac{S(t)dt}{\sqrt{|(P_2Q_2R_2)(t)|}} \quad \text{and} \quad \frac{t_1}{2}\int_{c_2}^{x_{1,2}} \frac{S(t)dt}{\sqrt{|(P_2Q_2R_2)(t)|}}.$$

We obtain then four real numbers $x_{2,1}, x_{2,2}, x_{2,3}, x_{2,4}$ from the correspondences. Using equations (4.2.1)-(4.2.6) again we obtain an expression of the first integral as a sum of a fraction of the integrals

$$\int_{a_1}^{a_1'} \frac{S(t)dt}{\sqrt{|P_1Q_1R_1(t)|}}, \int_{b_1}^{b_1'} \frac{S(t)dt}{\sqrt{|P_1Q_1R_1(t)|}}, \int_{c_1}^{c_1'} \frac{S(t)dt}{\sqrt{|P_1Q_1R_1(t)|}},$$

and a sum of integrals of the form

$$\varepsilon_{2,i}\frac{t_1t_2}{2^2}\int_{a_{2,i}}^{x_{2,i}}\frac{S(t)dt}{\sqrt{|P_3Q_3R_3(t)|}},$$

where $a_{2,i}$ is the largest root of $P_3Q_3R_3$ which is smaller than $x_{2,i}$ and $\varepsilon_{2,i}=\pm 1$. We carry on with the process using the appropriate correspondences. Then at the $n$-th step we have a list of $2^n$ real numbers $x_{n,i}$, $i=1\dots 2^n$, all in $(a_{n+1},a'_{n+1})\cup(b_{n+1},b'_{n+1})\cup(c_{n+1},c'_{n+1})$ and the original integral equals a sum of integrals of the form

$$2^{-n}\prod_{j=1}^{n}t_j\int_{a_{n,i}}^{x_{n,i}}\frac{S(t)dt}{\sqrt{|P_{n+1}Q_{n+1}R_{n+1}(t)|}},$$

where $a_{n,i}$ is the largest root of $P_{n+1}Q_{n+1}R_{n+1}$ which is smaller than $x_{n,i}$, together with a fraction of the integrals of $\frac{S(t)dt}{\sqrt{|P_1(t)Q_1(t)W_1(t)|}}$ along $(a_1,a'_1)$, $(b_1,b'_1)$ and $(c_1,c'_1)$. The precise relation is obtained from equations (4.2.1)-(4.2.6) and equation 4.2.7. Since we can sharply bound those integrals in terms of arcsines of expressions involving $x_{n,i}$ and the roots of $P_{n+1}Q_{n+1}R_{n+1}$ as we mentioned before, we obtain explicit upper and lower bounds

$$H_n\leq\int_{a_1}^{x}\frac{S(t)dt}{\sqrt{|P_1(t)Q_1(t)R_1(t)|}}\leq J_n, \tag{4.2.15}$$

and at every step, the difference between those bounds $J_n-H_n$ gets smaller as the sequences $(a_n)$, $(b_n)$ and $(c_n)$ converge quadratically. We stop the algorithm when the difference is smaller than the required precision.

## 4.3 Algorithms

In this section we present the algorithms we have developed in the previous section in concise form.

Let $a<a'<b<b'<c<c'$ be six real numbers. Put $f(x)=P(x)Q(x)R(x)$, where $P(x)=(x-a)(x-a')$, $Q(x)=(x-b)(x-b')$, and $R(x)=(x-c)(x-c')$. Let $S\in\mathbb{R}[x]$ be a polynomial of degree at most $1$.

The following is Bost and Mestre's algorithm found in [6, Appendice A2].

---

**Bost and Mestre's algorithm for the computation of the integrals**

$$I_a = \int_a^{a'} \frac{S(t)dt}{\sqrt{|f(t)|}},\ I_b = \int_b^{b'} \frac{S(t)dt}{\sqrt{|f(t)|}},\ \text{and}\ I_c = \int_c^{c'} \frac{S(t)dt}{\sqrt{|f(t)|}}.$$

---

INPUT: Six real numbers $a < a' < b < b' < c < c'$. An integer $p > 0$: the required number of digits of precision.

OUTPUT: Three real numbers $I_a^*, I_b^*, I_c^*$ such that $|I_a - I_a^*|$, $|I_b - I_b^*|$, $|I_c - I_c^*| \leq 10^{-p}$.

1. Put $a_1 = a$, $a_1' = a'$, $b_1 = b$, $b_1' = b'$ $c_1 = c$, $c_1' = c'$ and $d = 1$.

2. While the required precision has not been attained do:

   - Compute the maximum $M$ of the following quantities:

$$\frac{\max\{S(a_1), S(a_1')\}}{(b_1 - a_1')(c_1 - a_1')} - \frac{\min\{S(a_1), S(a_1')\}}{(b_1' - a_1)(c_1' - a_1)},$$
$$\frac{\max\{S(b_1), S(b_1')\}}{(b_1 - a_1')(c_1 - b_1')} - \frac{\min\{S(b_1), S(b_1')\}}{(b_1' - a_1)(c_1' - b_1)},$$
$$\frac{\max\{S(c_1), S(c_1')\}}{(c_1 - a_1')(c_1 - b_1')} - \frac{\min\{S(c_1), S(c_1')\}}{(c_1' - a_1)(c_1' - b_1)}.$$

     These are the differences between the upper and lower bounds for the desired integrals computed in the proof of Lemma 4.2.13.

   - Put $M_1 = \pi\sqrt{d}M$.

   - If $M_1 \leq 10^{-p}$ go directly to Step 3.

   - Put

$$a_2 = \frac{c_1c_1' - a_1a_1' - \sqrt{(c_1 - a_1)(c_1 - a_1')(c_1' - a_1)(c_1' - a_1')}}{c_1 + c_1' - a_1 - a_1'},$$
$$a_2' = \frac{a_1a_1' - b_1b_1' - \sqrt{(a_1 - b_1)(a_1 - b_1')(a_1' - b_1)(a_1' - b_1')}}{(a_1 + a_1' - b_1 - b_1')},$$

$$b_2 = \frac{a_1a_1' - b_1b_1' + \sqrt{(a_1-b_1)(a_1-b_1')(a_1'-b_1)(a_1'-b_1')}}{(a_1+a_1'-b_1-b_1')}.$$
$$b_2' = \frac{b_1b_1' - c_1c_1' - \sqrt{(c_1-b_1)(c_1-b_1')(c_1'-b_1)(c_1'-b_1')}}{b_1+b_1'-c_1-c_1'},$$
$$c_2 = \frac{b_1b_1' - c_1c_1' + \sqrt{(c_1-b_1)(c_1-b_1')(c_1'-b_1)(c_1'-b_1')}}{b_1+b_1'-c_1-c_1'},$$
$$c_2' = \frac{c_1c_1' - a_1a_1' + \sqrt{(c_1-a_1)(c_1-a_1')(c_1'-a_1)(c_1'-a_1')}}{c_1+c_1'-a_1-a_1'},$$

and

$$d_1 = (a_1a_1'(c_1+c_1'-b_1-b_1')+ b_1b_1'(a_1+a_1'-c_1-c_1') + c_1c_1'(b_1+b_1'-a_1-a_1'))\times \frac{4d}{(b_1+b_1'-c_1-c_1')(c_1+c_1'-a_1-a_1')(a_1+a_1'-b_1-b_1')}.$$

Note that $\sqrt{d_1/d} = t_n$ in the notation of Lemma 4.2.13.

- Put $a_1 = a_2, a_1' = a_2', b_1 = b_2, b_1' = b_2', c_1 = c_2, c_1' = c_2', d = d_1$.

3. Put

$$I_a^* = \frac{\pi\sqrt{d}S(a_1)}{(a_1-b_1)(a_1-c_1)}, I_b^* = \frac{\pi\sqrt{d}S(b_1)}{(b_1-a_1)(c_1-b_1)}, I_c^* = \frac{\pi\sqrt{d}S(c_1)}{(c_1-b_1)(c_1-a_1)}.$$

Now we present the modified algorithm for the computation of the integral

$$I = \int_{x_1}^{x_2} \frac{S(t)dt}{\sqrt{|P(t)Q(t)R(t)|}},$$

where $x_2 \in (a,a') \cup (b,b') \cup (c,c')$ and $x_1$ is the largest of the roots of $f$ with $x_1 < x_2$. We will use two procedures, one computing an upper and a lower bound for $I$ at the $n$-th step of the algorithm, as in the discussion preceding equation (4.2.15), and one to compute the exact relation between the integral $I$ and the integrals $I_a, I_b, I_c$, and

$$\int_{a_{n,i}}^{x_{n,i}} \frac{S(t)dt}{\sqrt{|P_{n+1}Q_{n+1}R_{n+1}(t)|}}$$

obtained from equations (4.2.1)-(4.2.6).

**Procedure A**

Let $x_{n,i} \in (a_{n+1}, a'_{n+1}) \cup (b_{n+1}, b'_{n+1}) \cup (c_{n+1}, c'_{n+1})$, $\varepsilon_{n,i} = \pm 1$, $i = 1, \ldots, 2^n$ and $\alpha, \beta, \gamma \in \mathbb{Q}$ such that

$$I = \alpha I_a + \beta I_b + \gamma I_c + 2^{-n} \prod_{j=1}^{n} t_j \sum \varepsilon_{n,i} \int_{a_{n,i}}^{x_{n,i}} \frac{S(t)dt}{\sqrt{|P_{n+1}Q_{n+1}R_{n+1}(t)|}},$$

where $a_{n,i}$ is the largest of $a_{n+1}, b_{n+1}, c_{n+1}$ with $a_{n,i} < x_{n,i}$.

Compute a lower and an upper bound for $I$.

---

INPUT: Six real numbers $a < a' < b < b' < c < c'$, a non-negative integer $n$, three rational numbers $\alpha, \beta, \gamma$, a list of $2^n$ pairs $(x_{n,i}, \varepsilon_{n,i}) \in D \times \mathbb{Q}$, $D = (a, a') \cup (b, b') \cup (c, c')$, a real number $d$.

OUTPUT: Two real numbers $H, J$ such that $H < I < J$.

1. Put $I_1 = \frac{1}{(b'-a)(c'-a)}$, $I'_1 = \frac{1}{(b-a')(c-a')}$, $I_2 = \frac{1}{(b'-a)(c'-b)}$, $I'_2 = \frac{1}{(b-a')(c-b')}$, $I_3 = \frac{1}{(c'-a)(c'-b)}$, $I'_3 = \frac{1}{(c-a')(c-b')}$.

2. For $i = 1 \ldots 2^n$ do

   - Compute $a_{n,i}$, the largest of $a_{n+1}, b_{n+1}, c_{n+1}$ with $a_{n,i} < x_{n,i}$. Set $a'_{n,i}$ to be $a', b', c'$ according to whether $a_{n,i} = a, b$ or $c$.
   - Put $\theta_i = \arcsin \sqrt{\frac{x_{n,i} - a_{n,i}}{a'_{n,i} - a_{n,i}}}$.
   - If $\varepsilon_{n,i} = -1$ then
     - Put

$$H_i = -\frac{\theta_i \sqrt{d}}{2^{n-1}} \times \begin{cases} I'_1 & a_{n,i} = a, \\ I'_2 & a_{n,i} = b, \\ I'_3 & a_{n,i} = c, \end{cases}$$

     and

$$J_i = -\frac{\theta_i \sqrt{d}}{2^{n-1}} \times \begin{cases} I_1 & a_{n,i} = a, \\ I_2 & a_{n,i} = b, \\ I_3 & a_{n,i} = c, \end{cases}$$

- Else do

  - Put

$$H_i = \frac{\theta_i\sqrt{d}}{2^{n-1}} \times \begin{cases} I_1 & a_{n,i} = a, \\ I_2 & a_{n,i} = b, \\ I_3 & a_{n,i} = c, \end{cases}$$

  and

$$J_i = \frac{\theta_i\sqrt{d}}{2^{n-1}} \times \begin{cases} I_1' & a_{n,i} = a, \\ I_2' & a_{n,i} = b, \\ I_3' & a_{n,i} = c. \end{cases}$$

3. Put

$$H_a = \alpha\pi\sqrt{d} \times \begin{cases} I_1 & \alpha \geq 0, \\ I_1' & \alpha < 0, \end{cases}, \quad J_a = \alpha\pi\sqrt{d} \times \begin{cases} I_1' & \alpha \geq 0, \\ I_1 & \alpha < 0, \end{cases},$$

$$H_b = \beta\pi\sqrt{d} \times \begin{cases} I_2 & \beta \geq 0, \\ I_2' & \beta < 0, \end{cases}, \quad J_b = \beta\pi\sqrt{d} \times \begin{cases} I_2' & \beta \geq 0, \\ I_2 & \beta < 0, \end{cases}$$

   and

$$H_c = \gamma\pi\sqrt{d} \times \begin{cases} I_3 & \gamma \geq 0, \\ I_3' & \gamma < 0, \end{cases}, \quad J_c = \gamma\pi\sqrt{d} \times \begin{cases} I_3' & \gamma \geq 0, \\ I_3 & \gamma < 0. \end{cases}$$

4. Put $H = H_a + H_b + H_c + \sum_{i=1}^{2^n} H_i$ and $J = J_a + J_b + J_c + \sum_{i=1}^{2^n} J_i$.

---

We now present the second procedure.

---

**Procedure B**

Let $x_{n,i} \in (a_{n+1}, a'_{n+1}) \cup (b_{n+1}, b'_{n+1}) \cup (c_{n+1}, c'_{n+1})$, $\varepsilon_{n,i} = \pm 1$, $i = 1, \ldots, 2^n$ and $\alpha, \beta, \gamma \in \mathbb{Q}$ such that

$$I = \alpha I_a + \beta I_b + \gamma I_c + 2^{-n} \prod_{j=1}^{n} t_j \sum \varepsilon_{n,i} \int_{a_{n,i}}^{x_{n,i}} \frac{S(t)dt}{\sqrt{|P_{n+1}Q_{n+1}R_{n+1}(t)|}},$$

where $a_{n,i}$ is the largest of $a_{n+1}, b_{n+1}, c_{n+1}$ with $a_{n,i} < x_{n,i}$.

Compute $\alpha', \beta', \gamma' \in \mathbb{Q}$ and for every $i = 1, \ldots, 2^n$ compute the values $z_1(x_{n,i}), z_2(x_{n,i})$, and $\eta_i, \xi_i \in \{-1, 1\}$ such that

$$I = \alpha' I_a + \beta' I_b + \gamma' I_c + \sum_{i=1}^{2^n} \eta_i \int_{b_{n,i}}^{z_1(x_{n,i})} \frac{S(t)dt}{\sqrt{|P_{n+1}Q_{n+1}R_{n+1}(t)|}} + \sum_{i=1}^{2^n} \xi_i \int_{c_{n,i}}^{z_2(x_{n,i})} \frac{S(t)dt}{\sqrt{|P_{n+1}Q_{n+1}R_{n+1}(t)|}},$$

where $b_{n,i}$ (resp. $c_{n,i}$) is the largest of the roots of $P_{n+1}Q_{n+1}R_{n+1}$ with $b_{n,i} < z_1(x_{n,i})$ (resp. $c_{n,i} < z_2(x_{n,i})$).

---

INPUT: Twelve different real numbers $a, v, w, a', b, w', u, b', c, u', v', c'$ ordered increasingly, a non-negative integer $n$, three rational numbers $\alpha, \beta, \gamma$, a list of $2^n$ pairs $(x_{n,i}, \varepsilon_{n,i}) \in D \times \mathbb{Q}$,
$D = (a, a') \cup (b, b') \cup (c, c')$, a real number $d$.

OUTPUT: Three rational numbers $\alpha', \beta', \gamma'$, a list of $2^{n+1}$ pairs $(x_{n+1,i}, \varepsilon_{n+1,i})$ with $\varepsilon_{n+1,i} = \pm 1$ and
$x_{n+1,i} \in (v, w) \cup (w', u) \cup (u', v')$.

1. For $i = 1 \ldots 2^n$ do

- Compute $a_{n,i}$, the largest of $a_{n+1}, b_{n+1}, c_{n+1}$ with $a_{n,i} < x_{n,i}$.
- Set $a'_{n,i}$ to be $a', b', c'$ according to whether $a_{n,i} = a, b$ or $c$.
- Compute the roots $z_1(x_{n,i}) < z_2(x_{n,i})$ of the degree 2 polynomial $F(z)$ given by

$$F(z) = \begin{cases} P(x_{n,i})U(z) + Q(x_{n,i})V(z), & a_{n,i} = a, \\ Q(x_{n,i})V(z) + R(x_{n,i})W(z), & a_{n,i} = b, \\ P(x_{n,i})U(z) + R(x_{n,i})W(z), & a_{n,i} = c. \end{cases}$$

- Put

$$\eta_i = \varepsilon_{n,i} \times \begin{cases} 1, & a_{n,i} = a \text{ and } x_{n,i} \le w, \\ -1, & \text{all other cases}, \end{cases}$$

and

$$\xi_i = \varepsilon_{n,i} \times \begin{cases} -1, & (a_{n,i} = b \text{ and } x_{n,i} > u) \text{ or } (a_{n,i} = c \text{ and } x_{n,i} > v'), \\ 1, & \text{all other cases.} \end{cases}$$

- Put

$$\alpha_i = \varepsilon_{n,i} \times \begin{cases} 2^{-n-1} & x_{n,i} \in (b, b'), \\ 2^{-n} & x_{n,i} \in (w, a') \\ 0 & \text{all other cases.} \end{cases}$$

$$\beta_i = \varepsilon_{n,i} \times \begin{cases} 2^{-n-1} & x_{n,i} \in (c, c'), \\ 2^{-n} & x_{n,i} \in (u, b') \\ 0 & \text{all other cases.} \end{cases}$$

and

$$\gamma_i = \varepsilon_{n,i} \times \begin{cases} -2^{-n-1} & x_{n,i} \in (a, a'), \\ 2^{-n} & x_{n,i} \in (v', c') \\ 0 & \text{all other cases.} \end{cases}$$

2. Put $\alpha' = \alpha + \sum_{i=1}^{2^n} \alpha_i$, $\beta' = \beta + \sum_{i=1}^{2^n} \beta_i$, , $\gamma' = \gamma + \sum_{i=1}^{2^n} \gamma_i$.

3. Put $x_{n+1,2i-1} = z_1(x_{n,i})$, $x_{n+1,2i} = z_2(x_{n,i})$, $\varepsilon_{n+1,2i-1} = \eta_i$ and $\varepsilon_{n+1,2i} = \xi_i$, $i = 1, \ldots, 2^n$.

---

We are now ready to present the modification of Bost and Mestre's algorithm.

---

**Algorithm for the computation of the integral**

$$I = \int_{x_1}^{x_2} \frac{S(t)dt}{\sqrt{|f(t)|}}.$$

INPUT: Six real numbers $a < a' < b < b' < c < c'$, a real number $x \in (a, a') \cup (b, b') \cup (c, c')$. An integer $p > 0$, the required number of digits of precision.

OUTPUT: A real number $I^*$ such that $|I - I^*| \leq 10^{-p}$.

1. Put $a_1 = a$, $a'_1 = a'$, $b_1 = b$, $b'_1 = b'$ $c_1 = c$, $c'_1 = c'$, $d = 1$, $n = 0$, and $\alpha = \beta = \gamma = 0$.

2. Let $L$ be the list consisting of the pair $(x, 1)$.

3. While the precision has not been attained do

   - Let $H, J$ be the lower and upper bounds for $I$ obtained from Procedure A applied to $a_1, a'_1, b_1, b'_1, c_1, c'_1$, $n$, $\alpha, \beta, \gamma$ and $d$.
   - Put $M_1 = J - H$.
   - If $(M_1 < 10^{-p})$ go directly to Step 4.
   - Compute $a_2, a'_2, b_2, b'_2, c_2, c'_2$ and $d_1$ as in Bost and Mestre's algorithm,
   - Apply Procedure B to $a_1, a'_1, b_1, b'_1, c_1, c'_1$, $n$, $\alpha, \beta, \gamma$ and $d$ to obtain a list $L'$ and rational numbers $\alpha', \beta', \gamma'$.
   - $n = n + 1$. Put $a_1 = a_2, a'_1 = a'_2, b_1 = b_2, b'_1 = b'_2, c_1 = c_2, c'_1 = c'_2, d = d_1$.
   - Put $L = L'$, $\alpha = \alpha'$, $\beta = \beta'$, $\gamma = \gamma'$.

4. Put $I^* = H$.

Note that since $H < I < J$ and $J - H \leq 10^{-p}$, then $|I - H| \leq 10^{-p}$ and the output of the algorithm is correct.

### 4.3.1 A note on precision

The complexity of Bost and Mestre's algorithm is $O(M(N) \log N)$, where $N$ is the number of decimal places of required precision and $M(N)$ stands for the complexity of the

algorithm used for the multiplication of two $N$-digit numbers. (See Section 9.2.2 of [19].)

In practice we will want to compute the integrals to a specific number of digits. We can estimate the number of iterations of the algorithms needed to attain such precision by means of the last statement of Lemma 4.2.12. We note that a coarse estimate shows that we lose about $10$ digits of precision with respect to the precision of the input at every iteration of Bost and Mestre's algorithm. When we compute the final output we lose about $8$ more digits. We can use these estimates to know how much precision we need on the input in order to have a correct output. For instance, in the example presented below, we require $1000$ digits of precision. We first estimate that we will need $12$ steps to attain $1000$ digits of precision. Then, if the input is given with $m$ digits of precision, the final output will be correct to $m - 130$ digits. Then, if the input is given to more than $1130$ digits of precision our output will be correct to $1000$ digits as required. For the example below we used real numbers given with $3000$ digits of precision, which is far more than what we need.

The modification of Bost and Mestre's algorithm will require more precision on the input, as every iteration involves more operations, and the final output will also require many operations. A coarse estimate shows that we lose about $23$ digits of precision at every iteration. If we stop the algorithm at the $m$-th iteration, we lose $2^m + 2$ digits from the computation of the final output. In the example below in order to obtain $1000$ digits of precision we need $12$ iterations. Then the final output will have $4374$ digits of precision less than the input. We thus need more than $5374$ digits of precision on the input. For the example, we used $10000$ digits of precision on the input.

The `MAGMA` algebra system prints reliable output. When one requires `MAGMA` to work with $3000$-digit arithmetic, it does not always print $3000$ decimal places of a required number. It presents less digits, but the digits printed are reliable. We conform ourselves with obtaining a printed output with slightly more than the required digits of precision, for we know that the output will be reliable to that precision.

**Example 4.3.1.** Consider the polynomial $f(X) = X^5 - 5X^3 - X^2 + 3X + 1$. It has five

real roots given by

$$a_1 = -1.96002661715932491777\ldots,\ a_2 = -0.72281270157961201762\ldots,$$
$$a_3 = -0.36968038412101119752\ldots,\ a_4 = 0.87809490178975922400\ldots,$$
$$a_5 = 2.17442480107018890892\ldots,$$

to $20$ decimal places. (We will not write here the more-than-$2000$ decimal places printed by MAGMA.)

Note that $f(0) = f(-1) = 1$, and $f(9/4) = (59/32)^2$. Let $x_1 = -1, x_2 = 0$, and $x_3 = 9/4$. We note that they lie respectively in the intervals $(a_1, a_2)$, $(a_3, a_4)$ and $(a_5, \infty)$. We will now use the algorithms presented in this chapter to compute the integrals of

$$\frac{dt}{\sqrt{f(t)}}, \quad \frac{t\,dt}{\sqrt{f(t)}},$$

along the intervals

$$(a_1, a_2),\ (a_5, \infty),$$
$$(x_1, a_2),\ (x_2, a_4),\ (x_3, \infty).$$

Since the degree of $f$ is $5$, we need to introduce a change of variables as explained in Section 4.1. We choose the following change of variables:

$$t' = g(t) = \frac{1}{t - (a_2 + a_3)/2}.$$

Note that according to Section 4.1 the integrals we need to compute are now of the form

$$\int \frac{dt'}{\sqrt{\tilde{f}(t')}}, \quad \int \frac{t'\,dt'}{\sqrt{\tilde{f}(t')}},$$

where $\tilde{f}$ is of degree $6$. The precise relation can be computed from Equation 4.1.2. We have chosen $(a_2 + a_3)/2$ as the point mapping to $\infty$ under the change of variables, so that $\tilde{f}$ is negative along the intervals corresponding to the original intervals we are

interested in. The roots of $f$ are mapped to five of the roots of $\tilde{f}$, and $\infty$ is mapped to $0$, which is the sixth root of $\tilde{f}$. The roots of $\tilde{f}$ are ordered as follows

$$a'_2 < a'_1 < 0 < a'_5 < a'_4 < a'_3,$$

where $a'_i = g(a_i)$. Moreover, the intervals $(x_1, a_2), (x_2, a_4), (x_3, \infty)$ are mapped to $(a'_2, x'_1), (a'_4, x'_2), (0, x'_3)$, so all integrals we need to compute are already in the form required by the algorithms to work. After only $7$ iterations we find the integrals along all the intervals to $32$ decimal places, and after $12$ iterations, the precision is at least of $1026$ decimal places, as computed by the difference of the bounds for the integral described in the previous section. The computation of each integral took less than two minutes. We reproduce the values of the integrals in Table 4.1, to $20$ decimal places. (The full output, with $1026$ decimal places can be found in the address below.) We

Table 4.1: Value of the integrals to $20$ decimal places.

| Interval | $\int dt/\sqrt{f(t)}$ | $\int t\ dt/\sqrt{f(t)}$ |
|---|---|---|
| $(a_1, a_2)$ | $1.345612414294682752214$ | $-1.560324774496408198666$ |
| $(a_3, \infty)$ | $0.386988322453914193981$ | $1.81246715789527708463$ |
| $(x_1, a_2)$ | $0.66475800776085826705$ | $-0.53709088385333377913$ |
| $(x_2, a_4)$ | $0.90105534714502372440$ | $0.46327467596785800929$ |
| $(x_3, \infty)$ | $0.30138196613949747325$ | $1.62420319614817059241$ |

have computed the integrals along $(a_1, a_2)$ and $(x_1, a_2)$ using the numerical integration methods provided by Mathematica [52]. We obtain the following values

$$\int_{a_1}^{a_2} \frac{dt}{\sqrt{f(t)}} = 1.34561241208, \qquad \int_{a_1}^{a_2} \frac{t\ dt}{\sqrt{f(t)}} = -1.5603247725,$$
$$\int_{x_1}^{a_2} \frac{dt}{\sqrt{f(t)}} = 0.66475800739, \qquad \int_{x_1}^{a_2} \frac{t\ dt}{\sqrt{f(t)}} = -0.5370908835,$$

Mathematica displayed a warning stating that the algorithm failed to converge at the ninth iteration. Note that the values computed by Mathematica agree with the values we have computed for the integrals to $9$ decimal places. But as remarked at the beginning of this subsection, our output is correct in the places where it differs from that given by Mathematica.

# Chapter 5

# Reduction of the upper bound for the size of the integral points

In Chapter 3 we described how one can completely determine all the $S$-integral points on a hyperelliptic curve. We noted that the second step for the determination of the $S$-integral points, namely the variant of the Mordell–Weil sieve can be time consuming and memory demanding, specially if one needs to sieve up to a very large bound. We would like to reduce the upper bound for the size of the $S$-integral points so that we can search for all the points below the bound, instead of performing an expensive sieve.

In [47], Stroeker and Tzanakis describe how one can solve elliptic Diophantine equations by estimating linear forms in elliptic logarithms. Their approach consists of using the classical theory of elliptic logarithms to turn the information given by the Mordell–Weil group of an elliptic curve $\mathcal{E}$ into numerical data that says how far an integral point is from the point at infinity on $\mathcal{E}$. They obtain an upper bound for the coefficients of the linear combination for a given point $P$ in terms of the generators of $\mathcal{E}(\mathbb{Q})$ and then they reduce it to manageable proportions using the LLL-algorithm.

In this chapter we develop an analogous method for the genus $2$ case. We must restrict our attention to the integral case ($S = \emptyset$). From now on we will only look for the integral points on a genus $2$ hyperelliptic curve. A further restriction that we will need is

assuming that the polynomial $f$ defining the curve has real roots only, all different, and that the generators of the free part of $J(\mathbb{Q})$ are given by representatives supported by real points only.

We now briefly sketch the strategy to find all the integral points on a genus $2$ hyperelliptic curve. First, we obtain a bound for the size of the integral points using the techniques from Chapter 3. We also take advantage of the Abel–Jacobi map $\phi$ to identify $J(\mathbb{C})$ with $\mathbb{C}^2/\Lambda$, where $\Lambda$ is a rank $4$ lattice generated by the periods of $\mathbb{C}$. Choose a fundamental domain in $\mathbb{C}^2$ for the lattice. Let $D_1, \ldots, D_r$ be generators for the free part of $J(\mathbb{Q})$. Assume $P$ is an (unknown) integral point on $\mathcal{C}$. Then, if $P_0$ is a fixed rational point on $\mathcal{C}$, the relation

$$P - P_0 = m_1 D_1 + \cdots + m_r D_r + T$$

in $J(\mathbb{Q})$, where $T$ is a torsion element, can be translated into a relationship between the image $\phi(D_i)$ in the fundamental domain of the generators of the $D_i$s and the (unknown) image $\phi(P - P_0)$ of the degree $0$ divisor $P - P_0$ modulo the lattice $\Lambda$. This relation is the linear form in hyperelliptic logarithms we will use. By completely elementary methods, one can also compute bounds for the norm of the entries in $\mathbb{C}$ of the vector $\phi(P - P_0)$. The upper bound for the size of the integral points is translated to an upper bound $M$ for the absolute value of the coefficients $m_i, i = 1, \ldots r$. We can rephrase the existence of this bound as follows: if $P$ is an integral point on $\mathcal{C}$, then the coefficients of the divisor $P - P_0$ in terms of the $D_i$s are at most $M$. The aim of the method is to reduce the bound $M$ in such a way that one can practically look for all possible combinations in $J(\mathbb{Q})$ of the $D_i$s and the torsion points with coefficients bounded by $M$ and deduce which combinations come from integral points. This would completely determine all the integral points on $\mathcal{C}$.

The chapter is arranged as follows. The first section is devoted to the background needed, namely, the standard material on the theory of Jacobians of a Riemann surface. Section 5.2 is concerned with the numerical computation of the periods of a genus $2$ curves defined over the reals and hyperelliptic logarithms using the algorithms

presented in Chapter 4. Section 5.3 explains how one obtains and estimates linear forms in hyperelliptic logarithms from the information given by $J(\mathbb{Q})$. Lastly, Section 5.4 describes how using the LLL-algorithm, one can reduce the estimates for the coefficients of the linear forms to manageable proportions.

## 5.1 Analytic Jacobians

Here we summarise standard material on the analytic Jacobian found in [33, 34, 26]. Let $\mathcal{S}$ be a compact Riemann surface of genus $g$. The genus $g$ is the 'number of handles' of the surface $\mathcal{S}$. The genus is also the dimension of the space of holomorphic differentials on $\mathcal{S}$. The Riemann surface $\mathcal{S}$ can be represented as a polygon with $4g$ sides identified as in Figure 5.1. The simple paths $A_i$, $B_i$ are disjoint except at their starting point. We

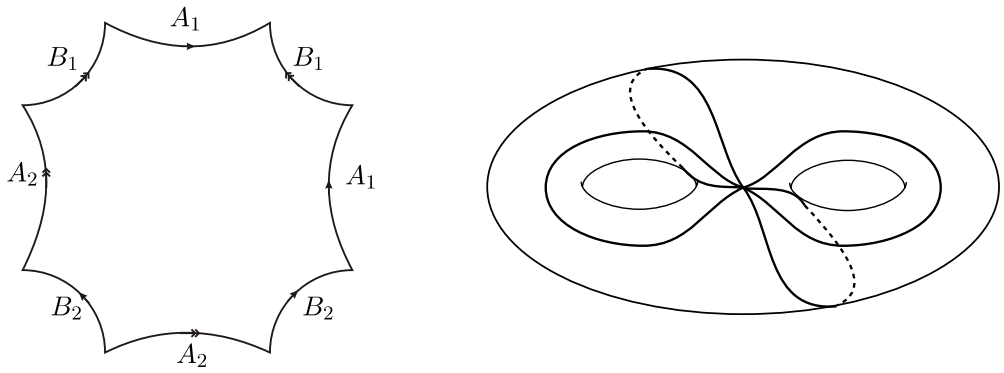


Figure 5.1: An octagon defining a genus $2$ surface.

note that the intersection product of the cycles $A_i$ and $A_j$ is $0$, with $i \neq j$, and the same for the cycles $B_i$ and $B_j$, whereas the intersection product of the cycles $A_i$ and $B_j$ is $\delta_{ij}$. The cycles $A_i$ and $B_i$ are then a basis for $H^1(\mathcal{S}, \mathbb{Z})$.

Now, let $\phi_1, \ldots, \phi_g \in H^0(\mathcal{S}, \Omega^1)$ be a basis for the space of holomorphic $1$-forms on $\mathcal{S}$. We take the following definition from [26, Chapter 2, Section 2].

**Definition.** The *period matrix of* $\mathcal{S}$ with respect to the basis $A_i$, $B_i$ and the basis $\phi_j$ is

the $g \times 2g$ matrix

$$\Omega = \begin{pmatrix} \int_{A_1} \phi_1 & \cdots & \int_{A_g} \phi_1 & \int_{B_1} \phi_1 & \cdots & \int_{B_g} \phi_1 \\ \vdots & \cdots & \vdots & \vdots & \cdots & \vdots \\ \int_{A_1} \phi_g & \cdots & \int_{A_g} \phi_g & \int_{B_1} \phi_g & \cdots & \int_{B_g} \phi_g \end{pmatrix}.$$

The column vectors $\left(\int_{A_i} \phi_1, \ldots, \int_{A_i} \phi_g\right) \in \mathbb{C}^g$ and $\left(\int_{B_i} \phi_1, \ldots, \int_{B_i} \phi_g\right) \in \mathbb{C}^g$ are called the *periods of* $\mathcal{S}$.

The $2g$ periods of $\mathcal{S}$ are linearly independent vectors over $\mathbb{R}$ [26, p. 228]. Then the periods generate a rank $2g$ lattice $\Lambda$ in $\mathbb{C}^g$ called the *period lattice* of $\mathcal{S}$.

**Definition.** The *Analytic Jacobian variety* $J(\mathcal{S})$ of $\mathcal{S}$ is the complex torus $\mathbb{C}^g/\Lambda$.

We now pick a base point $P_0 \in \mathcal{S}$. Consider the map

$$\phi : \mathcal{S} \to J(\mathcal{S}), \quad P \mapsto \left(\int_{P_0}^{P} \phi_1, \ldots, \int_{P_0}^{P} \phi_g\right) \bmod \Lambda.$$

This is well defined, as if $\gamma_1$ and $\gamma_2$ are paths connecting $P_0$ to $P$, the difference between the two vectors of integrals is a vector of integrals along a closed path and hence it is in the period lattice $\Lambda$. The map can be extended linearly to the group of degree $0$ divisors on $\mathcal{S}$, $\mathrm{Div}^0(\mathcal{S})$ by

$$\begin{aligned} \phi\left(\sum P_i - \sum Q_i\right) &= \sum(\phi(P_i)) - \sum(\phi(Q_i)) \\ &= \sum \left(\int_{Q_i}^{P_i} \phi_1, \ldots, \int_{Q_i}^{P_i} \phi_g\right) \bmod \Lambda. \end{aligned}$$

The following Proposition is Proposition §II.2.4 of [33].

**Proposition 5.1.1.** *Let $f$ be a meromorphic function on $\mathcal{S}$. Then $\phi((f)) = 0$, where $(f)$ denotes the principal divisor of $f$.*

We then have a well defined morphism

$$\phi : \mathrm{Pic}^0(\mathcal{S}) \to J(\mathcal{S}).$$

Abel's theorem states that $\phi$ is an injection. We present it here without proof and refer the reader to Chapter 2 of [33].

**Theorem 5.1.2** (Abel's Theorem)**.** *Let $D$ be a degree $0$ divisor on $\mathcal{S}$. Then $\phi(D) = 0 \bmod \Lambda$ if and only if $D$ is a principal divisor.*

Further, we have the following theorem [26, p. 235], telling us that we in fact have an isomorphism.

**Theorem 5.1.3** (Jacobi Inversion)**.** *The map*

$$\phi : \mathrm{Pic}^0(\mathcal{S}) \to J(\mathcal{S})$$

*is surjective.*

## 5.2 Computation of periods

We want to compute numerically the periods of the Riemann surface of a genus $2$ hyperelliptic curve $\mathcal{C}(\mathbb{C})$ and we also want to compute the value $\phi(P)$ for a given point $P \in \mathcal{C}(\mathbb{C})$ and a choice of a base point $P_0 \in \mathcal{C}(\mathbb{Q})$, where $\phi : \mathcal{C}(\mathbb{C}) \to J(\mathcal{C}(\mathbb{C}))$ is defined as in the previous section, and $J(\mathcal{C}(\mathbb{C}))$ is the analytic Jacobian variety of $\mathcal{C}(\mathbb{C})$.

We first need to choose a homology basis $A_i$, $B_i$ as in the previous section. There is a traditional way to do this. We follow Mumford [34, §III.5] with some small modifications. The curve

$$\mathcal{C} : Y^2 = f(X),$$

is a double cover of the projective line $\mathbb{P}^1(\mathbb{C})$, via the meromorphic function $X$, when considered as a compact Riemann surface. Let $a_1, a_2, a_3, a_4, a_5, a_6$ be the branch points. These are the roots of $f(X)$, together with the point at infinity if $f$ has degree $5$. A linear transformation $X' = 1/(X - a)$ and an associated transformation of $Y' = Y/(X + a)^3$ takes a hyperelliptic curve $C$ defined by a degree $5$ polynomial to a hyperelliptic curve given by a degree $6$ polynomial, for a suitable choice of $a$ (it should be different from the roots of $f$). So we can assume that the branch points are all in the complex plane $\mathbb{C}$ and the curve has two points at infinity. (Mumford takes

curves with the point at infinity as a branch point. But the present form is best for our purposes.) Figure 5.2 gives an illustration of how the Riemann surface of $\mathcal{C}(\mathbb{C})$ looks like. We choose disjoint segments on $\mathbb{C}$ joining $a_1$ and $a_2$, $a_3$ and $a_4$, $a_5$ and $a_6$. Note

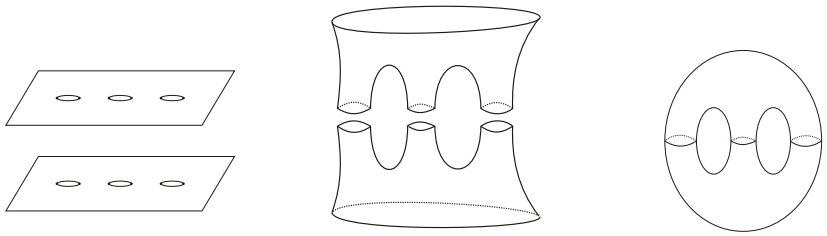

Figure 5.2: The Riemann surface of a hyperelliptic curve.

that if we choose a point $x \in (a_1, a_2)$, and a square root for $f(x)$, and then we go counter-clockwise around $a_1$, choosing continuously a square root, when we return to $x$ we have a different root to the one we had chosen in the beginning. In other words, when we think of the Riemann surface of $\mathcal{C}(\mathbb{C})$ as a two-layered cover of $\mathbb{P}^1(\mathbb{C})$, the lift of the path in $\mathbb{P}^1(\mathbb{C})$ to the Riemann surface 'interchanges' layers. To get the topological picture what we are doing is taking two copies of $\mathbb{P}^1$, we cut along the segments joining the $a_i$s, and we glue the two layers along the corresponding segments as in the figure.

We will need to choose representatives for a homology basis. We now take paths on $\mathbb{P}^1(\mathbb{C}) \setminus \{a_1, \ldots, a_6\}$ as in Figure 5.3. Since each path circles an even number

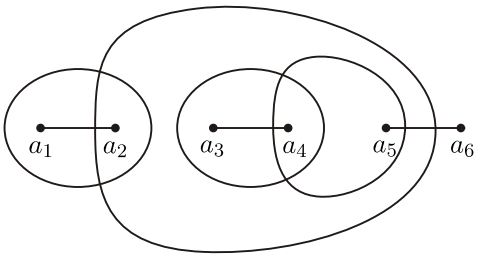


Figure 5.3: Paths below the cycles in the homology basis.

of branch points, these paths can be lifted to the double cover $\mathcal{C}(\mathbb{C})$. We will choose one lift for each path and that will be our choice of homology basis. We will denote by

$A_1$ the lift of the path around $a_1, a_2$ and by $A_2$ the the lift of the path around $a_3, a_4$. (We take care of choosing the lifts $A_1$, $A_2$ on the same layer.) We will denote by $B_1$ and $B_2$ the lifts of the paths around $a_2$, $a_3$, $a_4$, $a_5$ and $a_4$, $a_5$ respectively. We also need to choose a basis for the space of holomorphic differentials on $\mathcal{C}(\mathbb{C})$. The following is Proposition §III.5.2 in [34].

**Proposition 5.2.1.** *The $2$-dimensional vector space $\Gamma(\mathcal{C}(\mathbb{C}), \Omega^1)$ consists of the $1$-forms*

$$\omega = \frac{P(X)dX}{Y}, \quad P \text{ a polynomial of degree} < 2.$$

*Proof.* Since $Y^2 = f(X)$ we have $2YdY = f'(X)dX$. Hence

$$\frac{P(X)dX}{Y} = \frac{2P(X)dY}{f'(X)}.$$

On the affine piece of $\mathcal{C}(\mathbb{C})$, $Y = 0$ implies that $f(X) = 0$, and hence $f'(X) \neq 0$ as $f$ has no double roots. This implies that the form $\omega$ has no poles on the affine piece. Now, for the points at infinity we look at the affine piece with coordinates given by $X' = 1/(X + a)$, $Y' = Y/(X + a)^3$, where $a \in \mathbb{C}$ is not one of the branch points. We then have

$$\begin{aligned} dY' &= \frac{dY}{(X+a)^3} - 3\frac{YdX}{(X+a)^4} \\ &= \left(\frac{f'(X)}{2(X+a)^3} - 3\frac{Y^2}{(X+a)^4}\right)\frac{dX}{Y} \\ &= \left(\frac{f'(X)(X+a) - 6f(X)}{2(X+a)^4}\right)\frac{dX}{Y}, \end{aligned}$$

and hence

$$\frac{dX}{Y} = \frac{2(X+a)^4}{f'(X)(X+a) - 6f(X)} \cdot dY'.$$

Note that the denominator on the right hand side of the equation is a degree $5$ polynomial, so at the points at infinity $\frac{2(X+a)^4}{f'(X)(X+a)-6f(X)}$ has an order $1$ zero. Then, the form $\omega$ is holomorphic as the degree of $P$ is at most $1$. □

We choose the differentials $\{\phi_1, \phi_2\} = \{dX/Y, XdX/Y\}$ as a basis for the space $\Gamma(\mathcal{C}(\mathbb{C}), \Omega^1)$.

We are now interested in the numerical computation of the period lattice $\Lambda$ of $\mathcal{C}(\mathbb{C})$ relative to our choice of homology basis and the basis for the holomorphic forms. In the previous chapter we presented Bost and Mestre's algorithm [6] to compute integrals of the form

$$\int_a^b \frac{S(t)\,dt}{\sqrt{|f(t)|}}$$

to high precision, where $S$ is a degree one polynomial defined over the reals, $f$ is a degree $6$ monic polynomial defined over the reals with $6$ real roots, and $a$ and $b$ are two consecutive roots of $f$. We will first see how these integrals are related to the periods of $\mathcal{C}$. Let $a_1 < a_2 < a_3 < a_4 < a_5 < a_6$ be the roots of $f$ in ascending order. Since $f$ is monic, and all the roots are in $\mathbb{R}$ we have that $f$ is non-negative along the segments $(-\infty, a_1]$, $[a_2, a_3]$, $[a_4, a_5]$ and $[a_6, \infty)$; and it is negative along the segments $I_1 = (a_1, a_2)$, $I_2 = (a_3, a_4)$, and $I_3 = (a_5, a_6)$. The intervals $I_i$ are covered by the loops in $\mathcal{C}(\mathbb{C})$ consisting of the points $(x, \pm i\sqrt{-f(x)})$, with $x \in I_i$. The loop covering $I_1$ is homologous to $A_1$, whereas the loop covering $I_2$ is homologous to $A_2$. Similarly, the segment $[a_2, a_3]$ is covered by a loop in $\mathcal{C}(\mathbb{C})$ homologous to $B_1 - B_2$, and the interval $[a_4, a_5]$ is covered by a loop homologous to $B_2$. See Figure 5.4. (cf. Figure 5.2 and 5.3.) The period lattice $\Lambda$ of $\mathcal{C}(\mathbb{C})$ is then generated by the vectors of integrals

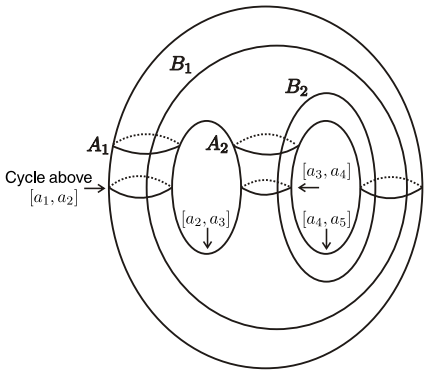


Figure 5.4: Cycles above $[a_i, a_{i+1}]$ compared to the chosen homology basis.

$$\omega_1 = \begin{pmatrix} 2\int_{a_2}^{a_3} \frac{dt}{\sqrt{f(t)}} \\ 2\int_{a_2}^{a_3} \frac{t\,dt}{\sqrt{f(t)}} \end{pmatrix}, \qquad \omega_2 = \begin{pmatrix} 2\int_{a_4}^{a_5} \frac{dt}{\sqrt{f(t)}} \\ 2\int_{a_4}^{a_5} \frac{t\,dt}{\sqrt{f(t)}} \end{pmatrix},$$

$$\omega_3 = \begin{pmatrix} 2i\int_{a_1}^{a_2} \frac{dt}{\sqrt{-f(t)}} \\ 2i\int_{a_1}^{a_2} \frac{t\,dt}{\sqrt{-f(t)}} \end{pmatrix}, \qquad \omega_4 = \begin{pmatrix} 2i\int_{a_3}^{a_4} \frac{dt}{\sqrt{-f(t)}} \\ 2i\int_{a_3}^{a_4} \frac{t\,dt}{\sqrt{-f(t)}} \end{pmatrix}.$$

We note that the first two vectors in our list have real coordinates, whereas the last two vectors have purely imaginary coordinates. In particular the rank $2$ lattice $\Lambda' = \Lambda \cap \mathbb{R}^2 \subset \mathbb{R}^2$ is generated by $\omega_1$ and $\omega_2$. Then, Bost and Mestre's algorithm serves our purposes for the computation of a set of generators for the period lattice, as the integrals computed by it are *half-periods* of $\mathcal{C}$.

We recall that Bost and Mestre's algorithm only computes the integrals

$$\int_{I_i} \frac{S(t)dt}{\sqrt{-f(x)}}$$

for the intervals $I_i$ where $f$ is negative. The authors of the algorithm observe that some modifications would allow one to compute the integral along the intervals where $f$ is positive, and we have given full details and proofs of the modifications in Chapter 4.

We will also need to numerically compute the value

$$\phi(P) = \left( \int_{P_0}^{P} \phi_1, \int_{P_0}^{P} \phi_2 \right),$$

for a fixed base point $P_0$ and a point $P \in \mathcal{C}(\mathbb{R})$.

**Definition.** Let $\mathcal{D}$ be a fundamental domain of the period lattice of $\mathcal{C}$. For every degree $0$ divisor $D$ the *hyperelliptic logarithm of* $D$ is the only point $z \in \mathcal{D}$ such that $\phi(D) = z \bmod \Lambda$. If $P_0$ is a base point in $\mathcal{C}$, the *hyperelliptic logarithm of* $P$ is the hyperelliptic logarithm of $P - P_0$.

Note that these hyperelliptic logarithms are not the same as those logarithms in Chapter 3, Sections 3.5 and 3.6. There we mapped the group of $S$-units into the reals or a $p$-adic field. Since the group of $S$-units cannot be explicitly computed in all cases we need, the logarithms there cannot be computed explicitly either and we

conformed ourselves with estimates given by Matveev, Győry and Yu for them. In the present chapter, we are concerned with the group $J(\mathbb{Q})$. We will map its generators to $\mathbb{C}^2$ modulo the period lattice. In this case, we can explicitly compute the period lattice and the values of the logarithms of the generators of $J(\mathbb{Q})$ to high precision with the algorithms given in Chapter 5 as we will see below.

Assume for a moment that $P_0 = (a, 0)$ where $a$ is one of the roots of $f$. If $P_0$ is not of that form, we choose one root $a$ of $f$ and define $P_1 = (a, 0)$ and we note that

$$\phi(P) = \left(\int_{P_1}^{P} \phi_1, \int_{P_1}^{P} \phi_2\right) - \left(\int_{P_1}^{P_0} \phi_1, \int_{P_1}^{P_0} \phi_2\right).$$

Let $(x, y)$ be the coordinates of $P$. We recall that the vector

$$\left(\int_{P_0}^{P} \phi_1, \int_{P_0}^{P} \phi_2\right)$$

is well defined independently of the choice of a path connecting $P_0$ to $P$ up to an element of $\Lambda$. We can assume for simplicity that $y > 0$, as the divisor $(x, y)+(x, -y)-2P_0$ is linearly equivalent to $0$, and then $\phi(\imath(P)) = -\phi(P)$, where $\imath$ denotes the hyperelliptic involution $(x, y) \mapsto (x, -y)$. If $x \geq a$ and $y > 0$ we will choose as a path the following: for $t \in [a, x]$ let $\gamma_t = (t, \sqrt{f(t)})$, where if $f(t) \geq 0$ we take the usual positive square root of $f(t)$, and if $f(t) < 0$ we choose $i\sqrt{-f(t)}$ as the square root of $f(t)$. We choose a similar path from $P_0$ to $P$ when $x < a$ and $y > 0$. Note that if $b$ is the nearest root of $f$ that is less or equal than $x$, then

$$\phi(P) = \left(\int_a^b \frac{dt}{\sqrt{f(t)}}, \int_a^b \frac{t\, dt}{\sqrt{f(t)}}\right) + \left(\int_b^x \frac{dt}{\sqrt{f(t)}}, \int_b^x \frac{t\, dt}{\sqrt{f(t)}}\right) \bmod \Lambda. \tag{5.2.1}$$

The first vector in the right hand side is a sum of half-periods computable by Bost and Mestre's algorithm. In particular,

$$2\phi(P) = 2\left(\int_b^x \phi_1, \int_b^x \phi_2\right) \bmod \Lambda.$$

Thus we only need to be able to compute integrals of the form

$$\int_a^x \frac{S(t)dt}{\sqrt{|f(t)|}}, \tag{5.2.2}$$

where $a$ is a root of $f$, $x \geq a$, and $x$ smaller than the roots of $f$ which are $> a$. Bost and Mestre say that a convenient modification of the algorithm given for the computation of the half-periods allows one to compute the integrals

$$\int_a^b \frac{S(t)dt}{\sqrt{|f(t)|}},$$

for arbitrary real numbers $a$ and $b$. We have done the required modifications to compute the integrals of the form (5.2.2) and the details are also given in Chapter 4.

## 5.3 The linear form in hyperelliptic logarithms

Stroeker and Tzanakis [47] describe a method for finding all the integral points on an elliptic curve by estimating a linear form in elliptic logarithms. They transformed the information provided by the Mordell–Weil group of the elliptic curve into a linear form and they gave estimates for it. What they did in the elliptic case, we want to do in the hyperelliptic case. In this section we explain how we transform the information provided by the Mordell–Weil group $J(\mathbb{Q})$ into a linear form in hyperelliptic logarithms and how we can give estimates for it.

We assume the existence of a rational point $P_0 \in \mathcal{C}(\mathbb{Q})$. As mentioned in the Introduction, if we do not know a rational point on the curve, it is possible that there are no rational points at all, and that this can be proved using the techniques of Bruin and Stoll [9, 10, 11].

We will make use of the Abel–Jacobi map

$$\jmath : \mathcal{C} \to J(\mathbb{Q}), \quad \jmath(P) = P - P_0.$$

Then, for any $P \in \mathcal{C}(\mathbb{Q})$ there exist rational integers $m_1, \ldots, m_r$ such that

$$\jmath(P) = \sum m_i D_i + T, \tag{5.3.1}$$

where $\{D_1, \ldots, D_r\}$ is a set of generators of the free part of the Mordell–Weil group $J(\mathbb{Q})$ and $T$ is a torsion element of the finite torsion subgroup $J(\mathbb{Q})_{\text{tors}}$.

Let $P$ be an integral point in $\mathcal{C}(\mathbb{Q})$, and let $M$ be the maximum of the $m_i$ from Equation (5.3.1). We want to find a small upper bound for $M$ so that we can compute linear combinations of the generators of the Mordell–Weil group with small coefficients and decide which of those come from integral points on the curve. With the tools developed in Chapter 3 we can find an upper bound for $M$ as we explain in what follows in this section, though in practice this bound will be very large. The next section will explain how we can improve the bound.

We also want to use the information provided by Equation (5.3.1) numerically, in a similar way as it is done in the elliptic case in [47]. As explained in the last section, we can compute the images of points in $\mathcal{C}(\mathbb{R})$ under the isomorphism $\phi : \mathrm{Pic}^0(\mathcal{C}) \to \mathbb{C}^2/\Lambda$ with the tools from the previous section, as long as we are given a model over the reals for our hyperelliptic curve defined by a degree $6$ polynomial with $6$ real roots. This is possible in the degree $5$ case if the polynomial $f$ defining $\mathcal{C}$ has real roots only, as a linear transformation in $X$ of the form $1/(X + a)$ and the associated transformation in $Y$ will give a model of a curve defined by a degree $6$ polynomial with real roots only as long as $a$ is not one of the roots of $f$. We will then assume that those conditions are satisfied. We will transform the relation in Equation (5.3.1) into a linear form in hyperelliptic logarithms.

The method for obtaining the linear forms and for bounding $M$ depends on whether the degree of $f$ is $5$ or $6$.

### 5.3.1 The odd degree case

When the polynomial $f$ has degree $5$, then the point at infinity of $\mathcal{C}$ is defined over $\mathbb{Q}$, so it will be our choice for $P_0$.

Let $P$ be an integral point on $\mathcal{C}$. Using Theorem 3.7.1 we can find an upper bound $B$ on the size of $X(P)$. We will transform that bound into a bound for $M$. We first will transform the bound for the height of $X(P)$ into a bound for the height of $\jmath(P)$. Recall that the height of $\jmath(P)$ is the height of the corresponding point in the Kummer

surface. In order to explicitly compute that height, we need to transform our curve into a curve defined by a degree $6$ polynomial. We do it by means of the linear transformation $X' = 1/X$ and the associated transformation of $Y$, $Y' = Y/X^3$, if the point $(0,0)$ does not belong to $\mathcal{C}$. Otherwise we need to choose $X' = 1/(X+a)$, where $a$ is not one of the roots of $f$. Let $f_0, \ldots, f_5 \in \mathbb{Z}$ be the coefficients of the polynomial $f$ defining $\mathcal{C}$. The new curve is then given by

$$Y'^2 = f_5 X' + f_4 X'^2 + f_3 X'^3 + f_2 X'^4 + f_1 X'^5 + f_0 X'^6.$$

Then, the point $P_0$ corresponds to $X' = 0, Y' = 0$. Assume that $X(P) \neq 0$. Then the divisor $\jmath(P) = P - \infty = P + \infty - 2\infty$ corresponds to $P' + (0,0) - \infty_+ - \infty_-$, where $P' = (X'(P), Y'(P))$. Then, $\jmath(P)$ is the following point in the Kummer surface, according to the formulae given in Chapter 2:

$$(1, X'(P), 0, f_5/X'(P)) = (1, 1/X(P), 0, f_5 X(P)) = (X(P), 1, 0, f_5 X(P)^2).$$

Then, if $P$ is an integral point with $X(P) \neq 0$, we have

$$h(\jmath(P)) = \log(|f_5| X(P)^2) = \log|f_5| + 2\log|X(P)| = \log(|f_5|) + 2\,\mathrm{h}(X(P)). \quad (5.3.2)$$

We will need the following lemma to bound the size of $M$ in terms of $B$. The proof is identical to the corresponding result in the elliptic case [47, Inequality 1].

**Lemma 5.3.1.** *Denote by $\mathcal{H}$ the height pairing matrix for the Mordell–Weil basis $\{D_1, \ldots, D_r\}$ (see Section 2.3 for its definition) and let $\lambda_1, \ldots, \lambda_r$ be its eigenvalues. Let $\mu_3 = \min_i\{\lambda_i\}$. Let $P \in \mathcal{C}(\mathbb{Q})$ be expressed as in* (5.3.1)*. Then*

$$\hat{h}(\jmath(P)) \geq \mu_3 \max_{1 \leq i \leq r} m_i^2, \quad (5.3.3)$$

*Proof.* We can write $\mathcal{H} = N^t \Lambda N$, where $N$ is orthogonal and $\Lambda$ is the diagonal matrix with diagonal entries $\lambda_i$. Write $\mathbf{x} = N\mathbf{m}$. Then

$$\hat{h}(\jmath(P)) = \mathbf{m}^t \mathcal{H} \mathbf{m} = \mathbf{x}^t \Lambda \mathbf{x} \geq \mu_3 \|\mathbf{x}\|^2 = \mu_3 \|\mathbf{m}\|^2 \geq \mu_3 \max_{1 \leq i \leq r} m_i^2.$$

□

We will now find an upper bound for $M$. We require a lower bound for the height difference as in (2.2.1).

**Lemma 5.3.2.** *Let $B$ be an upper bound for the height of the integral points on $\mathcal{C}$. Let $P$ be an integral point on $\mathcal{C}$. Express $\jmath(P)$ as in* (5.3.1). *Write $M = \max_i m_i$. Then*

$$M \leq \sqrt{\mu_3^{-1}\,(\log|f_5| + 2B - \mu_1)},$$

*where $\mu_1$ is a lower bound for the height difference $h(Q) - \hat{h}(Q)$.*

*Proof.* From Equation (5.3.2) we see that

$$h(\jmath(P)) \leq \log|f_5| + 2B.$$

Now, using the lower bound for the height difference we have

$$\hat{h}(\jmath(P)) \leq \log|f_5| + 2B - \mu_1.$$

Finally, form the previous Lemma we infer that

$$\mu_3 M^2 \leq \log|f_5| + 2B - \mu_1,$$

which proves the Lemma. □

In order to reduce the bound for $M$ to manageable proportions, we will turn the linear combination (5.3.1) into a linear form in the hyperelliptic logarithms of the $D_i$s, in a similar way as it is done in the elliptic case [47]. From now on, for a degree zero divisor $D$ we will write $\phi(D)$ for the hyperelliptic logarithm of $D$, that is, we choose a representative for $\phi(D) \in \mathbb{C}^2/\Lambda$ in the fundamental parallelogram generated by $\omega_1, \omega_2, \omega_3$ and $\omega_4$, where these vectors are defined as in the previous section. We note that, since $\phi$ is an isomorphism, then

$$\phi(nD) = n\phi(D) \qquad (\mathrm{mod}\ \Lambda).$$

Now, $n\phi(D)$ is in the parallelogram generated by the vectors $n\omega_i$ and then there exist integers $n_i$ with $|n_i| \leq |n|$ such that

$$\phi(nD) = n\phi(D) + n_1\omega_1 + n_2\omega_2 + n_3\omega_3 + n_4\omega_4. \tag{5.3.4}$$

Similarly, if $D_1, \ldots, D_n$ are degree zero divisors, and $m_1, \ldots m_n$ are integers, then the point

$$\sum_{i=1}^{n} m_i \phi(D_i)$$

is inside the parallelogram generated by the vectors $(|m_1| + \cdots + |m_n|)\omega_i$ or one of its translations which have the origin as one of its vertices. Then there are integers $n_1, n_2, n_3, n_4$ such that

$$\phi\left(\sum_i D_i\right) = \sum m_i \phi(D_i) + n_1\omega_1 + n_2\omega_2 + n_3\omega_3 + n_4\omega_4, \tag{5.3.5}$$

with $|n_i| \leq |m_1| + \cdots + |m_n|$.

We recall that if $Q = (x, y)$ is a real point on $\mathcal{C}$, then

$$\phi(Q) = \left(\int_x^a \frac{dt}{\sqrt{f(t)}}, \int_x^a \frac{t\, dt}{\sqrt{f(t)}}\right) + \omega,$$

where $a$ is the smallest of the real roots of $f$ that are $\geq x$, or $a = \infty$ if $x$ is greater or equal than all the roots of $f$, and $\omega$ is a sum of half periods of $\mathcal{C}$, as we noted in page 97. Then, if $D = P_1 + P_2 - 2\infty$ and $P_1, P_2$ are real points on $\mathcal{C}$, we have that $\phi(2D)$ is in $\mathbb{R}^2/\Lambda'$, where $\Lambda' = \mathbb{R}^2 \cap \Lambda$. We also note that if $P$ is an integral point and $X(P)$ is larger than all the roots of $f$, then

$$\phi(P) = \left(\int_{X(P)}^{\infty} \frac{dt}{\sqrt{f(t)}}, \int_{X(P)}^{\infty} \frac{t\, dt}{\sqrt{f(t)}}\right)$$

is also in $\mathbb{R}^2/\Lambda'$. Over $\mathbb{R}$, the curve $\mathcal{C}$ consists of two compact components and a non compact component, which includes the point $(\alpha_5, 0)$, where $\alpha_5$ is the largest of the roots of $f$. We can compute easily integral points belonging to the compact components of $\mathcal{C}(\mathbb{R})$ by a direct search. We will only consider then the problem of finding integral points on the infinite component.

**Example 5.3.3.** This is a continuation of Example 4.3.1. Put $f(X) = X^5 - 5X^3 - X^2 + 3X + 1$. As noted in Example 4.3.1 $f$ has real roots only. We computed in that example the integrals we need in this section defining the periods $\omega_1$, $\omega_2$ and the values $\phi(D)$

for the divisors $D_1 = (-1,1) - \infty$, $D_2 = (0,1) - \infty$, and $D_3 = (9/4, 59/32) - \infty$. We have

$$\omega_1 = \begin{pmatrix} 2.691224828589365\ldots \\ -3.120649548992816\ldots \end{pmatrix} \qquad \omega_2 = \begin{pmatrix} 0.773976644907828\ldots \\ 3.624934315790554\ldots \end{pmatrix}$$

$$\frac{\phi(2D_1)}{2} = \begin{pmatrix} 0.664758007760858\ldots \\ -0.537090883853333\ldots \end{pmatrix} \quad \frac{\phi(2D_2)}{2} = \begin{pmatrix} 0.901055347145023\ldots \\ 0.463274675967858\ldots \end{pmatrix}$$

and

$$\phi(D_3) = \begin{pmatrix} 0.301381966139497\ldots \\ 1.624203196148170\ldots \end{pmatrix}.$$

Using `MAGMA` we see that the Mordell–Weil group $J(\mathbb{Q})$ is free of rank $2$ generated by $D_1$ and $D_2$. The divisor $D_3$ equals $2D_1 - 2D_2$. According to what we have discussed in the previous page, there should exist integers $n_1, n_2$ with $|n_i| \leq 2$ such that $\phi(D_3) = \phi(2D_1) - \phi(2D_2) + n_1\omega_1 + n_2\omega_2$. Note that we can check numerically the identity setting $n_1 = 0$ and $n_2 = 1$.

Let $t$ be the order of the torsion subgroup $J(\mathbb{Q})_{\text{tors}}$ and denote by $\tilde{t}$ the least common multiple of $t$ and $2$. In view of Equation (5.3.1), for an integral point $P \in \mathcal{C}$ we have that

$$\tilde{t}_J(P) = \sum m_i \frac{\tilde{t}}{2}(2D_i). \tag{5.3.6}$$

We now apply the homomorphism $\phi$ to this equation and we obtain

$$\tilde{t}\phi(P) \equiv \phi(\tilde{t}_J(P)) \equiv \sum m_i \frac{\tilde{t}}{2}\phi(2D_i) \qquad (\mathrm{mod}\ \Lambda).$$

If, as we have assumed, the divisors $D_i$ are supported by points with real coordinates, and $X(P)$ is larger than all the roots of $f$, then all the $\phi$ values on the previous equation are in $\mathbb{R}^2$ and the equivalence is up to an element in $\Lambda'$. Then there are integers $n_1, n_2$ such that

$$\phi(P) = n_1\frac{\omega_1}{\tilde{t}} + n_2\frac{\omega_2}{\tilde{t}} + \sum m_i \frac{\phi(2D_i)}{2},$$

with $|n_i| \leq \tilde{t}rM/2 + \tilde{t}$ (recall (5.3.4) and (5.3.5)), where $M = \max_i m_i$. Now put

$$\begin{aligned}(L_1(P), L_2(P)) &= (L_1(n_1, n_2, m_1, \ldots, m_r), L_2(n_1, n_2, m_1, \ldots, m_r)) \\ &= n_1 \frac{\omega_1}{\tilde{t}} + n_2 \frac{\omega_2}{\tilde{t}} + \sum m_i \frac{\phi(2D_i)}{2}.\end{aligned}$$

The $L_i$s are the *linear forms in hyperelliptic logarithms* we will estimate in order to reduce our bound for $M$. Let $f \in \mathbb{R}[x]$ and define $c_{16}$ as

$$c_{16}(f) = \max\{1, 2 \max_{\alpha \in \mathbb{C}, f(\alpha)=0} \{|\alpha|\}\}.$$

We will use the following Lemma.

**Lemma 5.3.4.** *Let $\alpha_1, \ldots, \alpha_5$ be the roots of $f$. For all $x \geq c_{16}$*

$$\max\left\{\int_x^\infty \frac{dt}{\sqrt{f(t)}}, \int_x^\infty \frac{t\, dt}{\sqrt{f(t)}}\right\} \leq 2^{7/2}(f_5 x)^{-1/2}.$$

*Proof.* Note that $0 < f(t) = f_5 \prod |t - \alpha_i|$ for every $t \geq x$. Because of our assumption for $x$, we see that $|t - \alpha_i| \geq t - |\alpha_i| \geq t/2$. Then

$$\frac{\sqrt{f_5}}{\sqrt{f(t)}} \leq \left(\frac{t}{2}\right)^{-5/2} \quad \text{and} \quad \frac{t\sqrt{f_5}}{\sqrt{f(t)}} \leq \left(\frac{t}{2}\right)^{-3/2}.$$

We can see then that for large $N$

$$\sqrt{f_5} \int_x^N \frac{dt}{\sqrt{f(t)}} \leq \int_x^N \left(\frac{t}{2}\right)^{-5/2} dt = \frac{2^{7/2}}{3}(x^{-3/2} - N^{-3/2}),$$

and

$$\sqrt{f_5} \int_x^N \frac{tdt}{\sqrt{f(t)}} \leq \int_x^N \left(\frac{t}{2}\right)^{-3/2} dt = 2^{7/2}(x^{-1/2} - N^{-1/2}).$$

Letting $N$ tend to infinity completes the proof. □

We can easily find all the integral points on $\mathcal{C}$ with $X(P) < c_{16}$ by a direct search, as long as $c_{16}$ is not too large ($\leq \exp(15)$). For the remaining points we can find an upper bound for the linear form in hyperelliptic logarithms.

**Lemma 5.3.5.** *If $P$ is an integral point on $\mathcal{C}$ and $X(P) \geq c_{16}$, then*

$$\max\{|L_1(P)|, |L_2(P)|\} \leq 2^{7/2} f_5^{-1/4} e^{-\mu_1/4} e^{-(\mu_3/4)M^2}.$$

*Proof.* Since $c_{16} > 0$, then $X(P)$ is positive. Then either $P$ or $\imath(P)$ has positive $Y$-coordinate, where $\imath$ denotes the hyperelliptic involution. In any case, we recall that $P + \imath(P)$ is linearly equivalent to $2\infty$, and then $\phi(P) = -\phi(\imath(P))$. Assume then that $P$ has positive $Y$-coordinate. Then the integrals defining $\phi(P) = (L_1(P), L_2(P))$ are both positive. The inequality from Lemma 5.3.4 implies

$$\max\{|L_1(P)|, |L_2(P)|\} \leq 2^{7/2} f_5^{-1/2} X(P)^{-1/2}.$$

Now, $X(P)^{-1/2} = e^{-(\log X(P))/2}$, and since $X(P)$ is a positive integer we have $\mathrm{h}(X(P)) = \log(X(P))$. Now, from (5.3.2) and the bounds for the height difference (2.2.1)

$$\mathrm{h}(X(P)) = (h(\jmath(P)) - \log f_5)/2 \geq (\mu_1 + \hat{h}(\jmath(P)) - \log f_5)/2,$$

which implies

$$\max\{|L_1(P)|, |L_2(P)|\} \leq 2^{7/2} {f_5}^{-1/4} e^{-\mu_1/4} \exp(-\hat{h}(\jmath(P))/4).$$

The result now follows from Lemma 5.3.1. □

### 5.3.2 The even degree case

When the polynomial has degree $6$ then the divisor $\infty_- + \infty_+$ is defined over $\mathbb{Q}$, but the point $\infty_+$ is a rational point if and only if the leading coefficient $f_6$ of $f$ is a square. If this is the case we choose $P_0 = \infty_+$. If it is not, then we need to find a rational point $P_0$ on the affine model of $\mathcal{C}$. We note that if $f_6 < 0$, then the curve $\mathcal{C}(\mathbb{R})$ consists of compact closed curves in $\mathbb{R}^2$ and then we can find all integral points on $\mathcal{C}$ by a direct search, as long as the maximum of the absolute value of the roots of $f$ is not very large ($\leq \exp(15)$). We will assume then that $f_6 > 0$.

If the points at infinity are not rational points on $\mathcal{C}$ and $P_0$ is a rational point on $\mathcal{C}$, we will further assume that $X(P_0) = 0$. There is no loss of generality as we now show. Write $P_0 = (m/n, y_0)$ with $y_0 \in \mathbb{Q}$ and $m, n \in \mathbb{Z}$ with $n > 0$ and $(m, n) = 1$. We introduce the change of variables $X' = nX - m$, $Y' = n^3 Y$. Note that $X', Y'$ are

integers if $X, Y \in \mathbb{Z}$. Then, the problem of finding the integral points on $\mathcal{C} : Y^2 = f(X)$ is solved if we can find all the integral points on the curve

$$\mathcal{C}' \quad : \quad Y'^2 = \tilde{f}(X'),$$

where $\tilde{f}(X') = n^6 f((X' + m)/n)$. The point $P_0$ on $\mathcal{C}$ corresponds to the point $P_0' = (0, n^3 y_0)$.

Let $P$ be an integral point on $\mathcal{C}$. We can find an upper bound $B$ for the size of $X(P)$ using the methods from Chapter 3. As in the odd degree case, we want to transform this bound into a bound for $M = \max_i m_i$ in (5.3.1). We need to relate first the height of $X(P)$ to the height of $\jmath(P)$.

**Lemma 5.3.6.** *There is an effectively computable constant $k_1 \in \mathbb{Z}$, with $k_1 > 0$ such that, for all integral points $P$ in $\mathcal{C}$ we have*

$$h(\jmath(P)) \leq \log(k_1 X(P)^3),$$

*whenever $X(P) \neq 0$.*

*Proof.* Assume first that $P_0 = \infty_+$, in particular the integer $f_6$ is a square. The divisor $\jmath(P) = P - \infty_+$ is equal to $P + \infty_- - (\infty_+ + \infty_-)$. Then, according to the formulae for the corresponding point on the Kummer surface given in page 10, the height of $\jmath(P)$ is

$$h(\jmath(P)) = \log \max \left\{ 1, |X(P)|, \left| f_5 X(P)^2 + 2 f_6 X(P)^3 + 2y\sqrt{f_6} \right| \right\}.$$

Let $c_{17} = \max_i |f_i|$. Then, using the triangle inequality we have that $y^2 = f(x) \leq 7c_{17} X(P)^6$, if $X(P) \neq 0$, and then $|y| \leq \sqrt{7c_{17}} |X(P)^3|$. The triangle inequality applied to $f_5 X(P)^2 + 2f_6 X(P)^3 + 2y\sqrt{f_6}$ implies that

$$h(\jmath(P)) \leq \log(9c_{17} |X(P)^3|).$$

Putting $k_1 = 9c_{17}$ completes the proof in this case. Now, in the case that $P_0$ is not one of the points at infinity, $P_0 = (0, y_0)$ with $y_0 \in \mathbb{Z}$. Let $P$ be an integral point on $\mathcal{C}$. We

now want to estimate the height of the corresponding point on the Kummer surface to $\jmath(P) = P - P_0$ which is linearly equivalent to $P + (0, -y_0) - (\infty_+ + \infty_-)$. The formulae given in page 2.1 imply that

$$\jmath(P) = (1, X(P), 0, (2f_0 + f_1 X(P) + 2Y(P)y_0)/X(P)^2).$$

For integral $P$, we can then find a constant $k_1$ in a similar way as we did before for the case $P_0 = \infty_+$. This completes the proof of the Lemma. □

We now can describe explicitly an upper bound for $M$.

**Lemma 5.3.7.** *Let $B$ be an upper bound for the height of the integral points on $\mathcal{C}$. Let $P$ be an integral point on $\mathcal{C}$. Express $\jmath(P)$ as in* (5.3.1)*. Write $M = \max_i m_i$. Then*

$$M \leq \sqrt{\mu_3^{-1}(\log k_1 + 3B - \mu_1)},$$

*where $\mu_1$ is a lower bound for the height difference $h(Q) - \hat{h}(Q)$ and $k_1$ is as in Lemma 5.3.6.*

*Proof.* From Lemma 5.3.6 we have

$$h(\jmath(P)) \leq \log k_1 + 3\log(|X(P)|).$$

As $X(P)$ is an integer, $\log(|X(P)|) = \mathrm{h}(X(P))$. Now the result follows from the lower bound for the height difference and Lemma 5.3.1, as in the proof of Lemma 5.3.2. □

Now, let $D$ be a degree $0$ divisor of the form $P_1 + P_2 - \infty_+ - \infty_-$. We want to compute numerically the hyperelliptic logarithm of $D$ relative to the basis for the period lattice $\omega_1, \omega_2, \omega_3, \omega_4$ defined in Section 5.2. We can do so if $P_1, P_2$ are real points on $\mathcal{C}$. As in the degree $5$ case, we can see that if $P_1, P_2$ are real points, then the value $\phi(2D)$ is in $\mathbb{R}^2/\Lambda'$, where $\Lambda'$ is the lattice generated by the real periods $\omega_1$ and $\omega_2$. We want to use the linear combination given in (5.3.1) and the homomorphism $\phi$ to obtain a linear form in logarithms that we can bound.

Let $t$ be the order of the torsion subgroup $J(\mathbb{Q})_{\text{tors}}$ and let $\tilde{t}$ be the least common multiple of $2$ and $t$. As in the degree $5$ case, we have that

$$\tilde{t}_J(P) = \sum m_i \frac{\tilde{t}}{2}(2D_i).$$

We now work over the Jacobian of the curve defined over $\mathbb{C}$. We add to both sides of the previous equation the degree zero divisor $\tilde{t}(P_0 - \infty_+)$ (note we are adding zero if the base point for the Abel–Jacobi map is $\infty_+$). The equality becomes

$$\tilde{t}(P - \infty_+) = \tilde{t}(P_0 - \infty_+) + \sum m_i \frac{\tilde{t}}{2}(2D_i).$$

We now apply the isomorphism $\phi$ to the last equation and we get

$$\tilde{t}\phi(P-\infty_+) \equiv \phi(\tilde{t}(P-\infty_+)) \equiv \tilde{t}\phi(P_0-\infty_+)+\sum m_i \frac{\tilde{t}}{2}\phi(2D_i) \qquad (\mathrm{mod}\ \Lambda). \quad (5.3.7)$$

Note that if $P$ is an integral point on $\mathcal{C}$ and $|X(P)|$ is at least the maximum of the absolute value of the roots of $f$, then $\phi(P)$ is in $\mathbb{R}^2/\Lambda'$. The integral points with $|X(P)|$ less than the maximum of the absolute value of the roots of $f$ can be found by a direct search. Because of our assumptions for $D_i$, all the $\phi$ values in Equation (5.3.7) have representatives in $\mathbb{R}^2$ and then the equivalence is up to an element in $\Lambda'$. Then there are integers $n_1, n_2$ such that

$$\tilde{t}\phi(P - \infty_+) = \tilde{t}\phi(P_0 - \infty_+) + n_1\omega_1 + n_2\omega_2 + \sum m_i \frac{\tilde{t}}{2}\phi(2D_i),$$

with $|n_i| \leq \tilde{t}rM/2 + 2\tilde{t}$ (recall (5.3.4) and (5.3.5)), where $M = \max_i m_i$. Now put

$$\begin{aligned}(L_1(P), L_2(P)) &= (L_1(n_1, n_2, m_1, \ldots, m_r), L_2(n_1, n_2, m_1, \ldots, m_r)) \\ &= \frac{\phi(2P_0 - 2\infty_+)}{2} + n_1\frac{\omega_1}{\tilde{t}} + n_2\frac{\omega_2}{\tilde{t}} + \sum m_i \frac{\phi(2D_i)}{2}.\end{aligned}$$

The $L_i$s are the linear forms in hyperelliptic logarithms we were after in this degree $6$ case. We will estimate the linear forms by means of the following Lemma.

**Lemma 5.3.8.** *Let $\alpha_1, \ldots, \alpha_6$ be the roots of $f$. For all $x \geq c_{16}$*

$$\max\left\{\int_x^\infty \frac{dt}{\sqrt{f(t)}}, \int_x^\infty \frac{t\ dt}{\sqrt{f(t)}}\right\} \leq 8 f_6^{-1/2} x^{-1},$$

*and for all* $x \leq -c_{16}$

$$\max\left\{\int_{-\infty}^{x} \frac{dt}{\sqrt{f(t)}}, \int_{-\infty}^{x} \frac{|t|dt}{\sqrt{f(t)}}\right\} \leq 8 f_6^{-1/2} |x|^{-1}.$$

*Proof.* The proof is very similar to that of Lemma 5.3.4. We have that $0 < f(t) = f_6 \prod |t - \alpha_i|$ for every $t$ with $|t| \geq |x|$. We also have $|t - \alpha_i| \geq |t| - |\alpha_i| \geq |t|/2$. Then,

$$\sqrt{f_6} \max\left\{\frac{1}{\sqrt{f(t)}}, \frac{|t|}{\sqrt{f(t)}}\right\} \leq \frac{8}{t^2}.$$

Then, for large $N$ and $x \geq c_{16}$,

$$\sqrt{f_6} \int_x^N \frac{dt}{\sqrt{f(t)}} \leq 8 \int_x^N t^{-2} dt = 8(x^{-1} - N^{-1}).$$

Similar relations hold for the other integrals. Letting $N$ tend to infinity completes the proof. □

We can find all the integral points on $\mathcal{C}$ with $|X(P)| < c_{16}$ by a direct search. For the remaining points we can bound the linear form in hyperelliptic logarithms. We will limit ourselves to find integral points with $Y(P)/X(P)^3 > 0$. This roughly means that they are closer to $\infty_+$ than to $\infty_-$. The remaining points are found by changing the sign of $Y$.

**Lemma 5.3.9.** *If $P$ is an integral point on $\mathcal{C}$, with $Y(P)/X(P)^3 > 0$ and $|X(P)| \geq c_{16}$, then*

$$\max\{|L_1(P)|, |L_2(P)|\} \leq 8 f_6^{-1/2} \sqrt[3]{k_1} e^{-\mu_1/3} e^{-(\mu_3/3)M^2},$$

*where $k_1$ is the constant from Lemma 5.3.6 and $\mu_1$ is a lower bound for the height difference.*

*Proof.* Since $|X(P)| \geq c_{16}$ and the sign of $Y(P)$ is the same as the sign of $X(P)$, then

$$\phi(P) = \begin{cases} \left(\int_{X(P)}^{\infty} \frac{dt}{\sqrt{f(t)}}, \int_{X(P)}^{\infty} \frac{t\,dt}{\sqrt{f(t)}}\right), & X(P) > 0, \\ \left(\int_{-\infty}^{X(P)} \frac{dt}{\sqrt{f(t)}}, \int_{-\infty}^{X(P)} \frac{t\,dt}{\sqrt{f(t)}}\right), & X(P) < 0. \end{cases}$$

The inequality from Lemma 5.3.8 implies that

$$\max\{|L_1(P)|, |L_2(P)|\} \leq 8 f_6^{-1/2} |X(P)|^{-1}.$$

Since $X(P)$ is a nonzero integer, $\mathrm{h}(X(P)) = \log(|X(P)|)$. Then $|X(P)|^{-1} = \exp(-\mathrm{h}(X(P)))$. From Lemma 5.3.6 and the bound for the height difference we see that

$$\mathrm{h}(X(P)) \geq (h(\jmath(P)) - \log k_1)/3 \geq (\mu_1 + \hat{h}(\jmath(P)) - \log k_1)/3,$$

which implies

$$\max\{|L_1(P)|, |L_2(P)|\} \leq 8 f_6^{-1/2} \sqrt[3]{k_1} e^{-\mu_1/3} \exp(-\hat{h}(\jmath(P))/3).$$

The result now follows from Lemma 5.3.1. □

## 5.4 Reduction of the upper bound, the LLL-algorithm

As noted in the previous section, the upper bounds we have so far for the size of the coefficients $m_i$ in the equation

$$\jmath(P) = \sum_{i=1}^{r} m_i D_i + T$$

are huge. In this section we explain how to reduce the bound to manageable proportions. The bounds given by Lemmas 5.3.2 and 5.3.5 in the degree $5$ case, and Lemmas 5.3.7 and 5.3.9 in the degree $6$ case, can be rewritten as

$$|L_1(P)|, |L_2(P)| \leq K_1 e^{-K_2 M^2}, \quad M \leq K_3, \tag{5.4.1}$$

where $M = \max_{i=1,\ldots,r} m_i$. Let $\omega_1, \omega_2$ be the real periods of $\mathcal{C}$ generating $\Lambda'$. Write

$$\frac{\omega_i}{\tilde{t}} = (\omega_{i,1}, \omega_{i,2}) \in \mathbb{R}^2, \quad i = 1, 2,$$

and

$$\frac{\phi(2P_0 - 2\infty_+)}{2} = (\alpha_1, \alpha_2) \in \mathbb{R}^2,$$

and

$$\frac{\phi(2D_i)}{2} = (d_{i,1}, d_{i,2}) \in \mathbb{R}^2, quadi = 1, \dots r.$$

For real $r$ we denote by $[r]$ the nearest integer value to $r$, with any fixed convention for reals of the form $(2n+1)/2$, $n \in \mathbb{Z}$. Let $C$ be a 'large' positive integer and consider the matrix

$$\mathcal{A} = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & & \vdots & \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ [Cd_{1,1}] & [Cd_{2,1}] & \cdots & [Cd_{r,1}] & [C\omega_{1,1}] & [C\omega_{2,1}] \\ [Cd_{1,2}] & [Cd_{2,2}] & \cdots & [Cd_{r,2}] & [C\omega_{1,2}] & [C\omega_{2,2}] \end{pmatrix}.$$

The entries of the matrix $\mathcal{A}$ can be computed with the algorithms given in Chapter 4, as explained in Section 5.2. Since the periods $\omega_1$ and $\omega_2$ are linearly independent over $\mathbb{R}$, the matrix $\mathcal{A}$ is non-singular. We will explain later what large $C$ means. The columns of the matrix $\mathcal{A}$ define then a full rank lattice in $\mathbb{R}^{r+2}$.

Let $\mathbf{y}$ be the vector

$$\mathbf{y} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ -[C\alpha_1] \\ -[C\alpha_2] \end{pmatrix}.$$

Let $\mathcal{L}$ be the lattice in $\mathbb{R}^{r+2}$ generated by the columns of $\mathcal{A}$. We define the quantity $\ell(\mathcal{L}, \mathbf{y})$ as follows:

$$\ell(\mathcal{L}, \mathbf{y}) = \begin{cases} \min_{\mathbf{x} \in \mathcal{L}} \|\mathbf{x} - \mathbf{y}\|, & \mathbf{y} \notin \mathcal{L}, \\ \min_{\mathbf{x} \in \mathcal{L} \setminus 0} \|\mathbf{x}\|, & \mathbf{y} \in \mathcal{L}. \end{cases}$$

*Remark.* The vector $\mathbf{y}$ is nonzero only in the case when the polynomial $f$ defining $\mathcal{C}$ has degree $6$ and the point $\infty_+$ is not a rational point on $\mathcal{C}$.

Let $m_1, \dots, m_r, n_1, n_2 \in \mathbb{Z}$. Put $\mathbf{x} = \mathcal{A}\mathbf{z}$, where $\mathbf{z} = (m_1, \dots, m_r, n_1, n_2)$. The last two entries of the vector $\mathbf{x} - \mathbf{y}$ are an approximation of the linear forms in logarithms given above multiplied by the constant $C$. The length of $\mathbf{x} - \mathbf{y}$ is then bounded by above by a constant depending on $C$, $K_1$, $K_2$ and $M$. We can combine this information with the quantity $\ell(\mathcal{L}, \mathbf{y})$. This will result on an improvement on the bound for $M$. Unless we are very unlucky, see below, the following lemma will give an improvement on the bound for $M$ (cf. [42, Lemma VI.1]).

**Lemma 5.4.1.** *Set $T$ to be the constant $T = (rK_3(\tilde{t}+1)+3\tilde{t}+1)/2$. Let $c_{18}$ be a lower bound for $\ell(\mathcal{L}, \mathbf{y})$. If $c_{18}^2 > 2T^2 + rK_3^2$ then,*

$$M \leq \sqrt{\frac{1}{K_2}\left(\log(CK_1) - \log\left(\sqrt{(c_{18}^2 - rK_3^2)/2} - T\right)\right)}.$$

*Proof.* We follow the proof on [42]. Put

$$\Phi_i := [C\alpha_i] + n_1[C\omega_{1,i}] + n_2[C\omega_{2,i}] + \sum_{j=1}^{r} m_j[Cd_{j,i}], \quad i = 1, 2.$$

Notice that

$$|\Phi_i - C(\alpha_i + n_1\omega_{1,i} + n_2\omega_{2,i} + \sum_{j=1}^{r} m_j d_{j,i})| \leq (rK_3 + (rK_3+3)\tilde{t} + 1)/2 = T,$$

(recall $n_1, n_2 \leq (rK_3+3)\tilde{t}/2$) which implies

$$|\Phi_i| \leq T + CK_1 e^{-K_2 M^2}.$$

Now consider the lattice point $\mathbf{x} = \mathcal{A}\mathbf{z}$, where $\mathbf{z} = (m_1, \dots, m_r, n_1, n_2)$, so

$$\mathbf{x} - \mathbf{y} = (m_1, \dots, m_r, \Phi_1, \Phi_2).$$

Then either $\mathbf{x} = \mathbf{y}$ or

$$c_{18}^2 \leq \ell(\mathcal{L}, \mathbf{y}) \leq rK_3^2 + \Phi_1^2 + \Phi_2^2 \leq rK_3^2 + 2(T + CK_1 e^{-K_2 M^2})^2.$$

By assumption, $c_{18}^2 - rK_3^2 \geq 0$, so

$$e^{-K_2 M^2} \geq \frac{1}{CK_1}\left(\sqrt{(c_{18}^2 - rK_3^2)/2} - T\right).$$

Again, by our assumption, the right hand side is positive, and then we can take logarithms of both sides. The result follows. □

A lower bound for $\ell(\mathcal{L}, \mathbf{y})$ can be computed from an LLL-reduced basis for the lattice generated by the column vectors of the matrix $\mathcal{A}$. The following Lemmas ([42, Theorems V.9 and V.10]) give those bounds explicitly.

**Lemma 5.4.2.** *Let $\{\mathbf{b_1}, \ldots, \mathbf{b_{r+2}}\}$ be an LLL-reduced basis for the lattice $\mathcal{L}$. Let $\{\mathbf{b_1}^*, \ldots \mathbf{b_{r+2}}^*\}$ be the Gram–Schmidt basis associated to the $\mathbf{b_i}$s. A lower bound for the minimum of $\mathcal{L}$ is given by*

$$c = \min\{\|\mathbf{b_i}^*\| : i = 1, \ldots, r+2\}.$$

**Lemma 5.4.3.** *Let $B$ be the basis matrix of an LLL-reduced basis for the lattice $\mathcal{L}$. Let $\mathbf{y}' = B^{-1}\mathbf{y}$ and denote by $i_0$ the largest index such that $\mathbf{y}' \neq 0$. A lower bound for $\ell(\mathcal{L}, \mathbf{y})$ is given by*

$$c = \{\mathbf{y}'_{i_0}\}^{-1/2} \min\{\|\mathbf{b_i}^*\| : i = 1, \ldots, r+2\},$$

*where $\{r\}$ denotes the distance from $r \in \mathbb{R}$ to the nearest integer.*

In practice, the constant $\min\{\|\mathbf{b_i}^*\| : i = 1, \ldots, r+2\}$ has norm close to the norm of the first vector of an LLL-reduced basis. It can be argued that the norm of such vector is about of the order of $C^{2/(r+2)}$, since $\mathcal{A}$ has discriminant of the order of $C^2$. Then, if we choose $C$ to be larger than $\left(K_3 \tilde{t} \sqrt{r^2 + r}\right)^{r+2}$ we should expect that the lower bound for $\ell(\mathcal{L}, \mathbf{y})$ satisfies the required inequality in the statements of the previous two lemmas. If it does not, then we choose a larger $C$, so that we can apply the corresponding Lemma.

The ideas involved in the strategy to reduce the bound $M$ are not new. But they had not been implemented in the past because there was not a published algorithm to compute the hyperelliptic logarithms to high precision. There lies the importance of Chapter 4.

In the example we give at the end of the section, the upper bound for $M$ is about $10^{239}$, and $r = 2$. We choose $C$ to be $10^{1000}$, so we need to compute the periods and the values $\phi(2D_i)$ to more than $1000$ digits of precision. With the algorithms given in Chapter 4 we can make the computation to high precision in a short time.

**Example 5.4.4.** Let $\mathcal{C}$ be the curve defined by $Y^2 = f(X) = X^5 - 5X^3 - X^2 + 3X + 1$. Note that $f(X)$ is irreducible over $\mathbb{Q}$ and then an upper bound for the size of the integral points on $\mathcal{C}$ can be computed using the techniques from Chapter 3. We obtain that if $P$ is an integral point on $\mathcal{C}$, then

$$\mathrm{h}(X(P)) \leq 7.02 \times 10^{477}.$$

An upper bound for $M$ is then given by $1.2 \times 10^{239}$ from Lemma 5.3.2. We search for some integral points on $\mathcal{C}$ and we find

$$(X, Y) = (-1, -1),\ (-1, 1),\ (0, -1),\ (0, 1). \tag{5.4.2}$$

We proceed then to the reduction process. Using `MAGMA` [5] we see that $J(\mathbb{Q})$ is free of rank $2$ generated by

$$D_1 = (-1, 1) - \infty, \quad \text{and} \quad D_2 = (0, 1) - \infty.$$

We choose our large constant $C$ to be $10^{1000}$, which is larger than $(2M + 1)^2$. We compute the hyperelliptic logarithms of $2D_1$ and $2D_2$, and the real periods of $\mathcal{C}$ to more than $1000$ digits of precision with the algorithms in Chapter 4 (this was done in Example 4.3.1). We then apply `MAGMA`'s implementation of the LLL-algorithm with the matrix $\mathcal{A}$ given in Lemma 5.4.1 and we get the desired inequality for $c_{18}$. The new bound for $M$ is now $63$. We repeat the process with this new bound and we now get that an upper bound for $M$ is $6$. Searching for integral points using that bound is not difficult and we do not find any more points. We only need to look for integral points with $X(P) \leq 5$, but that region had already been covered by our previous search of points. Therefore, the only integral points on $\mathcal{C}$ are those given in (5.4.2).

The reader can find the MAGMA programs for verifying the above computations at:

http://www.warwick.ac.uk/staff/H.R.Gallegos-Ruiz/programs/hyperlogs/

# Bibliography


[1] A. Baker, *Bounds for the solutions of the hyperelliptic equation*, Proc. Cambridge Philos. Soc. **65** (1969), 439–444.

[2] Yuri Bilu, *Effective analysis of integral points on algebraic curves*, Israel J. Math. **90** (1995), no. 1-3, 235–252.

[3] Yuri F. Bilu, *Quantitative Siegel's theorem for Galois coverings*, Compositio Math. **106** (1997), no. 2, 125–158.

[4] Yuri F. Bilu and Guillaume Hanrot, *Solving superelliptic Diophantine equations by Baker's method*, Compositio Math. **112** (1998), no. 3, 273–312.

[5] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993).

[6] Jean-Benoît Bost and Jean-François Mestre, *Moyenne arithmético-géométrique et périodes des courbes de genre* $1$ *et* $2$, Gaz. Math. (1988), no. 38, 36–64.

[7] N. R. Bruin, *Chabauty methods and covering techniques applied to generalized Fermat equations*, CWI Tract, vol. 133, Stichting Mathematisch Centrum Centrum voor Wiskunde en Informatica, Amsterdam, 2002, Dissertation, University of Leiden, Leiden, 1999.

[8] Nils Bruin, *Chabauty methods using elliptic curves*, J. Reine Angew. Math. **562** (2003), 27–49.

[9] Nils Bruin and Michael Stoll, *Deciding existence of rational points on curves: an experiment*, Experiment. Math. **17** (2008), no. 2, 181–189.

[10] ———, *Two-cover descent on hyperelliptic curves*, Math. Comp. **78** (2009), no. 268, 2347–2370.

[11] Nils Bruin and Michael Stoll, *The Mordel–Weil sieve: proving non-existence of rational points on curves*, LMS Journal of Computation and Mathematics **13** (2010), no. -1, 272–306.

[12] Yann Bugeaud, *Bounds for the solutions of superelliptic equations*, Compositio Mathematica **107** (1997), 187–219.

[13] Yann Bugeaud and Kálmán Győry, *Bounds for the solutions of unit equations*, Acta Arithmetica **LXXIV** (1996), no. 1, 67–80.

[14] Yann Bugeaud and Kálmán Győry, *Bounds for the solutions of Thue-Mahler equations and norm form equations*, Acta Arith. **74** (1996), no. 3, 273–292.

[15] Yann Bugeaud, Maurice Mignotte, Samir Siksek, Michael Stoll, and Szabolcs Tengely, *Integral points on hyperelliptic curves*, Algebra & Number Theory **2** (2008), no. 8, 859–885.

[16] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus* $2$, London Mathematical Society Lecture Note Series, vol. 230, Cambridge University Press, Cambridge, 1996.

[17] Claude Chabauty, *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité*, C. R. Acad. Sci. Paris **212** (1941), 882–885.

[18] David A. Cox, *Gauss and the arithmetic-geometric mean*, Notices Amer. Math. Soc. **32** (1985), no. 2, 147–151.

[19] Régis Dupont, *Moyenne arithmético-géométrique, suites de Borchardt et applications*, Ph.D. thesis, École Polytechnique, 1997.

[20] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366.

[21] E. V. Flynn, *The group law on the Jacobian of a curve of genus* $2$, J. Reine Angew. Math. **439** (1993), 45–69.

[22] E. V. Flynn and N. P. Smart, *Canonical heights on the Jacobians of curves of genus* $2$ *and the infinite descent*, Acta Arith. **79** (1997), no. 4, 333–352.

[23] E. Victor Flynn and Joseph L. Wetherell, *Finding rational points on bielliptic genus* $2$ *curves*, Manuscripta Math. **100** (1999), no. 4, 519–533.

[24] ———, *Covering collections and a challenge problem of Serre*, Acta Arith. **98** (2001), no. 2, 197–205.

[25] Homero R. Gallegos-Ruiz, $s$*-integral points on hyperelliptic curves*, To appear in The International Journal of Number Theory, $\geq$ 2010.

[26] Phillip Griffiths and Joseph Harris, *Principles of algebraic geometry*, Wiley Classics Library, John Wiley & Sons Inc., New York, 1994, Reprint of the 1978 original.

[27] Kálmán Győry and Kunrui Yu, *Bounds for the solutions of* $S$*-unit equations and decomposable form equations*, Acta Arith. **123** (2006), no. 1, 9–41.

[28] H.W. Lenstra Jr., *Algorithms in algebraic number theory*, Bulletin of the American Mathematical Society **26** (1992), no. 2, 211–244.

[29] Edmund Landau, *Verallgemeinerung eines polyaschen satzes auf algebraische zahlkörper*, Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch–Physikalische Klasse (1918), 478–488.

[30] Serge Lang, *Algebraic number theory*, second ed., Graduate Texts in Mathematics, vol. 110, Springer-Verlag, New York, 1994.

[31] E. M. Matveev, *An explicit lower bound for a homogeneous rational form in logarithms of algebraic numbers. II*, Izv. Ross. Acad. Nauk Ser. Mat. **64** (2000), no. 6, 125–180, English translation in Izv. Math. **64** (2000), no. 6, 1217–1269.

[32] William McCallum and Bjorn Poonen, *The method of Chabauty and Coleman*, http://www-math.mit.edu/~poonen/papers/chabauty.pdf, June 2010.

[33] David Mumford, *Tata lectures on theta. I*, Modern Birkhäuser Classics, Birkhäuser Boston Inc., Boston, MA, 2007, With the collaboration of C. Musili, M. Nori, E. Previato and M. Stillman, Reprint of the 1983 edition.

[34] ———, *Tata lectures on theta. II*, Modern Birkhäuser Classics, Birkhäuser Boston Inc., Boston, MA, 2007, Jacobian theta functions and differential equations, With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura, Reprint of the 1984 original.

[35] Bjorn Poonen and Edward F. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*, J. Reine Angew. Math. **488** (1997), 141–188.

[36] Dimitrios Poulakis, *Solutions entières de l'équation* $Y^m = f(X)$, Sém. Théor. Nombres Bordeaux (2) **3** (1991), no. 1, 187–199.

[37] Edward F. Schaefer, $2$*-descent on the Jacobians of hyperelliptic curves*, J. Number Theory **51** (1995), no. 2, 219–232.

[38] ———, *Computing a Selmer group of a Jacobian using functions on the curve*, Math. Ann. **310** (1998), no. 3, 447–471.

[39] Jean-Pierre Serre, *Lectures on the Mordell-Weil theorem*, Aspects of Mathematics, E15, Friedr. Vieweg & Sohn, Braunschweig, 1989, Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt.

[40] Carl L. Siegel, *Über einige Anwendungen diophantischer Approximationen*, Abh. Pr. Akad. Wiss. (1929), no. 1.

[41] Joseph H. Silverman, *The difference between the Weil height and the canonical height on elliptic curves*, Math. Comp. **55** (1990), no. 192, 723–743.

[42] Nigel P. Smart, *The algorithmic resolution of Diophantine equations*, London Mathematical Society Student Texts, vol. 41, Cambridge University Press, Cambridge, 1998.

[43] V. G. Sprindžuk, *The arithmetic structure of integer polynomials and class numbers*, Trudy Mat. Inst. Steklov. **143** (1977), 152–174, 210, Analytic number theory, mathematical analysis and their applications (dedicated to I. M. Vinogradov on his 85th birthday).

[44] Michael Stoll, *On the height constant for curves of genus two*, Acta Arith. **90** (1999), no. 2, 183–201.

[45] ———, *Implementing $2$-descent for Jacobians of hyperelliptic curves*, Acta Arith. **98** (2001), no. 3, 245–277.

[46] ———, *On the height constant for curves of genus two. II*, Acta Arith. **104** (2002), no. 2, 165–182.

[47] R. J. Stroeker and N. Tzanakis, *Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms*, Acta Arith. **67** (1994), no. 2, 177–196.

[48] L. A. Trelina, *$S$-integral solutions of Diophantine equations of hyperbolic type*, Dokl. Akad. Nauk BSSR **22** (1978), no. 10, 881–884, 955.

[49] P. M. Voutier, *An upper bound for the size of integral solutions to $y^m = f(x)$*, J. Number Theory **53** (1995), no. 2, 247–271.

[50] ———, *An effective lower bound for the height of algebraic numbers*, Acta Arithmetica **LXXIV** (1996), no. 1, 81–95.

[51] Michel Waldschmidt, *Diophantine approximation on linear algebraic groups*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 326, Springer-Verlag, Berlin, 2000, Transcendence properties of the exponential function in several variables.

[52] Wolfram Research, Inc., *Mathematica Edition: Version 7.0*, 2008.

[53] Kunrui Yu, *$p$-adic logarithmic forms and group varieties. III*, Forum Math. **19** (2007), no. 2, 187–280.