Discrete and Complex Algorithms for Curves

Lynn Chua

Electrical Engineering and Computer Sciences
University of California at Berkeley

Technical Report No. UCB/EECS-2020-42
http://www2.eecs.berkeley.edu/Pubs/TechRpts/2020/EECS-2020-42.html

May 11, 2020

Discrete and Complex Algorithms for Curves

by

Lynn Chua

A dissertation submitted in partial satisfaction of the

requirements for the degree of

Doctor of Philosophy

in

Computer Science

in the

Graduate Division

of the

University of California, Berkeley

Committee in charge:

Professor Alessandro Chiesa, Co-chair
Professor Bernd Sturmfels, Co-chair
Professor Kenneth Ribet

Spring 2020

The dissertation of Lynn Chua, titled Discrete and Complex Algorithms for Curves, is approved:

Co-chair ______________________________ Date ____________

Co-chair ______________________________ Date ____________

______________________________ Date ____________

University of California, Berkeley

Discrete and Complex Algorithms for Curves

Abstract

Discrete and Complex Algorithms for Curves

by

Lynn Chua

Doctor of Philosophy in Computer Science

University of California, Berkeley

Professor Alessandro Chiesa, Co-chair

Professor Bernd Sturmfels, Co-chair

This dissertation consists of two parts. The first part pertains to the Schottky problem, which asks to characterize Jacobians of curves amongst abelian varieties. This has a complete solution only in the first non-trivial case where the genus is four, and the solution is described in terms of the Riemann theta function. We first present a Julia package for numerical evaluations of the Riemann theta function. We then describe numerical approaches to the Schottky problem in genus four and five. We present a solution to a variant of the Schottky problem in genus five, for Jacobians with a vanishing theta null. Finally, we describe solutions to the tropical Schottky problem, and relate the tropical and classical solutions to the Schottky problem in genus four.

The second part of this dissertation relates to cryptography. We first study cycles of pairing-friendly elliptic curves, for an application in pairing-based cryptography. We next study the concrete security of the Learning With Errors problem in lattice-based cryptography, when sampling the secret from a non-uniform, small distribution.

To my parents.

Contents

Acknowledgments

This thesis would not have been possible without the support of many people.

First and foremost, I would like to thank my advisors Bernd Sturmfels and Alessandro Chiesa, for their continual support and guidance throughout the past five years. They gave me freedom to pursue my interests, while shaping me as a researcher, and they were always available for me whenever I needed help. I would also like to thank Ken Ribet and Prasad Raghavendra for being on my dissertation or qualifying exam committees.

The results presented in this thesis were derived in collaboration with my collaborators, namely Daniele Agostini, Barbara Bolognese, Madeline Brandt, Hao Chen, Alessandro Chiesa, Mario Kummer, Kristin Lauter, Yongsoo Song, Bernd Sturmfels, and Matthew Weidner. I would also like to thank Daniel Plaumann, Rainer Sinn and Cynthia Vinzant, with whom I wrote my first paper in graduate school.

I would particularly like to thank the CS theory group at Berkeley, my academic sibilngs in the Berkeley Math department, and the Nonlinear Algebra group at the Max Planck Institute for Mathematics in the Sciences, in Leipzig. In particular, I would like to thank Pasin Manurangsi, Akshayaram Srinivasan, Siqi Liu, Peihan Miao, Nick Spooner, Tarun Kathuria, Aaron Schild, Fatemeh Mohammadi, Bo Lin, Carlos Améndola, Kathlén Kohn, Anna Seigal, Nidhi Kaihnsa, Mahsa Sayyary Namin, Diego Cifuentes, Türkü Özlüm Çelik, and Emre Sertöz.

Last but not least, I would like to thank Guang Hao Low and my parents for their unwavering love and support.

Chapter 1

Overview

In this dissertation, we present a collection of results which lie in the interface of computer science and mathematics. In the first part, we describe numerical algorithms for the Schottky problem, which asks to characterize Jacobians of curves amongst abelian varieties. We study both the classical Schottky problem, which relates to complex Riemann surfaces, and the tropical Schottky problem, which relates to tropical geometry. In the second part, we present a work on constructing elliptic curves for an application in cryptography, and another work on studying the concrete security parameters in lattice-based cryptography. The term "discrete" in the title of this dissertation refers to our study of curves over finite fields for cryptography, and fields of valuation in tropical geometry. The term "complex" in the title refers to our study of curves over the field of complex numbers in the classical Schottky problem.

1.1 Numerical algorithms for the Schottky problem

Riemann theta function

The *Riemann theta function* is the holomorphic function

$$\theta\colon \mathbb{C}^g \times \mathbb{H}_g \to \mathbb{C}\,, \qquad \theta(z,\tau) = \sum_{n\in\mathbb{Z}^g} \exp\left(\pi i n^t \tau n + 2\pi i n^t z\right) \tag{1.1.1}$$

where $\mathbb{H}_g$ is the *Siegel upper-half space*, which consists of all complex symmetric $g \times g$ matrices with positive definite imaginary part (see [94] for more details). In [3], we present a new package `Theta.jl` for numerical evaluations of theta functions, programmed in Julia. Our package is specialized for multiple evaluations of theta functions for the same Riemann matrix $\tau \in \mathbb{H}_g$ and different z, for small genus g. Our implementation is based on the algorithm from [52], which we extend to support computations of theta functions with characteristics and derivatives of arbitrary order. This is described in Chapter 2.

Classical Schottky problem

Given an algebraic curve C of genus g, we can associate with it an abelian variety which we call the Jacobian of the curve. The Schottky problem asks to characterize Jacobians of genus g curves amongst all abelian varieties of dimension g. If the curve C is defined over the complex numbers, then its Jacobian is a complex lattice of dimension g, defined by a matrix which we call the Riemann matrix. More generally, complex abelian varieties of dimension g are parametrized by the Siegel upper-half space $\mathbb{H}_g$, which consists of all complex symmetric $g \times g$ matrices with positive definite imaginary part. We refer the interested reader to the survey [70] and the textbook [26] for more details.

The Schottky locus is the subset of matrices in $\mathbb{H}_g$ that represent Jacobians. For $g = 1, 2, 3$, essentially all abelian varieties of dimension g are Jacobians of genus g curves. For $g \geq 4$, the inclusion is proper. The case where $g = 4$ was completely solved by Schottky and Igusa [75], who constructed a polynomial of degree 16 in theta constants defining the Schottky locus. However, the Schottky problem for $g \geq 5$ is still open, with only partial solutions [1, 59].

In joint work with Kummer and Sturmfels, we construct algorithms for the Schottky problem in genus four [43]. In [3], we describe numerical approaches for studying the Schottky problem in genus five. In particular, we use our package `Theta.jl` to compute the equations in [1, 59] which give a weak solution to the Schottky problem in genus five. These equations consist of products of many *theta constants*, which are theta functions evaluated at $z = 0$. These algorithms are described in Chapter 3.

We also present a solution to a variant of the weak Schottky problem in genus five, for Jacobians with a vanishing theta null [4]. This is described in Chapter 4.

Tropical Schottky problem

Curves, their Jacobians, and the Schottky locus have natural counterparts in the combinatorial setting of tropical geometry. For an introduction to tropical geometry, we refer to the textbook [86]. A tropical curve is a connected metric graph, and a tropical Jacobian is defined by a real symmetric and positive definite matrix. We describe the process of going from a curve to its tropical Jacobian and back, in joint work with Bolognese and Brandt [27].

In [43], we study the tropical Schottky locus in genus four, implementing algorithms for solving the tropical Schottky problem. We construct algorithms for recovering a tropical curve from its tropical Jacobian. We also relate the classical and tropical solutions to the genus four Schottky problem, by tropicalizing the modular form that defines the classical Schottky locus, and showing that the resulting tropical modular forms contain the tropical Schottky locus. This work is described in Chapter 5.

1.2 Elliptic curve cryptography

Many cryptography schemes today are constructed based on the hardness of the discrete logarithm problem, which is usually instantiated using elliptic curves. Together with Chiesa and Weidner [41], we study *cycles* of *pairing-friendly elliptic curves*. These are lists of elliptic curves defined over finite fields, such that the number of points on one curve equals the size of the field of definition of the next, in a cyclic way. Cycles are used in [21] to achieve recursive composition of *zkSNARKs* (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge). A zkSNARK is a cryptographic scheme that allows one party (the prover) to convince another party (the verifier) that the prover knows a certain secret, via a short proof that is cheap to verify and reveals no information about the secret.

Efficient zkSNARK constructions are obtained via pairing-friendly elliptic curves, and the cycle condition enables their recursive composition, while avoiding expensive modular arithmetic across fields of different characteristics. In [41], we initiate a systematic study of pairing-friendly cycles. We characterize all possibilities for cycles from the known families of pairing-friendly elliptic curves, while ruling out cycles under various assumptions. This is described in Chapter 6.

1.3 Lattice-based cryptography

Lattice-based cryptography is one of the leading candidates for *post-quantum* cryptography, i.e. cryptography which is resistant to attacks by quantum computers. In particular, many lattice-based cryptography schemes are based on the hardness of the *Learning With Errors (LWE)* problem [100].

Together with Chen, Lauter and Song from Microsoft Research, we conduct a systematic experimental study of the concrete security of LWE with small secret [38]. Our main motivation is to investigate the security parameters in the setting of *homomorphic encryption*. Homomorphic encryption allows computations on encrypted data, and its security is based on the LWE problem. For practical implementations of homomorphic encryption schemes, it is important to understand the concrete security levels of LWE. While there are various known security estimates, there is still a significant gap between our theoretical understanding of the performance of lattice reduction algorithms and their practical performance. We discuss this work in Chapter 7.

Part I

Numerical algorithms for the Schottky problem

Chapter 2

Riemann theta function

In this chapter, we introduce the Riemann theta function, and describe numerical algorithms for approximating it. We also present a new package `Theta.jl` for numerical computations of theta functions, programmed in Julia [25]. The material in this section is from the paper "Computing Theta Functions with Julia" authored with Daniele Agostini, and has been submitted for publication [3].

2.1 Definitions

The *Riemann theta function* is the holomorphic function

$$\theta\colon \mathbb{C}^g \times \mathbb{H}_g \to \mathbb{C}\,, \qquad \theta(z,\tau) = \sum_{n\in\mathbb{Z}^g} \mathbf{e}\left(\frac{1}{2}n^t\tau n + n^t z\right) \tag{2.1.1}$$

where $\mathbf{e}(x) = e^{2\pi i x}$ and $\mathbb{H}_g$ is the *Siegel upper-half space*, which consists of all complex symmetric $g \times g$ matrices with positive definite imaginary part. We define theta functions with characteristics as follows. A *characteristic* is an element $m \in (\mathbb{Z}/2\mathbb{Z})^{2g}$, which we represent as a vector $m = \begin{bmatrix}\varepsilon\\ \delta\end{bmatrix}$ where $\varepsilon, \delta \in \{0,1\}^g$. The *Riemann theta function with characteristic* m is defined as

$$\theta[m](z,\tau) = \theta\begin{bmatrix}\varepsilon\\ \delta\end{bmatrix}(z,\tau) = \sum_{n\in\mathbb{Z}^g} \mathbf{e}\left(\frac{1}{2}\left(n+\frac{\varepsilon}{2}\right)^t \tau \left(n+\frac{\varepsilon}{2}\right) + \left(n+\frac{\varepsilon}{2}\right)^t\left(z+\frac{\delta}{2}\right)\right) \tag{2.1.2}$$

and it is a holomorphic function $\theta[m]\colon \mathbb{C}^g \times \mathbb{H}_g \to \mathbb{C}$. The Riemann theta function in (2.1.1) is a special case of (2.1.2), where the characteristic is the all-zero vector. The *sign* of a characteristic m is defined as $e(m) = (-1)^{\varepsilon^t\delta}$, and we call a characteristic *even* or *odd* if the sign is 1 or -1 respectively. As a function of z, $\theta[m](z,\tau)$ is even (respectively odd) if and only if the characteristic m is even (respectively odd). There are $2^{g-1}(2^g+1)$ even theta characteristics and $2^{g-1}(2^g-1)$ odd theta characteristics.

The *theta constants* are the functions on $\mathbb{H}_g$ obtained by evaluating the theta functions with characteristics at $z = 0$,

$$\theta[m](\tau) = \theta[m](0, \tau) . \tag{2.1.3}$$

Theta constants corresponding to odd characteristics vanish identically.

The theta function satisfies a *heat equation* [26, Proposition 8.5.5],

$$\frac{\partial^2 \theta[m]}{\partial z_j \partial z_k} = (1 + \delta_{jk}) \cdot 2\pi i \frac{\partial \theta[m]}{\partial \tau_{jk}} , \tag{2.1.4}$$

where δ_{jk} is 1 if $j = k$ and 0 otherwise.

Moreover, theta functions have some remarkable symmetries. First of all, they are quasi-periodic with respect to the lattice $\mathbb{Z}^g \oplus \tau\mathbb{Z}^g$ defined by τ [26, Remark 8.5.3]. For all $a, b \in \mathbb{Z}^g$ and $z \in \mathbb{C}^g$, the following functional equation holds.

$$\theta \begin{bmatrix} \varepsilon \\ \delta \end{bmatrix} (z + \tau a + b, \tau) = \mathbf{e} \left(\varepsilon^t b - \delta^t a - \frac{1}{2} a^t \tau a - z^t a \right) \theta \begin{bmatrix} \varepsilon \\ \delta \end{bmatrix} (z, \tau) . \tag{2.1.5}$$

Theta functions also transform naturally under symplectic transformations. The group $\Gamma_g = \mathrm{Sp}(2g, \mathbb{Z})$ of integral symplectic transformations acts on $\mathbb{H}_g$ as follows. For $\gamma \in \Gamma_g$ and $\tau \in \mathbb{H}_g$,

$$\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} , \qquad \gamma \cdot \tau = (A\tau + B)(C\tau + D)^{-1} . \tag{2.1.6}$$

This extends to an action on $\mathbb{C}^g \times \mathbb{H}_g$ by

$$\gamma \cdot (z, \tau) = ((C\tau + D)^{-t} z, \gamma \cdot \tau) , \tag{2.1.7}$$

and there is a corresponding action on the set of characteristics $(\mathbb{Z}/2\mathbb{Z})^{2g}$ by

$$\gamma \cdot \begin{bmatrix} \varepsilon \\ \delta \end{bmatrix} = \begin{pmatrix} D & -C \\ -B & A \end{pmatrix} \begin{bmatrix} \varepsilon \\ \delta \end{bmatrix} + \begin{bmatrix} \mathrm{diag}(CD^t) \\ \mathrm{diag}(AB^t) \end{bmatrix} . \tag{2.1.8}$$

We now state the *Theta Transformation Formula* [26, Section 8.6]:

$$\theta[\gamma \cdot m](\gamma \cdot (z, \tau)) = \phi(\gamma, m, z, \tau) \cdot \sqrt{\det(C\tau + D)} \cdot \theta[m](z, \tau) \tag{2.1.9}$$

where $\phi(\gamma, m, z, \tau) \in \mathbb{C}^*$ is an explicit function of the parameters with the same sign ambiguity as $\sqrt{\det(C\tau + D)}$.

2.2 Numerically approximating theta functions

We describe in this section algorithms for computing theta functions, by generalizing the algorithm from [52] for theta functions with characteristics and derivatives of arbitrary order.

Notation

We standardize here the notation for the whole section. We separate $z \in \mathbb{C}^g$ and $\tau \in \mathbb{H}_g$ into real and imaginary parts, by writing $z = x + iy$, $\tau = X + iY$, where $x, y \in \mathbb{R}^g$ and X, Y are real symmetric $g \times g$ matrices. Let $Y = T^t T$ be the Cholesky decomposition of Y, where T is upper-triangular. For any real vector $V \in \mathbb{R}^g$, we use $[V]$ to denote the vector whose entries are the entries of V rounded to the closest integers, and we denote $[\![V]\!] = V - [V]$.

We also denote $v(n) = \sqrt{\pi} T(n + [\![Y^{-1}y]\!])$ and we define the lattice $\Lambda = \{v(n) \mid n \in \mathbb{Z}^g\}$, letting ρ be the length of the shortest nonzero vector in Λ. We denote by $\Gamma(z, x) = \int_x^\infty t^{z-1} e^{-t} dt$ the incomplete Gamma function.

Pointwise and uniform approximations

In [52], Deconinck et al. derive a *pointwise approximation* of the theta function, which approximates (2.1.1) by a finite sum with a specified error, given inputs z, τ.

Theorem 2.2.1 ([52, Theorem 2])**.** *Fix $z \in \mathbb{C}^g$, $\tau \in \mathbb{H}_g$ and $\varepsilon > 0$. Let R be the greater of $(\sqrt{2g} + \rho)/2$ and the real positive solution of R in $\varepsilon = g2^{g-1}\Gamma(g/2, (R - \rho/2)^2)/\rho^g$. The Riemann theta function $\theta(z, \tau)$ is approximated by*

$$e^{\pi y^t Y^{-1} y} \sum_{n \in S_R} \mathbf{e}\left(\frac{1}{2}\left(n - [Y^{-1}y]\right)^t X \left(n - [Y^{-1}y]\right) + \left(n - [Y^{-1}y]\right)^t x\right) e^{-\|v(n)\|^2}, \qquad (2.2.1)$$

with an absolute error ε on the sum, where

$$S_R = \{n \in \mathbb{Z}^g \mid \|v(n)\| < R\}. \qquad (2.2.2)$$

Note that the ellipsoid S_R in (2.2.2) depends on the input z. If we are evaluating the theta function at multiple inputs z for the same matrix τ, it would be more efficient to compute a bigger ellipsoid such that the approximation works for every z, instead of computing a different ellipsoid for each z. Although this increases the number of terms in the sum in (2.2.1), we would only need to compute the ellipsoid once, which is often preferable as the computation of the ellipsoid is usually expensive. This is the idea behind the following *uniform approximation* of the theta function.

Theorem 2.2.2 ([52, Theorem 3])**.** *Fix $\tau \in \mathbb{H}_g$ and $\varepsilon > 0$. Let R be defined as in Theorem 2.2.1. For any $z \in \mathbb{C}^g$, the Riemann theta function $\theta(z, \tau)$ is approximated by* (2.2.1) *with an absolute error ε on the sum, but with the set S_R replaced by U_R, where*

$$U_R = \{n \in \mathbb{Z}^g \mid \pi(n - c)^t Y(n - c) < R^2, |c_j| < 1/2, \forall j = 1, \ldots, g\}. \qquad (2.2.3)$$

The set U_R in (2.2.3) can be thought of as a deformed ellipsoid, which is the union of all ellipsoids S_R from (2.2.2), as $z \in \mathbb{C}^g$ varies. By taking this union, we get a uniform approximation of the theta function for all inputs z.

Theta functions with characteristics

We extend Theorem 2.2.2 for computing theta functions with characteristics.

Theorem 2.2.3. *Fix $\tau \in \mathbb{H}_g$ and $\varepsilon > 0$. Let R be defined as in Theorem 2.2.1. For any input $z \in \mathbb{C}^g$ and characteristic $\begin{bmatrix} \varepsilon \\ \delta \end{bmatrix} \in \{0,1\}^{2g}$, the Riemann theta function with characteristic $\theta\begin{bmatrix} \varepsilon \\ \delta \end{bmatrix}(z,\tau)$ is approximated by*

$$e^{\pi y^t Y^{-1} y} \sum_{n \in C_R} \mathbf{e}\left(\frac{1}{2}(n-\eta)^t X (n-\eta) + (n-\eta)^t \left(x + \frac{\delta}{2}\right)\right) e^{-\|v(n+\frac{\varepsilon}{2})\|^2}\,, \tag{2.2.4}$$

with an absolute error ε on the sum, where $\eta = [Y^{-1}y] - \frac{\varepsilon}{2}$ and

$$C_R = \{n \in \mathbb{Z}^g \,|\, \pi(n-c)^t Y(n-c) < R^2\,, |c_j| < 1\,, \forall j = 1, \ldots, g\}\,. \tag{2.2.5}$$

Proof. From (2.1.2), we can compute theta functions with characteristics in a similar way as the usual theta function, by translating z to $z + \frac{\delta}{2}$, and translating the lattice points in the sum from n to $n + \frac{\varepsilon}{2}$. Note that this only changes the real part of z, while the imaginary part stays the same. Hence the pointwise approximation in Theorem 2.2.1 holds for theta functions with characteristics, if we replace (2.2.1) by the formula in (2.2.4), where we take the sum over

$$S_{R,\varepsilon} = \left\{ n \in \mathbb{Z}^g \,\middle|\, \left\| v\left(n + \frac{\varepsilon}{2}\right)\right\| < R \right\}\,. \tag{2.2.6}$$

To obtain a uniform approximation for any $z \in \mathbb{C}^g$ and any characteristic, we take the union of the ellipsoids $S_{R,\varepsilon}$ from (2.2.6) as z and ε vary. Since $v(n + \frac{\varepsilon}{2}) = \sqrt{\pi}T(n + [\![Y^{-1}y]\!] + \frac{\varepsilon}{2})$, and the entries of $[\![Y^{-1}y]\!] + \frac{\varepsilon}{2}$ have absolute value at most 1, it follows that the deformed ellipsoid C_R from (2.2.5) is the union of the ellipsoids $S_{R,\varepsilon}$. □

Note that in (2.2.5), we use a larger deformed ellipsoid whose center wanders about a cube with side length twice as large as in (2.2.3), in order to get a uniform approximation for arbitrary characteristics.

Derivatives of theta functions

We denote the N-th order derivative of the theta function along the vectors $k^{(1)}, \ldots, k^{(N)}$ as

$$D\left(k^{(1)}, \ldots, k^{(N)}\right)\theta(z,\tau) = \sum_{i_1,\ldots,i_N=1}^{g} k^{(1)}_{i_1} \cdots k^{(N)}_{i_N} \frac{\partial^N \theta(z,\tau)}{\partial z_{i_1} \cdots \partial z_{i_N}}\,. \tag{2.2.7}$$

In [52], formulae are given for the pointwise and uniform approximations of the first and second derivatives of the theta function. We generalize these to arbitrary order derivatives here. First we will need the following lemma.

Lemma 2.2.4 ([52, Lemma 2])**.** *Let Λ be a g-dimensional affine lattice in $\mathbb{R}^g$, and let $p \in \mathbb{Z}$ be positive. Let ρ be the length of the shortest nonzero vector in Λ, and let $R > \frac{\rho}{2} + \frac{1}{2}\sqrt{g + 2p + \sqrt{g^2 + 8p}}$. Then*

$$\sum_{y \in \Lambda, \|y\| \geq R} \|y\|^p e^{-\|y\|^2} \leq \frac{g}{2}\left(\frac{2}{\rho}\right)^g \Gamma\left(\frac{g+j}{2}, \left(R - \frac{\rho}{2}\right)^2\right). \tag{2.2.8}$$

Pointwise approximation

We first give a formula for a pointwise approximation of the theta function, with derivatives of arbitrary order.

Theorem 2.2.5. *Fix $\tau \in \mathbb{H}_g$ and $\varepsilon > 0$. Let R be the greater of $\frac{1}{2}\sqrt{g + 2N + \sqrt{g^2 + 8N}} + \frac{\rho}{2}$ and the real positive solution of R in*

$$\varepsilon = (2\pi)^N \frac{g}{2}\left(\frac{2}{\rho}\right)^g \|k^{(1)}\| \cdots \|k^{(N)}\| \left[\sum_{j=0}^{N} \binom{N}{j} \frac{1}{\pi^{j/2}} \|T^{-1}\|^j \|Y^{-1}y\|^{N-j} \Gamma\left(\frac{g+j}{2}, \left(R - \frac{\rho}{2}\right)^2\right)\right].$$

Let S_R be defined as in (2.2.2). The N-th derivative $D(k^{(1)}, \ldots, k^{(N)})\theta(z, \tau)$ of the theta function is approximated by

$$\begin{aligned} &e^{\pi y^t Y^{-1} y}(2\pi i)^N \sum_{n \in S_R} \left(k^{(1)} \cdot (n - [Y^{-1}y])\right) \cdots \left(k^{(N)} \cdot (n - [Y^{-1}y])\right) \\ &\quad \times \mathbf{e}\left(\frac{1}{2}(n - [Y^{-1}y])^t X (n - [Y^{-1}y]) + (n - [Y^{-1}y])^t x\right) e^{-\|v(n)\|^2}, \end{aligned} \tag{2.2.9}$$

with an absolute error ε on the product of $(2\pi i)^N$ with the sum. By $v \cdot w$ we denote the usual scalar product of vectors.

Proof. Firstly, from [52] we can change the index of summation in

$$D(k^{(1)}, \ldots, k^{(N)})\theta(z, \tau) = (2\pi i)^N \sum_{n \in \mathbb{Z}^g} (k^{(1)} \cdot n) \cdots (k^{(N)} \cdot n) \mathbf{e}\left(\frac{1}{2} n^t \tau n + n^t z\right)$$

to get the expression in (2.2.9), but with the set S_R replaced by $\mathbb{Z}^g$. Thus the error in the approximation is

$$\begin{aligned}
\varepsilon = \Bigg|&(2\pi i)^N \sum_{n\in\mathbb{Z}^g\setminus S_R} \left(k^{(1)}\cdot(n-[Y^{-1}y])\right)\cdots\left(k^{(N)}\cdot(n-[Y^{-1}y])\right)\\
&\times \mathbf{e}\left(\frac{1}{2}(n-[Y^{-1}y])^t X(n-[Y^{-1}y]) + (n-[Y^{-1}y])^t x\right) e^{-\|v(n)\|^2}\Bigg|\\
&\leq (2\pi)^N \|k^{(1)}\|\cdots\|k^{(N)}\| \sum_{n\in\mathbb{Z}^g\setminus S_R} \left\|n-[Y^{-1}y]\right\|^N e^{-\|v(n)\|^2}\\
&= (2\pi)^N \|k^{(1)}\|\cdots\|k^{(N)}\| \sum_{n\in\mathbb{Z}^g\setminus S_R} \left\|\frac{1}{\sqrt{\pi}}T^{-1}v(n) - Y^{-1}y\right\|^N e^{-\|v(n)\|^2}\\
&\leq (2\pi)^N \|k^{(1)}\|\cdots\|k^{(N)}\| \sum_{n\in\mathbb{Z}^g\setminus S_R} \left(\frac{1}{\sqrt{\pi}}\|T^{-1}\|\cdot\|v(n)\| + \|Y^{-1}y\|\right)^N e^{-\|v(n)\|^2}\\
&= (2\pi)^N \|k^{(1)}\|\cdots\|k^{(N)}\| \sum_{n\in\mathbb{Z}^g\setminus S_R} \sum_{j=0}^{N} \binom{N}{j} \frac{1}{\pi^{j/2}} \|T^{-1}\|^j \|v(n)\|^j \|Y^{-1}y\|^{N-j} e^{-\|v(n)\|^2}\\
&= (2\pi)^N \|k^{(1)}\|\cdots\|k^{(N)}\| \sum_{j=0}^{N} \binom{N}{j} \frac{1}{\pi^{j/2}} \|T^{-1}\|^j \|Y^{-1}y\|^{N-j} \sum_{n\in\mathbb{Z}^g\setminus S_R} \|v(n)\|^j e^{-\|v(n)\|^2}
\end{aligned}$$

where we use the Cauchy-Schwarz and triangle inequalities. We then apply Lemma 2.2.4 to get the bound

$$\begin{aligned}
\varepsilon &\leq (2\pi)^N \|k^{(1)}\|\cdots\|k^{(N)}\| \sum_{j=0}^{N} \binom{N}{j} \frac{1}{\pi^{j/2}} \|T^{-1}\|^j \|Y^{-1}y\|^{N-j} \frac{g}{2}\left(\frac{2}{\rho}\right)^g \Gamma\left(\frac{g+j}{2}, \left(R-\frac{\rho}{2}\right)^2\right),\\
&\leq (2\pi)^N \frac{g}{2}\left(\frac{2}{\rho}\right)^g \|k^{(1)}\|\cdots\|k^{(N)}\| \sum_{j=0}^{N} \binom{N}{j} \frac{1}{\pi^{j/2}} \|T^{-1}\|^j \|Y^{-1}y\|^{N-j} \Gamma\left(\frac{g+j}{2}, \left(R-\frac{\rho}{2}\right)^2\right).
\end{aligned}$$

□

Uniform approximation

We now give a formula for a uniform approximation of derivatives of the theta function. First, we remark that by the quasi-periodicity of the theta function from (2.1.5), it suffices to consider inputs z of the form $z = a + \tau b$, for $a, b \in [0,1)^g$, which is what we do here.

Theorem 2.2.6. *Fix $\tau \in \mathbb{H}_g$, $\varepsilon > 0$. Let $k^{(1)}, \ldots, k^{(N)}$ be unit vectors, and let R be the greater of $\frac{1}{2}\sqrt{g + 2N + \sqrt{g^2 + 8N}} + \frac{\rho}{2}$ and the real positive solution of R in*

$$\varepsilon = (2\pi)^N \frac{g}{2}\left(\frac{2}{\rho}\right)^g \sum_{j=0}^{N} \binom{N}{j} \frac{1}{\pi^{j/2}} \|T^{-1}\|^j \sqrt{g}^{N-j} \Gamma\left(\frac{g+j}{2}, \left(R-\frac{\rho}{2}\right)^2\right). \tag{2.2.10}$$

For inputs z of the form $z = a+\tau b$, for $a, b \in [0,1)^g$, the N-th derivative $D(k^{(1)},\ldots,k^{(N)})\theta(z,\tau)$ of the theta function is approximated by (2.2.9) *but with the set S_R replaced by U_R from* (2.2.3)*, with an absolute error ε on the product of $(2\pi i)^N$ with the sum.*

Proof. For inputs z of the form $z = a + \tau b$, we can write z as $z = a + (X + iY)b = (a + Xb) + iYb = x + iy$. Then $\|Y^{-1}y\| = \|b\| \leq \sqrt{g}$. Substituting this and $\|k^{(1)}\| = \cdots = \|k^{(N)}\| = 1$ into the expression for ε in Theorem 2.2.5, the result follows. □

Derivatives of theta functions with characteristics

We generalize Theorem 2.2.6 for derivatives of theta functions with characteristics. This follows from exactly the same argument as in Theorem 2.2.3, by computing the sum over a larger ellipsoid.

Theorem 2.2.7. *Fix $\tau \in \mathbb{H}_g$, $\varepsilon > 0$. Let $k^{(1)},\ldots,k^{(N)}$ be unit vectors, and let R be defined as in Theorem 2.2.6. For z of the form $z = a + \tau b$, for $a, b \in [0,1)^g$, and $\begin{bmatrix}\varepsilon\\ \delta\end{bmatrix} \in \{0,1\}^{2g}$, the N-th derivative $D(k^{(1)},\ldots,k^{(N)})\theta\begin{bmatrix}\varepsilon\\ \delta\end{bmatrix}(z,\tau)$ of the theta function with characteristic is approximated by*

$$\begin{aligned} &e^{\pi y^t Y^{-1} y}(2\pi i)^N \sum_{n\in C_R} \left(k^{(1)}\cdot(n-\eta)\right)\cdots\left(k^{(N)}\cdot(n-\eta)\right) \\ &\times \mathbf{e}\left(\frac{1}{2}(n-\eta)^t X (n-\eta) + (n-\eta)^t\left(x+\frac{\delta}{2}\right)\right) e^{-\|v(n+\frac{\varepsilon}{2})\|^2}, \end{aligned} \tag{2.2.11}$$

with an absolute error ε on the product of $(2\pi i)^N$ with the sum, where $\eta = [Y^{-1}y] - \frac{\varepsilon}{2}$ and C_R is as defined in (2.2.5)*.*

2.3 Computing theta functions in Julia

In this section, we introduce our Julia package `Theta.jl` for numerical computations of theta functions. Our package is specialized for multiple evaluations of theta functions for the same Riemann matrix $\tau \in \mathbb{H}_g$ and different z, for small values of the genus g. The main application that we had in mind when designing our package was for numerical approaches to the Schottky problem in genus five, which we describe in more detail in Chapter 3.

Interface

Our Julia package `Theta.jl` is available at the following website, which has instructions and a link to more detailed documentation.

`https://github.com/chualynn/Theta.jl`

We describe the basic interface of the package here. To use `Theta.jl`, we recommend installing Julia in version 1.1 or above. The package can be installed and used with the following commands in Julia.

```
julia> import Pkg
julia> Pkg.add("Theta")
julia> using Theta
```

Starting with a matrix $\tau \in \mathbb{H}_g$, we first construct a `RiemannMatrix` from it. This is a type in `Theta.jl` which contains information needed to compute the theta function with input τ. This includes the ellipsoids used for computing the theta function and its derivatives, as well as the Siegel-transformed matrix. To construct a `RiemannMatrix`, we give as input τ, a boolean flag `siegel` which specifies if we want to perform a Siegel transformation on τ, a floating point number ε which specifies the error in computing the theta functions, and an integer `nderivs` which specifies the highest order of the derivative for which we want to compute the theta function.

As an example, we start with a genus 5 curve defined by

$$x^6y^2-4x^4y^2-2x^3y^3-2x^4y+2x^3y+4x^2y^2+3xy^3+y^4+4x^2y+2xy^2+x^2-4xy-2y^2-2x+1\,.$$

We pick this curve as it has a vanishing theta null; we refer to Example 4.4.9 for more details and further computations on this curve. We compute the Riemann matrix τ of the curve using the package [35] in Sage [103], and we type it as an input in Julia.

$$\begin{pmatrix} 0.40243+0.68413i & -0.18138+0.21894i & 0.24323-0.13416i & 0.00403+0.05085i & -0.31818+0.14383i \\ -0.18137+0.21894i & 0.27914+1.01836i & -0.09799+0.46222i & -0.06566+0.60959i & -0.14647+0.37006i \\ 0.24323-0.13416i & -0.09799+0.46222i & 0.16663+0.68136i & -0.28606+0.02038i & 0.18558-0.15061i \\ 0.00403+0.05085i & -0.06566+0.60959i & -0.28606+0.02038i & 0.04136+1.40560i & 0.19025+0.82885i \\ -0.31818+0.14384i & -0.14647+0.37006i & 0.18558-0.15061i & 0.19025+0.82885i & 0.74873+1.01168i \end{pmatrix}$$

We then construct a `RiemannMatrix` in `Theta.jl`, where we specify in the input the options to compute a Siegel transformation, an error of 10^{-12}, and to compute derivatives up to the fourth order.

```
    julia> R = RiemannMatrix(τ, siegel=true, ε=1.0e-12, nderivs=4);
```

We pick some input z and compute the theta function $\theta(z,\tau)$ as follows.

```
julia> z = [1.041+0.996im; 1.254+0.669im; 0.591+0.509im; -0.301+0.599im;
0.388+0.051im];
julia> theta(z, R)
-854877.6514446283 + 2.3935081163150463e6im
```

We can compute first derivatives of theta functions by specifying the direction using the optional argument `derivs`. For instance, to compute $\frac{\partial\theta}{\partial z_1}(z,\tau)$, we use

```
julia> theta(z, R, derivs=[[1,0,0,0,0]])
2.6212151525759254e7 + 9.28714502306052e6im
```

We specify higher order derivatives by adding more elements in the input to `derivs`, where each element specifies the direction of the derivative. For instance, to compute $\frac{\partial^3 \theta}{\partial z_3 \partial z_4}(z, \tau)$, we use

```
julia> theta(z, R, derivs=[[0,0,1,0,0], [0,0,0,1,0]])
1.0478325534969474e8 - 3.369999441122761e8im
```

We can compute theta functions with characteristics using the optional argument `char`.

```
julia> theta(z, R, char=[[0,1,1,0,0],[1,0,1,1,0]])
1.8859811381826473e6 - 1.6046614411453768e6im
```

We can also compute derivatives of theta functions with characteristics.

```
julia> theta(z, R, derivs=[[1,0,0,0,0]], char=[[0,1,0,0,1],[1,1,0,0,1]])
-2.448093122926732e7 + 3.582557740667034e7im
```

Algorithms

We describe here some details of the algorithms and the design choices that we made in our implementation.

Choice of ellipsoid

The main application of our package is for computing theta functions at the same Riemann matrix τ, and for multiple choices of inputs z, characteristics and derivatives. As such, in our implementation we use the algorithm for uniform approximations of theta functions described in Theorem 2.2.7, which allows us to compute derivatives of theta functions with characteristics, for inputs z of the form $z = a + \tau b$, for $a, b \in [0, 1)^g$.

In Theorem 2.2.7, we approximate the theta function by taking the sum over a deformed ellipsoid C_R from (2.2.5). For a fixed $\tau \in \mathbb{H}_g$ and error $\varepsilon > 0$, the ellipsoid C_R depends only on the order N of the derivative. Hence for each order of the derivative for which we are interested in computing the theta function, we compute an ellipsoid C_R. Then we can compute theta functions with any input $z = a + \tau b$, any characteristic, and N-th order derivatives along N unit vectors.

While C_R is larger than the ellipsoids for the other less general approximations in Section 2.2, we make this design choice as it is expensive to compute the ellipsoid relative to computing more terms in the sum in (2.2.11). Hence if we are computing multiple values of the theta function for a fixed matrix τ, it is faster to compute a bigger ellipsoid and use the same ellipsoid for every computation, rather than repeatedly computing a slightly smaller ellipsoid for each computation.

Lattice reductions

In [52], the authors approximate the length ρ of the shortest vector of the lattice generated by T using the LLL algorithm by Lenstra, Lenstra and Lovász [85]. This is a reasonable choice if g is large, since computing the shortest vector is in general NP-hard under randomized reductions [5] and is impractical for large dimensions. On the other hand, the LLL algorithm gives a polynomial time approximation, but with an error that grows exponentially with the dimension. In our implementation, since we focus on lattices with small dimensions $g = 5$, we compute the shortest vector exactly using the enumeration algorithm in [106], which is fast for small dimensions. Moreover, by computing ρ exactly, we obtain a smaller ellipsoid (2.2.5) than if we use an overestimation of ρ from the LLL algorithm.

If we are interested in computing the theta function for a fixed τ at many values of z, it may be more efficient if we transform τ such that the ellipsoids in (2.2.3) or (2.2.5) are less eccentric, so that they contain fewer lattice points. This can be done via symplectic transformations, which modify the theta function according to the Theta Transformation Formula (2.1.9). For this purpose, we use Siegel's algorithm [109], which iteratively finds a new matrix where the corresponding ellipsoid has a smaller eccentricity. Siegel's algorithm is implemented in [52]. A variant is described in [60], and we implement the latter in our package, where we use the algorithm for Hermite-Korkine-Zolotareff (HKZ) reduction in [122] as a subroutine. In `Theta.jl`, we compute the Siegel transformation once for each Riemann matrix, and work with the Siegel-transformed matrix for all computations. This helps us to achieve a lower amortized running time for computing many values of the theta function on a fixed Riemann matrix.

Comparisons with other packages

We compare `Theta.jl` with the other packages for computing theta functions that we are aware of, namely algcurves [52] in Maple, the MATLAB package in [60] and `abelfunctions` [114] in Sage.

Functionality

The main advantage of `Theta.jl` in terms of functionality is that we support computations of theta functions with characteristics, as well as their derivatives, which to our knowledge is not implemented in other packages. Moreover, we make optimizations described in Section 2.3 for faster computations in applications where we do many computations with a fixed Riemann matrix of low genus.

Performance

We compare the performance of `Theta.jl` with the Sage package `abelfunctions` [114], by comparing the average time taken to compute the genus 5 FGSM relations by Farkas, Grushevsky and Salvati Manni [59] (see Section 3.3), as well as to compute the Hessian matrix of Chapter 4.

For our experiments, we sample matrices in the Siegel upper-half space as follows. First we sample 5×5 matrices M_X, M_Y such that the entries are random floating point numbers between -1 and 1, using the random number generators in Julia and NumPy. Then we sample $\tau \in \mathbb{H}_5$ as $\tau = \frac{1}{2}(M_X + M_X^t) + M_Y^t M_Y i$. This is implemented in `Theta.jl` for general dimensions g, in the function `random_siegel(g)`.

In each experiment, we sample 1000 random matrices using the routine described above, and do our computations on each matrix using `Theta.jl` and `abelfunctions`, with a standard laptop. We list in the table below the average time and standard deviation using `Theta.jl` and `abelfunctions`, for computing the FGSM relations in genus 5, and the genus 5 Hessian matrix.

Experiment	Package	Average time (s)	Standard deviation (s)
FGSM	`Theta.jl`	2.5	0.6
	`abelfunctions`	114.2	290.5
Hessian	`Theta.jl`	0.7	0.2
	`abelfunctions`	20.3	58.0

One major reason for the faster runtime on `Theta.jl` is the use of the Siegel transformation on the Riemann matrix, which is not implemented in `abelfunctions`. This also leads to the higher standard deviation in the computation for the latter.

2.4 Conclusion

In this chapter, we described the Riemann theta function and algorithms for numerically approximating it. We also introduced our Julia package `Theta.jl` for numerical computations of theta functions. In the next two chapters, we discuss the classical Schottky problem, whose solutions are described in terms of theta functions. We will see applications of `Theta.jl` in numerical solutions to the Schottky problem, at the end of Chapter 4.

Chapter 3

Classical Schottky problem

In this chapter, we introduce the classical Schottky problem, and we describe numerical approaches for solving it in genus four and five. The material in this chapter is from the paper "Computing Theta Functions with Julia" authored with Daniele Agostini, which has been submitted for publication [3], and the paper "Schottky Algorithms: Classical meets Tropical" authored with Mario Kummer and Bernd Sturmfels, which is published in Mathematics of Computation [43].

3.1 Introduction

The *Schottky problem* [70] concerns the characterization of Jacobians of genus g curves $\mathcal{J}_g$ among all abelian varieties of dimension g. An abelian variety is a projective variety that has the structure of an algebraic group, and it is a fundamental object in algebraic geometry. Let $\mathbb{H}_g$ be the *Siegel upper-half space*, which is the set of complex symmetric $g \times g$ matrices with positive definite imaginary part. For every $\tau \in \mathbb{H}_g$, we define a *principally polarized abelian variety (ppav)* as the quotient $A_\tau = \mathbb{C}^g/\Lambda_\tau$, where $\Lambda_\tau = \mathbb{Z}^g \oplus \tau\mathbb{Z}^g$ is a sublattice of $\mathbb{C}^g$. The polarization on A_τ is given by the *theta divisor*

$$\Theta_\tau = \{z \in A_\tau \,|\, \theta(z,\tau) = 0\} \,. \tag{3.1.1}$$

This is well-defined on A_τ because of the quasi-periodicity of the theta function in (2.1.5). Every such abelian variety is a group via the usual addition on $\mathbb{C}^g$. At the same time, the theta functions with characteristics can be used to give an embedding of A_τ inside $\mathbb{P}^{3^g-1}$, so that A_τ is a projective variety as well.

Two ppavs A_τ and $A_{\tau'}$ are isomorphic if and only if the corresponding Riemann matrices are related via the action (2.1.6) of the symplectic group $\Gamma_g = \mathrm{Sp}(2g,\mathbb{Z})$. Hence, the quotient $\mathcal{A}_g = \mathbb{H}_g/\,\mathrm{Sp}(2g,\mathbb{Z})$ is the *moduli space of principally polarized abelian varieties of dimension g*. This is a quasi-projective variety of dimension

$$\dim \mathcal{A}_g = \dim \mathbb{H}_g = \frac{g(g+1)}{2} \,. \tag{3.1.2}$$

The theta constants $\theta[m](0,\tau)$ give homogeneous coordinates on a finite cover of $\mathcal{A}_g$. First we consider the following subgroups of Γ_g:

$$\Gamma_g(4) = \{\gamma \in \Gamma_g \mid \gamma \equiv \mathrm{Id} \mod 4\}\,, \tag{3.1.3}$$

$$\Gamma_g(4,8) = \left\{ \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma_g(4) \;\middle|\; \mathrm{diag}(A^tB) \equiv \mathrm{diag}(C^tB) \equiv 0 \mod 8 \right\}. \tag{3.1.4}$$

The group $\Gamma_g(4,8)$ is normal of finite index in Γ_g, so the corresponding quotient $\mathcal{A}_g(4,8) = \mathbb{H}_g/\Gamma_g(4,8)$ is a finite Galois cover of $\mathcal{A}_g$. Moreover, the Theta Transformation Formula (2.1.9) shows that for every $\gamma \in \Gamma_g(4,8)$ and characteristic $m \in (\mathbb{Z}/2\mathbb{Z})^g$ we have

$$\theta[m](0,\gamma\cdot\tau) = \sqrt{\det(C\tau+D)}\cdot\theta[m](0,\tau)\,. \tag{3.1.5}$$

Thus the even theta constants define a map to projective space,

$$\mathcal{A}_g(4,8) \longrightarrow \mathbb{P}^{2^{g-1}(2^g+1)-1}\,, \qquad [\tau] \mapsto [\theta[m](0,\tau)]_{m \text{ even}} \tag{3.1.6}$$

which is actually an embedding, and realizes $\mathcal{A}_g(4,8)$ as an irreducible quasi-projective variety. By definition, polynomials in the homogeneous coordinates of $\mathbb{P}^{2^{g-1}(2^g+1)-1}$ correspond to polynomials in the theta constants.

Historically, abelian varieties arose from Jacobians of Riemann surfaces. For a Riemann surface C of genus g, we define its *Jacobian* as the quotient

$$J(C) = H^0(C,\omega_C)^\vee / H_1(C,\mathbb{Z})\,, \tag{3.1.7}$$

where the lattice $H^1(C,\mathbb{Z})$ is embedded in $H^0(C,\omega_C)^\vee$ via the integration pairing

$$H^0(C,\omega_C)\times H^1(C,\mathbb{Z}) \longrightarrow \mathbb{C}\,, \qquad (\omega,\alpha)\mapsto \int_\alpha \omega\,. \tag{3.1.8}$$

The Jacobian is a principally polarized abelian variety, and the corresponding Riemann matrix $\tau \in \mathcal{A}_g$ can be obtained by computing bases of $H^0(C,\omega_C)$ and $H^1(C,\mathbb{Z})$, as well as the integration pairing. This is implemented numerically in the packages `abelfunctions` [114] and [35] in Sage, and `algcurves` [52] in Maple. In this setting, the action of Γ_g on the Riemann matrices corresponds to a change of basis for $H^0(C,\omega_C)$ or $H^1(C,\mathbb{Z})$.

The Jacobian construction defines the *Torelli map* from the moduli space $\mathcal{M}_g$ of genus g Riemann surfaces to the moduli space $\mathcal{A}_g$ of dimension g ppavs:

$$\mathcal{J}\colon \mathcal{M}_g \longrightarrow \mathcal{A}_g\,, \qquad [C]\mapsto [J(C)]\,. \tag{3.1.9}$$

The image of this map is precisely the set of Jacobian varieties and its closure $\mathcal{J}_g$ in $\mathcal{A}_g$ is the *Schottky locus*. The *Schottky problem* asks for a characterization of $\mathcal{J}_g$ inside $\mathcal{A}_g$. It is one of the most celebrated questions in algebraic geometry, dating from the 19th century; we refer to [70] for a recent overview.

There are many possible interpretations and solutions to the Schottky problem. Here we focus on the most classical one, which asks for equations in the theta constants $\theta[m](0,\tau)$ that vanish exactly on the Schottky locus. In terms of the projective embedding of (3.1.6), this means determining the ideal generated by $\mathcal{J}_g(4,8)$ inside $\mathbb{P}^{2^{g-1}(2^g+1)-1}$, where we denote by $\mathcal{J}_g(4,8)$ the pullback of the Schottky locus along the finite cover $\mathcal{A}_g(4,8) \to \mathcal{A}_g$.

In this form, the Schottky problem is completely solved only in genus 4, with an explicit equation given by Schottky [107] and Igusa [75]. We discuss this further in Section 3.2.

The *weak Schottky problem* asks for explicit equations that characterize Jacobians up to extra irreducible components. A solution to this problem was given in genus 5 by Accola [1], and in a recent breakthrough, by Farkas, Grushevsky and Salvati Manni in all genera [59]. We describe these in Section 3.3.

3.2 Classical Schottky problem in genus four

In this section, we describe numerical solutions to the classical Schottky problem in genus four. We utilize the software `abelfunctions` [42] to test whether the Schottky–Igusa modular form [75] vanishes. In the affirmative case, we use a numerical version of Kempf's method [81] to compute a canonical embedding into $\mathbb{P}^3$.

We recall from Section 2.1 that the *sign* of a characteristic $m = \begin{bmatrix}\varepsilon\\ \delta\end{bmatrix}$ is defined as $e(m) = (-1)^{\varepsilon^t\delta}$, and we call a characteristic *even* or *odd* if the sign is 1 or -1 respectively. A triple of characteristics $\{m_1, m_2, m_3\} \subset (\mathbb{Z}/2\mathbb{Z})^8$ is called *azygetic* if

$$e(m_1)e(m_2)e(m_3)e(m_1+m_2+m_3) = -1\,. \tag{3.2.1}$$

Suppose that this holds. Then we choose a rank 3 subgroup N of $(\mathbb{Z}/2\mathbb{Z})^8$ such that all elements of $(m_1+N)\cup(m_2+N)\cup(m_3+N)$ are even. We consider the following three products of eight *theta constants* each:

$$\pi_i \quad = \prod_{m\in m_i+N} \theta[m](\tau,0) \qquad \text{for} \quad i = 1,2,3\,. \tag{3.2.2}$$

Theorem 3.2.1 (Igusa [75])**.** *The function $\mathbb{H}_4 \to \mathbb{C}$ that takes a symmetric 4×4-matrix τ to*

$$\pi_1^2 + \pi_2^2 + \pi_3^2 - 2\pi_1\pi_2 - 2\pi_1\pi_3 - 2\pi_2\pi_3 \tag{3.2.3}$$

is independent of the choices above. It vanishes if and only if τ lies in the closure of the Schottky locus $\mathcal{J}_4$.

We refer to the expression (3.2.3) as the *Schottky–Igusa modular form.* This is a polynomial of degree 16 in the theta constants $\theta[m](\tau,0)$. Of course, the formula is unique only modulo the ideal that defines the embedding of the moduli space $\mathcal{A}_4$ in the $\mathbb{P}^{15}$ of theta constants.

Our implementation uses the polynomial that is given by the following specific choices:

$$m_1 = \begin{pmatrix} 1 & 1 \\ 0 & 0 \\ 1 & 1 \\ 0 & 0 \end{pmatrix},\ m_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \\ 0 & 0 \\ 1 & 0 \end{pmatrix},\ m_3 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \\ 1 & 1 \\ 1 & 1 \end{pmatrix},\ n_1 = \begin{pmatrix} 0 & 1 \\ 0 & 1 \\ 0 & 1 \\ 1 & 0 \end{pmatrix},\ n_2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 1 & 0 \\ 1 & 1 \end{pmatrix},\ n_3 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \\ 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

The vectors n_1, n_2, n_3 generate the subgroup N in $(\mathbb{Z}/2\mathbb{Z})^8$. One checks that the triple $\{m_1, m_2, m_3\}$ is azygetic and that the three cosets $m_i + N$ consist of even elements only. The computations to be described next were done with the `Sage` library `abelfunctions` [42].

The algorithm in [51] finds the Riemann matrix $\tau \in \mathcal{J}_g$ of a plane curve in $\mathbb{C}^2$. It is implemented in `abelfunctions`. We first check that (3.2.3) does indeed vanish for such τ.

Example 3.2.2. *The plane curve $y^5 + x^3 - 1 = 0$ has genus four. Using* `abelfunctions`*, we compute its Riemann matrix τ:*

$$\begin{pmatrix} 0.16913 + 1.41714\mathrm{i} & -0.81736 - 0.25138\mathrm{i} & -0.05626 - 0.44830\mathrm{i} & 0.24724 + 0.36327\mathrm{i} \\ -0.81736 - 0.25138\mathrm{i} & -0.31319 + 0.67096\mathrm{i} & -0.02813 - 0.57155\mathrm{i} & 0.34132 + 0.40334\mathrm{i} \\ -0.05626 - 0.44830\mathrm{i} & -0.02813 - 0.57155\mathrm{i} & 0.32393 + 1.44947\mathrm{i} & -0.96494 - 0.63753\mathrm{i} \\ 0.24724 + 0.36327\mathrm{i} & 0.34132 + 0.40334\mathrm{i} & -0.96494 - 0.63753\mathrm{i} & 0.62362 + 0.73694\mathrm{i} \end{pmatrix}.$$

Evaluating the 16 theta constants $\theta[m](\tau, 0)$ numerically with `abelfunctions`*, we find that*

$$\begin{aligned} \pi_1^2 + \pi_2^2 + \pi_3^2 &= -5.13472888270289 + 6.13887870578982\mathrm{i}, \\ 2(\pi_1\pi_2 + \pi_1\pi_3 + \pi_2\pi_3) &= -5.13472882638710 + 6.13887931435788\mathrm{i}. \end{aligned}$$

We trust that (3.2.3) is zero, and conclude that τ lies in the Schottky locus $\mathcal{J}_4$, as expected.

Suppose now that we are given a matrix τ that depends on one or two parameters, so it traces out a curve or surface in $\mathbb{H}_4$. Then we can use our numerical method to determine the Schottky locus inside that curve or surface. Here is an illustration for a surface in $\mathbb{H}_4$.

Example 3.2.3. *The following one-parameter family of genus 4 curves is found in [73, §2]:*

$$y^6 \;=\; x(x+1)(x-t).$$

This is both a Shimura curve and a Teichmüller curve; we refer to [73] for the definitions. Its Riemann matrix is $\rho(t) = Z_2^{-1}Z_1$ where Z_1, Z_2 are given in [73, Prop. 6]. Consider the following two-parameter family in $\mathbb{H}_4$:

$$\tau(s,t) \;=\; s \cdot \mathit{diag}(2,3,5,7) \;+\; \rho(t). \tag{3.2.4}$$

We are interested in the restriction of the Schottky locus $\mathcal{J}_4$ to the (s,t)-plane. For our experiment, we assume that the two parameters satisfy $s \in [-0.5, 0.5]$ and $\lambda^{-1}(t) \in [\mathrm{i}, \mathrm{i}+1]$, where λ is the function in [73, Prop. 6]. Using `abelfunctions`*, we computed the absolute* *value of the modular form (3.2.3) at 6400 equally spaced rational points in the square* $[-0.5, 0.5] \times [i, i+1]$*. That graph is shown in Figure 3.2.4. For s different from zero, the smallest absolute value of (3.2.3) is* 4.3×10^{-3}*. For* $s = 0$*, all absolute values are below* 2.9×10^{-8}*. Based on this numerical evidence, we conclude that the Schottky locus of our family is the line* $s = 0$*.*

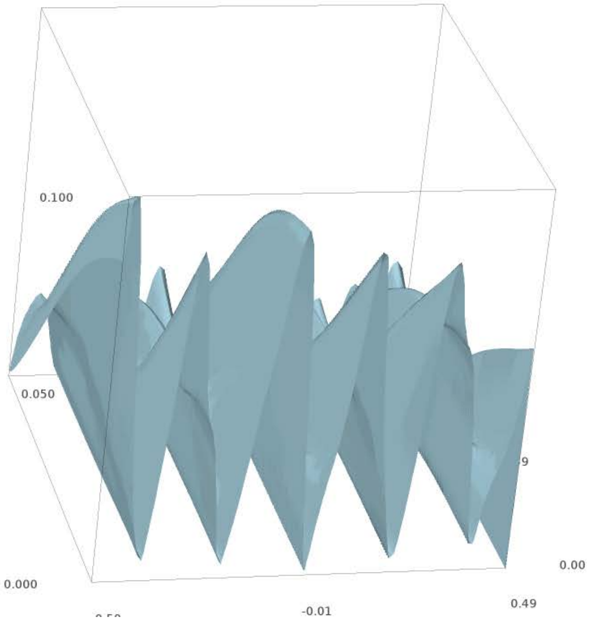


Figure 3.1: Absolute value of the Schottky–Igusa modular form on the 2-parameter family (3.2.4).

We now come to the Schottky Recovery Problem. Our input is a matrix τ in $\mathcal{J}_4$. Our task is to compute a curve whose Riemann matrix equals τ. We use the following result from Kempf's paper [81]. The *theta divisor* in the Jacobian $\mathbb{C}^4/(\mathbb{Z}^4 + \mathbb{Z}^4\tau)$ is the zero locus $\Theta^{-1}(0)$ of the Riemann theta function $\Theta(z) := \theta[0](\tau, z)$. For generic τ this divisor is singular at precisely two points. These represent 3-to-1 maps from the curve to $\mathbb{P}^1$. We compute a vector $z^* \in \mathbb{C}^4$ that is a singular point of $\Theta^{-1}(0)$ by solving the system of five equations

$$\Theta(z) \;=\; \frac{\partial\Theta}{\partial z_1}(z) = \frac{\partial\Theta}{\partial z_2}(z) = \frac{\partial\Theta}{\partial z_3}(z) = \frac{\partial\Theta}{\partial z_4}(z) = 0. \qquad (3.2.5)$$

The Taylor series of the Riemann theta function Θ at the singular point z^* has the form

$$\Theta(z^* + x) \;=\; f_2(x) \,+\, f_3(x) \,+\, f_4(x) \,+\, \text{higher order terms}, \qquad (3.2.6)$$

where f_s is a homogeneous polynomial of degree s in $x = (x_1, x_2, x_3, x_4)$.

Proposition 3.2.4 (Kempf [81]). *The canonical curve with Riemann matrix τ is the degree 6 curve in $\mathbb{P}^3$ that is defined by the quadratic equation $f_2 = 0$ and the cubic equation $f_3 = 0$.*

Thus our algorithm for the Schottky Recovery Problem consists of solving the five equations (3.2.5) for $z^* \in \mathbb{C}^4$, followed by extracting the polynomials f_2 and f_3 in the Taylor series (3.2.6). Both of these steps can be done numerically using the software `abelfunctions` [42].

Example 3.2.5. *Let $\tau \in \mathcal{J}_4$ be the Riemann matrix of the genus 4 curve*

$$C = \{x^3y^3 + x^3 + y^3 = 1\}.$$

We obtain τ numerically using `abelfunctions`. We want to recover C from τ. To be precise, given only τ, we want to find defining equations $f_2 = f_3 = 0$ in $\mathbb{P}^3$ of the canonical embedding of C. For that we use evaluations of $\Theta(z)$ and its derivatives in `abelfunctions`, combined with a numerical optimization routine in `SciPy` [119]. We solve the equations (3.2.5) starting from random points $z = u + \tau v$ where $u, v \in \mathbb{R}^4$ with entries between 0 and 1. After several tries, the local method in `SciPy` converges to the following solution of our equations:

$$z^* = \big(0.55517 + 0.69801\mathrm{i}, 0.53678 + 0.26881\mathrm{i}, -0.50000 - 0.58958\mathrm{i}, 0.55517 + 0.69801\mathrm{i}\big).$$

Using (3.2.6), we computed the quadric f_2, which is nonsingular, as well as the cubic f_3:

$$\begin{aligned} f_2(x) \quad = \quad & (-3.044822827 + 21.980542613\mathrm{i}) \cdot x_1^2 + (-237.95207224 + 252.54744634\mathrm{i}) \cdot x_1x_2 \\ & +(-222.35552015 + 139.95612952\mathrm{i}) \cdot x_1x_3 + (-200.66932133 - 16.596272620\mathrm{i}) \cdot x_1x_4 \\ & +(-191.16241727 - 85.22650070\mathrm{i}) \cdot x_2^2 + (-429.11449060 + 167.32094535\mathrm{i}) \cdot x_2x_3 \\ & +(-237.952072 + 252.54744632\mathrm{i}) \cdot x_2x_4 + (-206.75896934 + 27.364814282\mathrm{i}) \cdot x_3^2 \\ & +(222.35552013 + 139.95612953\mathrm{i}) \cdot x_3x_4 + (-3.0448227745 + 21.980542601\mathrm{i}) \cdot x_4^2 \end{aligned}$$

$$\begin{aligned} f_3(x) \quad = \quad & (441.375966486 + 61.14097461986\mathrm{i}) \cdot x_1^3 + (2785.727151434 + 2303.609067429\mathrm{i}) \cdot x_1^2x_2 \\ & + \quad \cdots\cdots \quad + \quad (441.3759668263 + 61.14097402189\mathrm{i}) \cdot x_4^3. \end{aligned}$$

As a proof of concept we also computed the 120 tritangent planes numerically directly from τ. These planes are indexed by the 120 odd theta characteristics m. In analogy to the computation in [114, Section 5.2] of the 28 bitangents for $g = 3$, their defining equations are

$$\left.\frac{\partial\theta[m](\tau,z)}{\partial z_1}\right|_{z=0} \cdot x_1 + \left.\frac{\partial\theta[m](\tau,z)}{\partial z_2}\right|_{z=0} \cdot x_2 + \left.\frac{\partial\theta[m](\tau,z)}{\partial z_3}\right|_{z=0} \cdot x_3 + \left.\frac{\partial\theta[m](\tau,z)}{\partial z_4}\right|_{z=0} \cdot x_4 = 0.$$

We verified numerically that each such plane meets $\{f_2 = f_3 = 0\}$ in three double points.

Remark 3.2.6. *On our website (5.1.1), we offer a program in `Sage` whose input is a symmetric 4×4-matrix $\tau \in \mathbb{H}_4$, given numerically. The code decides whether τ lies in $\mathcal{J}_4$ and, in the affirmative case, it computes the canonical curve $\{f_2 = f_3 = 0\}$ and its 120 tritangent planes.*

3.3 Classical Schottky problem in genus five

For genus five and above, the classical Schottky problem is open. In this section, we describe two weak solutions to the Schottky problem in genus five, from [1] and [59]. We also describe numerical implementations of these solutions using our package `Theta.jl` from Section 2.3.

Farkas, Grushevsky and Salvati Manni's solution

In a recent preprint [59], H. Farkas, Grushevsky and Salvati Manni give a solution to the weak Schottky problem in arbitrary genus. To state their result, consider for every $g \geq 4$ and every $\varepsilon \in (\mathbb{Z}/2\mathbb{Z})^{g-4}$ the following three monomials of degree 8 in theta constants (here we denote characteristics as row vectors for notational simplicity):

$$\begin{aligned}
RR^1_{34,\varepsilon} = \;& \theta\left[\begin{smallmatrix} E & 0 & 0 & 0 & \varepsilon \\ 0 & 0 & 0 & 0 & \mathbf{0} \end{smallmatrix}\right]\theta\left[\begin{smallmatrix} E & 0 & 0 & 0 & \varepsilon \\ 1 & 1 & 1 & 1 & \mathbf{1} \end{smallmatrix}\right]\theta\left[\begin{smallmatrix} E & 0 & 1 & 1 & \varepsilon \\ 0 & 1 & 0 & 0 & \mathbf{0} \end{smallmatrix}\right]\theta\left[\begin{smallmatrix} E & 0 & 1 & 1 & \varepsilon \\ 1 & 0 & 1 & 1 & \mathbf{1} \end{smallmatrix}\right] \\
& \theta\left[\begin{smallmatrix} 1+E & 1 & 0 & 0 & \varepsilon \\ 0 & 0 & 0 & 1 & \mathbf{0} \end{smallmatrix}\right]\theta\left[\begin{smallmatrix} 1+E & 1 & 0 & 0 & \varepsilon \\ 1 & 1 & 1 & 0 & \mathbf{1} \end{smallmatrix}\right]\theta\left[\begin{smallmatrix} 1+E & 1 & 1 & 1 & \varepsilon \\ 0 & 1 & 0 & 1 & \mathbf{0} \end{smallmatrix}\right]\theta\left[\begin{smallmatrix} 1+E & 1 & 1 & 1 & \varepsilon \\ 1 & 0 & 1 & 0 & \mathbf{1} \end{smallmatrix}\right] \\
RR^2_{34,\varepsilon} = \;& \theta\left[\begin{smallmatrix} 1+E & 0 & 1 & 0 & \varepsilon \\ 0 & 0 & 0 & 0 & \mathbf{0} \end{smallmatrix}\right]\theta\left[\begin{smallmatrix} 1+E & 0 & 1 & 0 & \varepsilon \\ 1 & 1 & 1 & 1 & \mathbf{1} \end{smallmatrix}\right]\theta\left[\begin{smallmatrix} 1+E & 0 & 0 & 1 & \varepsilon \\ 0 & 1 & 0 & 0 & \mathbf{0} \end{smallmatrix}\right]\theta\left[\begin{smallmatrix} 1+E & 0 & 0 & 1 & \varepsilon \\ 1 & 0 & 1 & 1 & \mathbf{1} \end{smallmatrix}\right] \\
& \theta\left[\begin{smallmatrix} E & 1 & 1 & 0 & \varepsilon \\ 0 & 0 & 0 & 1 & \mathbf{0} \end{smallmatrix}\right]\theta\left[\begin{smallmatrix} E & 1 & 1 & 0 & \varepsilon \\ 1 & 1 & 1 & 0 & \mathbf{1} \end{smallmatrix}\right]\theta\left[\begin{smallmatrix} E & 1 & 0 & 1 & \varepsilon \\ 0 & 1 & 0 & 1 & \mathbf{0} \end{smallmatrix}\right]\theta\left[\begin{smallmatrix} E & 1 & 0 & 1 & \varepsilon \\ 1 & 0 & 1 & 0 & \mathbf{1} \end{smallmatrix}\right] \\
RR^3_{34,\varepsilon} = \;& \theta\left[\begin{smallmatrix} E & 0 & 0 & 0 & \varepsilon \\ 0 & 0 & 1 & 1 & \mathbf{0} \end{smallmatrix}\right]\theta\left[\begin{smallmatrix} E & 0 & 0 & 0 & \varepsilon \\ 1 & 1 & 0 & 0 & \mathbf{1} \end{smallmatrix}\right]\theta\left[\begin{smallmatrix} E & 0 & 1 & 1 & \varepsilon \\ 0 & 1 & 1 & 1 & \mathbf{0} \end{smallmatrix}\right]\theta\left[\begin{smallmatrix} E & 0 & 1 & 1 & \varepsilon \\ 1 & 0 & 0 & 0 & \mathbf{1} \end{smallmatrix}\right] \\
& \theta\left[\begin{smallmatrix} 1+E & 1 & 0 & 0 & \varepsilon \\ 0 & 0 & 1 & 0 & \mathbf{0} \end{smallmatrix}\right]\theta\left[\begin{smallmatrix} 1+E & 1 & 0 & 0 & \varepsilon \\ 1 & 1 & 0 & 1 & \mathbf{1} \end{smallmatrix}\right]\theta\left[\begin{smallmatrix} 1+E & 1 & 1 & 1 & \varepsilon \\ 0 & 1 & 1 & 0 & \mathbf{0} \end{smallmatrix}\right]\theta\left[\begin{smallmatrix} 1+E & 1 & 1 & 1 & \varepsilon \\ 1 & 0 & 0 & 1 & \mathbf{1} \end{smallmatrix}\right]
\end{aligned} \tag{3.3.1}$$

where for $\varepsilon = (\varepsilon_1, \ldots, \varepsilon_{g-4})$, we denote $E = \varepsilon_1 + \cdots + \varepsilon_{g-4} \in \mathbb{Z}/2\mathbb{Z}$. Given three maps $a, b, c\colon (\mathbb{Z}/2\mathbb{Z})^{g-4} \to \{\pm 1\}$, define

$$s_{34}^{a,b,c} = \sum_{\varepsilon \in (\mathbb{Z}/2\mathbb{Z})^{g-4}} a_\varepsilon \sqrt{RR^1_{34,\varepsilon}} + b_\varepsilon \sqrt{RR^2_{34,\varepsilon}} + c_\varepsilon \sqrt{RR^3_{34,\varepsilon}}\,. \tag{3.3.2}$$

We take the product

$$S_{34} = \prod_{\substack{a,b,c \\ a_{0,0,\ldots,0}=1}} s_{34}^{a,b,c} \tag{3.3.3}$$

to get a polynomial in the theta constants of degree $4 \cdot 2^{3\cdot 2^{g-4}-1} = 2^{3\cdot 2^{g-4}+1}$. For any $3 \leq j < k \leq g$, let $RR^1_{jk,\varepsilon}$, $RR^2_{jk,\varepsilon}$, $RR^3_{jk,\varepsilon}$, $s_{jk}^{a,b,c}$, S_{jk} be obtained from $RR^1_{34,\varepsilon}$, $RR^2_{34,\varepsilon}$, $RR^3_{34,\varepsilon}$, $s_{34}^{a,b,c}$, S_{34} by swapping the columns $3, j$ and $4, k$ in all the characteristics.

Theorem 3.3.1 ([59, Main Theorem])**.** *The equations $\{S_{jk}\}_{3\leq j<k\leq g}$ cut out a locus in $\mathcal{A}_g(4,8)$ that contains the Schottky locus as an irreducible component.*

Observe that there are $\binom{g-2}{2} = \frac{(g-2)(g-3)}{2}$ equations S_{jk}, which is exactly the same number as the codimension of $\mathcal{J}_g$ inside $\mathcal{A}_g$.

Remark 3.3.2. *In the genus 5 case, we have three equations S_{34}, S_{35} and S_{45}. We know from a result by Donagi [54] that these equations define extra components in addition to the Schottky locus, namely the intermediate Jacobian locus coming from cubic threefolds.*

Numerical computations

For numerical computations, instead of checking that the product in (3.3.3) vanishes, we directly evaluate the expressions in (3.3.2) to reduce the numerical error. To determine if a matrix $\tau \in \mathbb{H}_g$ is in the vanishing locus of S_{jk}, we compute the smallest absolute value of the expressions in (3.3.2) and check if it is smaller than some numerical tolerance. This procedure gives a real number for each S_{jk}, and to determine if τ is in the locus defined by all the S_{jk}'s, we take the maximum of these numbers and check if it is smaller than a numerical tolerance.

We implement this for genus 5 in the function `fgsm()` in our package `Theta.jl` from Section 2.3. Using the same example matrix τ from Section 2.3, the function `fgsm(`τ`)` gives us the output 7.850462293418876e-16. This is expected since τ is the Jacobian of a genus 5 curve.

Accola's equations in genus 5

A solution to the weak Schottky problem in genus 5 was given already by Accola [1] in 1983, in the form of eight equations in the theta constants whose zero locus contains the Schottky locus as an irreducible component. To describe these equations, we first introduce some definitions.

Definition 3.3.3 (Azygetic basis). *An azygetic basis of $(\mathbb{Z}/2\mathbb{Z})^{2g}$ is an ordered set of distinct elements $(v_1, \dots, v_{2g+1})$ such that*

1. *The v_i generate $(\mathbb{Z}/2\mathbb{Z})^{2g}$.*
2. *$\sum_{i=1}^{2g+1} v_i = 0$.*
3. *$e(v_i, v_j) = -1$ for all $i \neq j$, where $e(v, v') = (-1)^{\varepsilon^t \delta' - \varepsilon'^t \delta}$ for $v = \begin{pmatrix} \varepsilon \\ \delta \end{pmatrix}$, $v' = \begin{pmatrix} \varepsilon' \\ \delta' \end{pmatrix}$.*

Example 3.3.4. *Mumford [94, Section 9] gives the following example of an azygetic basis.*

$$\begin{gathered} v_1 = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 \end{bmatrix}, v_2 = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 1 & 1 & 0 & \cdots & 0 \end{bmatrix}, \dots, v_g = \begin{bmatrix} 0 & 0 & 0 & \cdots & 1 \\ 1 & 1 & 1 & \cdots & 1 \end{bmatrix}, \\ v_{g+1} = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \end{bmatrix}, v_{g+2} = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 \end{bmatrix}, \dots, v_{2g} = \begin{bmatrix} 0 & 0 & 0 & \cdots & 1 \\ 1 & 1 & 1 & \cdots & 0 \end{bmatrix} \\ M = \sum_{i=1}^{2g} v_i = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 1 & \cdots & 1 \end{bmatrix}. \end{gathered} \tag{3.3.4}$$

The characteristics $v_1, \dots, v_g$ are odd whereas $v_{g+1}, \dots, v_{2g}$ and M are even (refer to the start of Section 3.2 for definitions). Any other azygetic basis can be obtained from this one via the action of the symplectic group $\mathrm{Sp}(2g, \mathbb{Z}/2\mathbb{Z})$ on $(\mathbb{Z}/2\mathbb{Z})^{2g}$, acting as the subgroup of $GL(2g, \mathbb{Z}/2\mathbb{Z})$ with the symplectic form $e(\cdot, \cdot)$.

Definition 3.3.5 (Hyperelliptic fundamental system)**.** *A hyperelliptic fundamental system in genus* 5 *is a set of eleven characteristics* $\{m_1, \ldots, m_{11}\} \subset (\mathbb{Z}/2\mathbb{Z})^{10}$ *such that*

1. *The* m_i *are all even.*

2. *The set is azygetic, i.e.* $e(m_i + m_j + m_k) = -1$ *for all pairwise distinct* i, j, k*.*

3. *The sum of an even number of the* m_i *is not zero.*

Example 3.3.6. *Let* $(v_1, \ldots, v_{10}, M)$ *be the azygetic basis from Example 3.3.4. Then*

$$v_6, \ldots, v_{10}, v_1 + M, \ldots, v_4 + M, \alpha, \alpha + M\,, \tag{3.3.5}$$

where $\alpha = \sum_{i=1}^{4} v_i$*, is a hyperelliptic fundamental system. We can write this explicitly as*

$$\begin{gathered}\begin{bmatrix}1&0&0&0&0\\0&0&0&0&0\end{bmatrix}, \begin{bmatrix}0&1&0&0&0\\1&0&0&0&0\end{bmatrix}, \begin{bmatrix}0&0&1&0&0\\1&1&0&0&0\end{bmatrix}, \begin{bmatrix}0&0&0&1&0\\1&1&1&0&0\end{bmatrix},\\ \begin{bmatrix}0&0&0&0&1\\1&1&1&1&0\end{bmatrix}, \begin{bmatrix}1&0&0&0&0\\0&1&1&1&1\end{bmatrix}, \begin{bmatrix}0&1&0&0&0\\0&0&1&1&1\end{bmatrix}, \begin{bmatrix}0&0&1&0&0\\0&0&0&1&1\end{bmatrix},\\ \begin{bmatrix}0&0&0&1&0\\0&0&0&0&1\end{bmatrix}, \begin{bmatrix}1&1&1&1&0\\0&1&0&1&0\end{bmatrix}, \begin{bmatrix}1&1&1&1&0\\1&0&1&0&1\end{bmatrix}.\end{gathered} \tag{3.3.6}$$

Given a hyperelliptic fundamental system $m_1, \ldots, m_{11}$, we denote by $n = \sum_{i=1}^{11} m_i$ the sum and we also denote $a_i = n + m_i$. Now consider the subgroup

$$G_8^{1234} = \langle a_5 + a_6 + a_7 + a_8, a_5 + a_6 + a_9 + a_{10}, a_5 + a_7 + a_9 + a_{11} \rangle \subset (\mathbb{Z}/2\mathbb{Z})^{2g}\,. \tag{3.3.7}$$

This has 8 elements and $e(m_i + s) = 1$ for all $s \in G_8^{1234}$, $i = 1, 2, 3, 4$. Define

$$r_i(\tau) = \prod_{s \in G_8^{1234}} \theta[m_i + s](0, \tau)\,, \qquad \text{for } i = 1, 2, 3, 4\,. \tag{3.3.8}$$

These are monomials of degree 8 in the theta constants, with product

$$SR_{1234} = \prod_{a,b,c=\pm 1} (\sqrt{r_1} + a\sqrt{r_2} + b\sqrt{r_3} + c\sqrt{r_4}) = \left(\sum_i r_i^2 - 2\sum_{i<j} r_i r_j\right)^2 - 64 r_1 r_2 r_3 r_4\,. \tag{3.3.9}$$

This is a polynomial of degree 4 in the r_i's, hence of degree 32 in the theta constants. Moreover, for any $k = 5, \ldots, 11$, we can define the group G_8^{123k} by swapping k with 4 in the definition of G_8^{1234}. This changes the monomials r_i in (3.3.8), to give us new polynomials SR_{123k}.

Theorem 3.3.7. *[1] The zero locus of the polynomials* SR_{123k}*, for* $k = 4, \ldots, 11$*, contains the Schottky locus* $\mathcal{J}_5$ *as an irreducible component.*

Remark 3.3.8. *It is not known whether Accola's equations contain components apart from the Schottky locus. It would be interesting to study whether the equations vanish on the Intermediate Jacobian locus.*

Numerical computations

Similarly to the equations in (3.3.3), instead of checking if the product in (3.3.9) vanishes, we directly evaluate the factors to reduce the numerical error. To determine if a matrix $\tau \in \mathbb{H}^5$ is in the vanishing locus of (3.3.9), we compute the smallest absolute value of the eight factors and check if it is smaller than some numerical tolerance. This procedure gives a real number for each k, and to determine if τ is in the locus defined by all the SR_{123k}, we take the maximum of these numbers and check if it is smaller than a numerical tolerance.

We implement this in the function `accola()` in our package `Theta.jl` from Section 2.3. Again using the example τ from Section 2.3, the function `accola(`τ`)` gives us the output 3.062334813867916e-9, which is expected since τ is in the Schottky locus.

3.4 Conclusion

In this chapter, we discussed the classical Schottky problem in genus four and five. We describe Igusa's solution in genus four, which we implement numerically. We also implement an algorithm to recover a canonical embedding of a genus four curve, given its Riemann matrix. In genus five, the Schottky problem is open, and we describe two weak solutions which we implement numerically. In the next chapter, we present a solution to a variant of the Schottky problem for genus five Jacobians with a vanishing theta null. In Chapter 5, we will discuss the tropical Schottky problem, which is the analogue of the Schottky problem in tropical geometry.

Chapter 4

Schottky problem for genus five Jacobians with a vanishing theta null

In this chapter, we present a solution to a variant of the weak Schottky problem in genus five, for Jacobians with a vanishing theta null. The material in this chapter is from the paper "On the Schottky problem for genus five Jacobians with a vanishing theta null" authored with Daniele Agostini, which will appear in Annali della Scuola Normale Superiore di Pisa, Classe di Scienze [4].

4.1 Introduction

We focus on Jacobians with a vanishing theta null, which is an even two-torsion point in the theta divisor Θ. The abelian varieties with this property have been intensely studied [20, 50, 71, 72, 93] and they form a divisor θ_{null} in $\mathcal{A}_g$. The Schottky problem in this case becomes that of recognizing $\mathcal{J}_g \cap \theta_{\text{null}}$ inside θ_{null}.

The first observation is that a vanishing theta null is automatically a singular point of the theta divisor. Hence, following the Andreotti-Mayer philosophy, one is led to study the local structure of Θ around the singular point, and the first natural invariant is the *rank of the quadric tangent cone.* More precisely, if the divisor is cut out by a theta function, $\Theta = \{\theta = 0\}$, then the quadric tangent cone $Q_p\Theta$ at $p \in \Theta^{sing}$ is defined by the Hessian matrix evaluated at p:

$$Q_p\Theta \sim \begin{pmatrix} \frac{\partial^2\theta}{\partial {z_1}^2} & \frac{\partial^2\theta}{\partial z_1 \partial z_2} & \cdots & \frac{\partial^2\theta}{\partial z_1 \partial z_g} \\ \frac{\partial^2\theta}{\partial z_1 \partial z_2} & \frac{\partial^2\theta}{\partial {z_2}^2} & \cdots & \frac{\partial^2\theta}{\partial z_2 \partial z_g} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial^2\theta}{\partial z_1 \partial z_g} & \frac{\partial^2\theta}{\partial z_2 \partial z_g} & \cdots & \frac{\partial^2\theta}{\partial z_g^2} \end{pmatrix}. \tag{4.1.1}$$

The rank of $Q_p\Theta$ is the rank of the Hessian. This leads to a stratification of θ_{null}, first introduced by Grushevsky and Salvati Manni [71],

$$\theta^0_{\mathrm{null}} \subseteq \theta^1_{\mathrm{null}} \subseteq \cdots \subseteq \theta^{g-1}_{\mathrm{null}} \subseteq \theta^g_{\mathrm{null}} = \theta_{\mathrm{null}} \tag{4.1.2}$$

where θ^h_{null} is the locus of abelian varieties with a vanishing theta null, with a quadric tangent cone of rank at most h. In particular, if a Jacobian has a vanishing theta null, then a result of Kempf [80] shows that the quadric tangent cone has rank at most three, hence

$$\mathcal{J}_g \cap \theta_{\mathrm{null}} \subseteq \theta^3_{\mathrm{null}} \, . \tag{4.1.3}$$

Grushevsky and Salvati Manni proved in [71] that this inclusion is actually an equality in genus 4, confirming a conjecture of H. Farkas. In the same paper, they ask whether $\mathcal{J}_g \cap \theta_{\mathrm{null}}$ is an irreducible component of θ^3_{null} in higher genera, which would imply a solution to the weak Schottky problem for Jacobians with a vanishing theta null. Our main result is an affirmative answer to this question in genus 5.

Theorem 4.1.1. *In genus five, the locus $\mathcal{J}_5 \cap \theta_{null}$ is an irreducible component of θ^3_{null}.*

This solution to the weak Schottky problem is very much in the classical spirit of finding explicit equations in the period matrix. Indeed, the condition of having an even two-torsion point in the theta divisor can be checked by evaluating the theta function at these (finitely many) points, and then the rank of the Hessian can be computed numerically. We include an example of this computation in Example 4.4.9.

The strategy of our proof is to bound the dimension of θ^3_{null}, by working over a partial compactification $\overline{\mathcal{A}_g}^1 = \mathcal{A}_g \cup \partial\mathcal{A}_g$ of $\mathcal{A}_g$, following [72]. Via a study of nodal curves with a theta characteristic, we can describe the intersection $(\mathcal{J}_5 \cap \theta_{\mathrm{null}}) \cap \partial\mathcal{A}_g$. We can then bound the dimension $\theta^3_{\mathrm{null}} \cap \partial\mathcal{A}_g$ via a study of the ramification loci, or Thom-Boardman loci, for the Gauss map of the theta divisor, leading to the proof of our main theorem. In particular, the study of these ramification loci fits with classical and recent work on the Gauss map [2, 10, 14, 46, 82], and might give a way to extend our main result in higher dimensions.

4.2 Singularities of theta divisors at points of order two

For a general ppav $(A, \Theta) \in \mathcal{A}_g$, the theta divisor is smooth. The locus $N_0 \subseteq \mathcal{A}_g$ where the theta divisor is singular is called the Andreotti-Mayer locus, and it is a divisor in $\mathcal{A}_g$ [11]. Mumford [93], Beauville [20] and Debarre [50] proved that N_0 has two irreducible components θ_{null} and N_0'. The component θ_{null} is the locus where the theta divisor contains an even two-torsion point of A, a so-called *vanishing theta null*, and N_0' is the residual component. Theta divisors containing even two-torsion points correspond to period matrices τ such that $\theta[m](0, \tau) = 0$ for some even characteristic m. These points are always singular, since all the derivatives $\frac{\partial\theta[m]}{\partial z_i}$ are odd. Moreover, we can give explicit equations for the lift of θ_{null} in $\mathcal{A}_g(4,8)$ as

$$\theta_{\text{null}} = \{\tau \mid \theta[m](0,\tau) = 0, \text{ for some even characteristic } m\} \; . \tag{4.2.1}$$

Thus, on $\mathcal{A}_g(4,8)$ the divisor θ_{null} splits into irreducible components corresponding to the even characteristics, and these components are all conjugate under the action of Γ_g.

As explained in Section 4.1, the rank of the quadric tangent cone at the vanishing theta null leads to a stratification

$$\theta^0_{\text{null}} \subseteq \theta^1_{\text{null}} \subseteq \cdots \subseteq \theta^{g-1}_{\text{null}} \subseteq \theta^g_{\text{null}} = \theta_{\text{null}} \tag{4.2.2}$$

where θ^h_{null} is the locus of ppav whose theta divisor contain an even two-torsion point with a quadric tangent cone of rank at most h. In $\mathcal{A}_g(4,8)$, the locus θ^h_{null} is given by the equations

$$\begin{aligned}\theta^h_{\text{null}} &= \left\{\tau \in \mathcal{A}_g(4,8) \mid \exists\, m \text{ even: } \theta[m](0,\tau) = 0, \;\operatorname{rk}\left(\frac{\partial^2\theta[m]}{\partial z_i \partial z_j}(0,\tau)\right) \leq h\right\} \\ &= \left\{\tau \in \mathcal{A}_g(4,8) \mid \exists\, m \text{ even: } \theta[m](0,\tau) = 0, \;\operatorname{rk}\left((1+\delta_{ij})\frac{\partial\theta[m]}{\partial\tau_{ij}}(0,\tau)\right) \leq h\right\}\end{aligned} \tag{4.2.3}$$

where the second equality comes from the heat equation (2.1.4). One should be slightly careful with this description because, as noted by Grushevsky and Salvati Manni, the condition $\left\{\operatorname{rk}\left((1+\delta_{ij})\frac{\partial\theta[m]}{\partial\tau_{ij}}(0,\tau)\right) \leq h\right\}$ is not well-defined on $\mathcal{A}_g(4,8)$; it is well-defined only together with the condition $\{\theta[m](0,\tau) = 0\}$. An alternative set of equations that fixes this problem is given in [71].

If C is a smooth curve of genus g, a vanishing theta null on the Jacobian $J(C)$ corresponds to an even theta characteristic κ such that $h^0(C,\kappa) \geq 2$. As explained in Section 4.1,

$$\mathcal{J}_g \cap \theta_{\text{null}} \subseteq \theta^3_{\text{null}} \, . \tag{4.2.4}$$

In [71], it was proved that this is an equality in genus four, and it was asked whether $\mathcal{J}_g \cap \theta_{\text{null}}$ is an irreducible component of θ^3_{null} in higher genus. In the rest of this paper, we will discuss this problem and present a proof for genus five.

4.3 Partial compactification and Gauss maps

Our strategy is to bound the dimension of the irreducible component of θ^3_{null} which contains $\mathcal{J}_g \cap \theta_{\text{null}}$. To do so, we will use a partial compactification of $\mathcal{A}_g$.

Partial compactification of $\mathcal{A}_g$

The idea is to follow the strategy of [72], by studying the boundary of θ^3_{null} inside the partial compactification $\overline{\mathcal{A}}^1_g = \mathcal{A}_g \cup \partial\mathcal{A}_g$ of $\mathcal{A}_g$. This was introduced by [74] and then studied by

Mumford [93]. The boundary divisor $\partial\mathcal{A}_g$ parametrizes rank one degenerations of ppavs, which we briefly describe here, referring to [93] for more details. Let $(B,\Xi) \in \mathcal{A}_{g-1}$ be a ppav and let G be an algebraic group, which is an extension of B by $\mathbb{C}^*$:

$$0 \longrightarrow \mathbb{C}^* \longrightarrow G \longrightarrow B \longrightarrow 0\,. \tag{4.3.1}$$

Then we can look at G as a $\mathbb{C}^*$-bundle on B, which can be completed naturally to a $\mathbb{P}^1$-bundle, together with two sections B_0, B_∞. These sections can be glued together via translation by a point $b \in B$, and the resulting variety $\overline{G}$ is a limit of abelian varieties. It also carries a divisor $D \subseteq \overline{G}$, which is a limit of theta divisors. Thus, the boundary divisor is a fibration $p\colon \partial\mathcal{A}_g \to \mathcal{A}_{g-1}$, with fiber $B/\operatorname{Aut}(B,\Xi)$ over $(B,\Xi) \in \mathcal{A}_{g-1}$, and the general fiber is $B/\langle\pm 1\rangle$, the Kummer variety of B. Analytically, points on the boundary can be seen as limits of $g \times g$ period matrices $\tau = \tau(t)$ such that the imaginary part of τ_{gg} goes to $+\infty$ as $t \to 0$, and all the other coordinates converge. Hence, the limit has the form

$$\tau = \begin{pmatrix} \tau' & z' \\ z'^t & i\infty \end{pmatrix} \tag{4.3.2}$$

where τ' is the period matrix of $(B,\Xi) \in \mathcal{A}_{g-1}$ and z' represents the translation point $b \in B$. Hence we see that, at least around a point $(B,\Xi) \in \mathcal{A}_{g-1}$, we have a surjective map

$$\mathcal{X}_{g-1} \to \partial\mathcal{A}_{g-1} \tag{4.3.3}$$

that over (B,Ξ) corresponds to $B \to B/\operatorname{Aut}(B)$.

The boundary of the theta null divisor in the partial compactification was computed by Mumford [93].

Theorem 4.3.1 (Mumford)**.** *Let θ_{null} be the closure of the theta null divisor in $\overline{\mathcal{A}}^1_g$. Then*

$$\theta_{null} \cap \partial\mathcal{A}_{g-1} = \left(\bigcup_{(B,\Xi)} 2_B(\Xi) \right) \cup p^{-1}(\theta_{null,g-1}) \tag{4.3.4}$$

where $2_B(\Xi) = \{2x \,|\, x \in \Xi\}$ is the image of the divisor under the multiplication map.

More precisely, by $\bigcup 2_B(\Xi)$ we mean the image of the universal double theta divisor under the map $\mathcal{X}_{g-1} \to \partial\mathcal{A}_{g-1}$. We denote this component by X_g and sometimes we will not distinguish whether we take it in $\mathcal{X}_{g-1}$ or in $\partial\mathcal{A}_{g-1}$. We can write

$$X_g = \{(2z',\tau') \,|\, \theta'(z',\tau') = 0\} \tag{4.3.5}$$

where now θ' is the Riemann theta function in genus $g-1$. The intersections of the strata θ^h_{null} with X_g were determined by Grushevsky and Salvati Manni [72].

Theorem 4.3.2 (Grushevsky, Salvati Manni)**.** *Denote again by θ^h_{null} the closure in $\overline{\mathcal{A}}^1_g$ of the corresponding stratum in $\mathcal{A}_g$. Define the matrix*

$$D\gamma(z',\tau') := \begin{pmatrix} \frac{\partial^2\theta'}{\partial {z'_1}^2} & \frac{\partial^2\theta'}{\partial z'_1\partial z'_2} & \cdots & \frac{\partial\theta'}{\partial z'_1\partial z'_{g-1}} & \frac{\partial\theta'}{\partial z'_1} \\ \frac{\partial^2\theta'}{\partial z'_1\partial z'_2} & \frac{\partial^2\theta'}{\partial {z'_2}^2} & \cdots & \frac{\partial\theta'}{\partial z'_2\partial z'_{g-1}} & \frac{\partial\theta'}{\partial z'_2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \frac{\partial^2\theta'}{\partial z'_1\partial z'_{g-1}} & \frac{\partial^2\theta'}{\partial z'_2\partial z'_{g-1}} & \cdots & \frac{\partial\theta'}{\partial z'^2_{g-1}} & \frac{\partial\theta'}{\partial z'_{g-1}} \\ \frac{\partial\theta'}{\partial z'_1} & \frac{\partial\theta'}{\partial z'_2} & \cdots & \frac{\partial\theta'}{\partial z'_{g-1}} & 0 \end{pmatrix} \tag{4.3.6}$$

evaluated at (z',τ'). Then

$$\theta^h_{null} \cap X_g = \{(2z',\tau') \,|\, \theta'(z',\tau') = 0,\ \operatorname{rk} D\gamma(z',\tau') \le h\}\ . \tag{4.3.7}$$

Thom-Boardman loci of the Gauss map

The last result is best understood in terms of the Gauss map for the theta divisor. If $(B,\Xi) \in \mathcal{A}_{g-1}$ is a ppav, then the Gauss map is the rational map

$$\gamma\colon \Xi \dashrightarrow \mathbb{P}(T_0B) \tag{4.3.8}$$

that associates to each smooth point $p \in \Xi$ the tangent space $T_p\Xi$, seen as a subspace of T_0B via translation by p. The base locus of the map is precisely the singular locus of Ξ, and if $\Xi = \{\theta'(z',\tau') = 0\}$, then the Gauss map can be written explicitly as

$$\gamma = \left[\frac{\partial\theta'}{\partial z'_1}, \dots, \frac{\partial\theta'}{\partial z_{g-1}}\right]\ . \tag{4.3.9}$$

The Gauss map is related to Theorem 4.3.2 by the following result, whose proof is the same as [72, Lemma 2]; see also [49, 102].

Lemma 4.3.3. *Let $(B,\Xi) \in \mathcal{A}_{g-1}$ be a ppav, with the theta divisor given as $\Xi = \{\theta'(z',\tau') = 0\}$. If $z' \in \Xi$ is a smooth point, then*

$$\operatorname{rk} D\gamma(z',\tau') \le h \qquad \textit{if and only if} \qquad \operatorname{rk} d\gamma_{z'} \le h-2 \tag{4.3.10}$$

where $d\gamma_{z'}$ is the differential of the Gauss map at z'. If instead $z' \in \Xi$ is a singular point,

$$\operatorname{rk} D\gamma(z',\tau') \le h \qquad \textit{if and only if} \qquad \operatorname{rk} Q_{z'}\Xi \le h \tag{4.3.11}$$

where $Q_{z'}\Xi$ is the quadric tangent cone to Ξ at z'.

For a map $f\colon X \to Y$ between two smooth connected varieties, the (closed) *Thom-Boardman loci* are defined as

$$\Sigma^i(f) := \{p \in X \mid \dim\ker df_p \geq i\}\,, \tag{4.3.12}$$

$$\Sigma_i(f) := \Sigma^{\dim X - i}(f) = \{p \in X \mid \operatorname{rk} df_p \leq i\}\,. \tag{4.3.13}$$

Hence we can interpret Lemma 4.3.3 as saying that for a theta divisor $\Xi_{\tau'} = \{\theta'(z',\tau') = 0\}$, the locus of smooth points where $\operatorname{rk} D\gamma(z',\tau') \leq h$ coincides with the Thom-Boardman locus $\Sigma_{h-2}(\gamma_{\tau'})$ of the Gauss map $\gamma_{\tau'}\colon \Xi^{sm}_{\tau'} \to \mathbb{P}^{g-2}$. Moreover, Lemma 4.3.3 suggests also that the Thom-Boardman loci can be naturally extended to a closed subset of Ξ by

$$\overline{\Sigma}_{h-2}(\gamma_{\tau'}) = \Sigma_{h-2}(\gamma_{\tau'}) \cup \{z' \in \Xi^{sing} \mid \operatorname{rk} Q_{z'}\Xi_{\tau'} \leq h\}\,. \tag{4.3.14}$$

Thus Theorem 4.3.2 can be rephrased as saying that

$$\theta^h_{\text{null}} \cap X_g = \bigcup_{(B,\Xi)\in\mathcal{A}_{g-1}} 2_B(\overline{\Sigma}_{h-2}(\gamma_\Xi))\,, \tag{4.3.15}$$

where the set on the right can be viewed as the universal second multiple of the Thom-Boardman locus inside the universal family $\mathcal{X}_{g-1} \to \mathcal{A}_{g-1}$. Observe that this is well-defined in $\mathcal{X}_{g-1}$ because of the multiplication by two.

4.4 Jacobians with a vanishing theta null in genus five

Now we turn to the proof of our main theorem. To begin with, we observe that $\mathcal{J}_g \cap \theta_{\text{null}}$ is the image under the Torelli map of the locus of curves with a vanishing theta null. It was proved by Teixidor [115] that this is an irreducible divisor in $\mathcal{M}_g$, and since the Torelli map is injective, we see that $\mathcal{J}_g \cap \theta_{\text{null}}$ is irreducible of dimension $3g-4$. What we need to prove is that the irreducible component $\mathcal{Z}_g$ of θ^3_{null} which contains $\mathcal{J}_g \cap \theta_{\text{null}}$ has the same dimension. Equivalently, we can compute the codimension inside the divisor θ_{null}, and we expect that

$$\operatorname{codim}_{\theta_{\text{null}}}(\mathcal{Z}_g) \geq \operatorname{codim}_{\theta_{\text{null}}}(\mathcal{J}_g \cap \theta_{\text{null}}) = \frac{g(g+1)}{2} - 1 - (3g-4) = \frac{1}{2}(g-2)(g-3)\,. \tag{4.4.1}$$

We can bound the codimension of $\mathcal{Z}_g$ by considering its intersection with X_g. More precisely, we proceed in two steps.

1. Prove that $\mathcal{J}_g \cap \theta_{\text{null}}$ intersects X_g at a smooth point of θ_{null}. Then $\mathcal{Z}_g$ also intersects X_g at a smooth point of θ_{null}, and it is a standard fact that $\operatorname{codim}_{\theta_{\text{null}}} \mathcal{Z}_g \geq \operatorname{codim}_{X_g}(\mathcal{Z}_g \cap X_g)$.
2. Show that $\operatorname{codim}_{X_g}(\theta^3_{\text{null}} \cap X_g) \geq \frac{1}{2}(g-2)(g-3)$. Then $\operatorname{codim}_{X_g}(\mathcal{Z}_g \cap X_g) \geq \frac{1}{2}(g-2)(g-3)$, and from the previous step we have $\operatorname{codim}_{\theta_{\text{null}}} \mathcal{Z}_g \geq \frac{1}{2}(g-2)(g-3)$ as well.

We proceed to carry out these steps in genus five.

Limits of Jacobians in the partial compactification

Here we consider points in the intersection $\mathcal{J}_g \cap \partial\mathcal{A}_g$ coming from nodal curves. Let C be a smooth and irreducible curve of genus $g-1 \geq 4$ with two distinct marked points $p, q \in C$, and let $\overline{C}$ be the nodal curve obtained by identifying these two points. This is a stable curve of arithmetic genus g and the map $\nu\colon C \to \overline{C}$ is the normalization.

The group $\operatorname{Pic}^0(\overline{C})$ fits naturally into an exact sequence [12]

$$0 \longrightarrow \mathbb{C}^* \longrightarrow \operatorname{Pic}^0(\overline{C}) \xrightarrow{\nu^*} J(C) \longrightarrow 0 \tag{4.4.2}$$

where $J(C) = \operatorname{Pic}^0(C)$ is the Jacobian of C. This says that a bundle $\overline{L}$ on $\overline{C}$ is equivalent to a bundle L on C, together with an identification of the two fibers $L(p), L(q)$, which is given by an element in $\mathbb{C}^*$. Hence we see that $\operatorname{Pic}^0(\overline{C})$ is a rank one extension of the ppav $J(C)$, as in (4.3.1). Moreover, in this situation we also have a natural element in $J(C)$ given by $\mathcal{O}(p-q)$. According to the description of Section 4.3, this gives us an element in $\mathcal{J}_g \cap \partial\mathcal{A}_g$.

Now we consider nodal curves with a vanishing theta null, following Cornalba's construction [47, Example 3.2, Example 6.2].

Lemma 4.4.1. *Let L be a line bundle on C such that $2L \sim K_C + p + q$. Then L descends to a line bundle $\overline{L}$ on $\overline{C}$ such that $2\overline{L} \sim K_{\overline{C}}$ and $h^0(\overline{C}, \overline{L}) = h^0(C, L)$.*

Proof. We sketch the proof here, referring to [47] for more details. First we observe that $\deg L = g-1$, and the Riemann-Roch theorem shows that $h^0(C, L-p-q) = h^0(C,L) - 1$, so the linear system of L does not separate the two points p, q. Moreover, this shows that there is a section $\sigma_0 \in H^0(C, L)$ that does not vanish at either p or q; in fact σ_0 does not vanish at both points. Indeed, suppose that $\sigma_0(q) = 0$ and $\sigma_0(p) \neq 0$. Then σ_0^2 is a section of $2L(-q) \sim K_C + p - q$ that does not vanish at p, which cannot happen because p is a base point of $K_C + p - q$, since C has positive genus.

Hence, we can identify the two fibers of $L(p)$, $L(q)$ by identifying $\sigma_0(p)$ with $\sigma_0(q)$. This induces a line bundle $\overline{L}$ on $\overline{C}$ such that $2\overline{L} \sim K_{\overline{C}}$, and the sections $H^0(\overline{C}, \overline{L})$ correspond to sections $\sigma \in H^0(C, L)$ such that $\sigma(p) = \sigma(q)$. Moreover, we know that $H^0(C, L)$ does not separate p, q, which means precisely that $H^0(\overline{C}, \overline{L}) = H^0(C, L)$. □

According to [47], this gives a theta characteristic on $\overline{C}$, and if $h^0(C, L) = 2$, we get that $h^0(\overline{C}, \overline{L}) = 2$, so this is an even and effective theta characteristic on $\overline{C}$. This actually gives an element in $(\mathcal{J}_g \cap \theta_{\text{null}}) \cap X_g$ as follows.

Lemma 4.4.2. *Let L be a line bundle on C such that $2L \sim K_C + p + q$ and $h^0(C, L) = 2$. Then $(J(C), \mathcal{O}(p-q))$ gives a point in $(\mathcal{J}_g \cap \theta_{null}) \cap X_g$.*

Proof. According to the description of Section 4.3, we need to show that $\mathcal{O}(p-q) \in 2\cdot\Theta$, where $\Theta \subseteq J(C)$ is a symmetric theta divisor. Recall that all the symmetric theta divisors on $J(C)$ are of the form $W_{g-2}(C) - \kappa$, where $W_{g-2}(C) = \{M \in \operatorname{Pic}^{g-2}(C) \mid h^0(C, M) > 0\}$, and κ is a theta characteristic, hence $2 \cdot \Theta = 2 \cdot W_{g-2}(C) - K_C$. Then we observe that $L(-q) \in W_{g-2}(C)$ and moreover $2L(-q) \sim K_C + p - q$, so $p - q \sim 2L(-q) - K_C \in 2 \cdot W_{g-2}(C) - K_C$. □

Via this construction, we obtain many points in $(\mathcal{J}_g \cap \theta_{\text{null}}) \cap X_g$ and we can give conditions for these to be smooth points of θ_{null}. This is done in the next two lemmas.

Lemma 4.4.3. *Let $(B, \Xi) \in \mathcal{A}_{g-1}$ be such that $\operatorname{Aut}(B, \Xi) = \{\pm 1\}$ and let $b \in 2_B(\Xi)$ be a point such that*

1. *b is not a two-torsion point.*
2. *The set $2_B^{-1}(b) \cap \Xi$ consists precisely of one point b'.*
3. *The point b' has multiplicity at most two in Ξ.*

Then (B, Ξ) and b give a smooth point of X_g which is also a smooth point of θ_{null}.

Proof. First observe that X_g is a component of the intersection of the two divisors θ_{null} and $\partial\mathcal{A}_g$, so a smooth point in X_g is smooth in both θ_{null} and $\partial\mathcal{A}_g$. Hence it is enough to prove smoothness in X_g.

To do so, we look at the point $(b, (B, \Xi))$ in the universal abelian variety $\mathcal{X}_{g-1}$; this gives a point in $\partial\mathcal{A}_g$ via the map $\mathcal{X}_{g-1} \to \partial\mathcal{A}_g$ of (4.3.3). Since we are assuming that (B, Ξ) has no extra automorphisms and that b is not a two-torsion point, we see that the map is a local isomorphism around $(b, (B, \Xi))$, hence we can work in $\mathcal{X}_{g-1}$ instead of in $\partial\mathcal{A}_g$. Moreover, the fact that (B, Ξ) has no extra automorphisms also tells us that the map $\mathcal{X}_g(4, 8) \to \mathcal{X}_g$ is a local isomorphism around $(b, (B, \Xi))$. So we can work directly inside $\mathcal{X}_g(4, 8)$, where we can look at $X_g = \bigcup_{(B,\Xi)} 2_B(\Xi)$ as the image of the universal theta divisor $\Xi_{g-1} = \bigcup_{(B,\Xi)} \Xi$ under the global multiplication-by-two map $2\colon \mathcal{X}_{g-1}(4, 8) \to \mathcal{X}_{g-1}(4, 8)$.

Now, our second assumption on b shows that the fiber of this map over $(b, (B, \Xi))$ consists of a single point $(b', (B, \Xi))$. We also know that the differential of the multiplication-by-2 map is just the usual scalar multiplication by 2, so it is an isomorphism. Hence, the tangent space to X_g at $(b, (B, \Xi))$ is isomorphic to the tangent space to the universal theta divisor Ξ_{g-1} at $(b', (B, \Xi))$. In local coordinates (z', τ'), the universal theta divisor is given by $\{\theta(z', \tau') = 0\}$, and the heat equation shows that a point (z', τ') is singular if and only if z' is a singular point of $\Xi_{\tau'}$ of multiplicity at least 3, which in our case is ruled out by the third assumption. □

Lemma 4.4.4. *Let C be a smooth curve of genus $g - 1 \geq 4$ with only trivial automorphisms and let $D \in C_{g-3}$ be an effective divisor such that*

1. *$h^0(C, D) = 1$.*
2. *$K_C - 2D \sim p + q$ with p, q two distinct points on C.*
3. *$h^0(C, \eta + D) = 0$ for each $\eta \in \operatorname{Pic}^0(C)[2] \setminus \{\mathcal{O}_C\}$.*

Then $J(C)$ together with the point $\mathcal{O}(p - q)$ give a point in $(\mathcal{J}_g \cap \theta_{null}) \cap X_g$ which is a smooth point of θ_{null}.

Proof. First we observe that $\deg(K_C - 2D) = 2(g-1) - 2 - 2(g-3) = 2$, and since the curve is not hyperelliptic, this implies $h^0(C, K_C - 2D) \leq 1$, so the points p, q in (2) are uniquely determined.

We then apply Lemma 4.4.3. Since the automorphism group of C is trivial, Torelli's theorem implies that $J(C)$ has no extra automorphisms. Moreover, if κ is any theta characteristic on C, we can fix the symmetric theta divisor given by $W_{g-2}(C) - \kappa$, and twice the theta divisor is $2W_{g-2}(C) - K_C$. Then $\mathcal{O}(p-q) \in 2W_{g-2}(C) - K_C$, since if we set $L = \mathcal{O}(D+p+q)$, then $2L \sim K_C + p + q$ because of assumption (2). Reasoning as in the proof of Lemma 4.4.1, we get that $h^0(C, L) = h^0(C, D) + 1 = 2$, and also $h^0(C, L(-p)) = h^0(C, L(-q)) = h^0(C, L) - 1 = 1$. Hence $p - q \sim 2L(-q) - K_C$, with $L(-q) \in W_{g-2}(C)$.

Now we check the three conditions of Lemma 4.4.3. We see that $\mathcal{O}(p-q)$ cannot be a two-torsion point, because otherwise $2p \sim 2q$, but p, q are distinct and C is not hyperelliptic. For the second condition, since $p - q \sim 2L(-q) - K_C$, we see that

$$2^{-1}_{J(C)}(p-q) \cap (W_{g-2}(C) - \kappa) \cong \{L(-q) + \eta \,|\, \eta \in J(C)[2],\, h^0(L + \eta - q) > 0\}\,. \qquad (4.4.3)$$

For any $\eta \in \operatorname{Pic}^0(C)[2]$, we see that $2(L+\eta) \sim 2L \sim K_C + p + q$, hence from the proof of Lemma 4.4.1, $h^0(C, L + \eta - q) = h^0(C, L + \eta) - 1 = h^0(C, L + \eta - p - q) = h^0(C, D + \eta)$. Thus assumption (3) implies that the intersection (4.4.3) consists of the unique point $L(-q)$.

For the last condition, we need to check that $L(-q)$ has multiplicity at most two in the theta divisor $W_{g-2}(C)$. But Riemann's singularity theorem shows that $\operatorname{mult}_{L(-q)} W_{g-2}(C) = h^0(C, L - q) = h^0(C, L)$, and $h^0(C, L) = 1$ by assumption (1). □

We now specialize this discussion to $g = 5$.

Proposition 4.4.5. *$\mathcal{J}_5 \cap \theta_{null}$ and X_5 intersect at a smooth point of θ_{null}.*

Proof. We follow Lemma 4.4.4. Let C be a general curve of genus 4, with only trivial automorphisms. We consider the locus

$$Z = \{D \in C_2 \,|\, h^0(C, K_C - 2D) > 0\} \qquad (4.4.4)$$

and we show that a general element in Z satisfies the three conditions of Lemma 4.4.4. First, we compute the dimension of Z. The condition $h^0(C, K_C - 2D) > 0$ is equivalent to the fact that the evaluation map $\mathrm{ev}_D \colon H^0(C, K_C) \to H^0(C, K_C \otimes \mathcal{O}_{2D})$ is not injective, or not an isomorphism, since $h^0(C, K_C) = h^0(C, K_C \otimes \mathcal{O}_{2D}) = 4$. The evaluation map globalizes to a map of rank four bundles $\mathrm{ev} \colon H^0(C, K_C) \otimes \mathcal{O}_{C_2} \to E$ on C_2, where the fiber of E at $D \in C_2$ is precisely $H^0(C, K_C \otimes \mathcal{O}_{2D})$. Thus, Z is precisely the degeneracy locus of the global evaluation map. In particular, if we can show that $Z \neq \emptyset$ and $Z \neq C_2$, it will follow that Z is a divisor in C_2. To prove this, let $x \in C$ be a general point, then $h^0(C, K_C - 2x) = 2$, so after removing the eventual base locus B, we get a map $\varphi \colon C \to \mathbb{P}^1$. If y is a point where φ is ramified, we see that $D = x + y \in Z$; if instead y' is a point outside of B where φ is not ramified, then $D' = x + y' \notin Z$.

Now we check the conditions in Lemma 4.4.4. If $D \in Z$, then $h^0(C,D)=1$, otherwise the curve would be hyperelliptic. For the second condition, suppose that $K_C - 2D \sim 2p$ for some $p \in C$. Then $K_C \sim 2D + 2p$, so $\mathcal{O}_C(D+p)$ is a theta characteristic on C. There are only finitely many effective theta characteristics κ and since C is general, they all satisfy $h^0(C,\kappa)=1$. Hence there are only finitely many such D, and since $\dim Z = 1$, a general D in any component of Z will give $K_C - 2D \sim p + q$ for two distinct points $p,q \in C$.

For the third condition, if we look at C_2 in $\operatorname{Pic}^2(C)$ via the Abel-Jacobi map, we see that $D \in Z$ satisfies the third condition precisely when $D \notin \bigcup_\eta (C_2 + \eta)$, as η varies in $J(C)[2] \setminus \{\mathcal{O}_C\}$. Suppose by contradiction that $Z \subseteq \bigcup_\eta (C_2+\eta)$ and let $Z' \subseteq Z$ be an irreducible component. Then there must be an $\eta \in J(C)[2] \setminus \{\mathcal{O}_C\}$ such that $Z' \subseteq C_2 + \eta$, so that $Z' \subseteq C_2 \cap (C_2 + \eta)$. In particular $\dim(C_2 \cap (C_2+\eta)) \geq 1$, and we will now prove that this cannot happen. To do so, observe that if $\dim(C_2 \cap (C_2+\eta)) \geq 1$, then the difference map

$$\phi_2 \colon C_2 \times C_2 \longrightarrow \operatorname{Pic}^0(C)\,, \qquad (D,E) \mapsto D - E \tag{4.4.5}$$

has a positive-dimensional fiber at η, and by [13, Exercise V.D-4] this is possible only if $\eta \cong \mathcal{O}(x-y)$ for two distinct points $x,y \in C$, or if $\eta \cong M_1 - M_2 \cong 2M_1 - K_C$, where M_1 is one $\mathfrak{g}^1_3$ on C and $M_2 = K_C - M_1$ is the other. The first possibility cannot happen because then $2x \sim 2y$, and C is not hyperelliptic. For the second possibility, observe that if $2M_1 - K_C$ is two-torsion, then $4M_1 \sim 2K_C$. Since C is not hyperelliptic, we know from Noether's theorem that it is projectively normal in the canonical embedding $C \subseteq \mathbb{P}^3$, hence $4M_1 \sim 2K_C$ if and only if for every divisor $H \in |M_1|$, the divisor $4H$ is cut out by a quadric in $\mathbb{P}^3$. Using Macaulay2 [69], we can easily find a curve where this does not happen, for example the curve $C = \{X_0X_3 - X_1X_2 = X_0^3 + X_0^2X_1 + X_1^3 + X_2^3 + X_3^3 = 0\}$ and the divisor $H = C \cap \{X_2 = X_3 = 0\}$. □

Thom-Boardman loci for the Gauss map in dimension 4

Now we need to bound the codimension of $\theta^3_{\text{null}} \cap X_g$ inside X_g, and by (4.3.15), we can do it by studying the Thom-Boardman loci in one dimension less.

Lemma 4.4.6. *Suppose that*

$$\operatorname{codim}_{\mathcal{A}_{g-1}}\{(B,\Xi) \mid \dim \overline{\Sigma}_1(\gamma_\Xi) \geq i\} \geq i + \frac{(g-2)(g-5)}{2}\,, \qquad \text{for } i = 0,\ldots,g-2\,. \tag{4.4.6}$$

Then

$$\operatorname{codim}_{X_g}(\theta^3_{null} \cap X_g) \geq \frac{1}{2}(g-2)(g-3)\,. \tag{4.4.7}$$

Proof. We know from (4.3.15) that $\theta^3_{\text{null}} \cap X_g = \bigcup_{(B,\Xi)} 2_B(\overline{\Sigma}_1(\gamma_\Xi))$, and we can bound the dimension of this by bounding the dimension of the fibers and of the image along the projection $p \colon \theta^3_{\text{null}} \cap X_g \to \mathcal{A}_{g-1}$. More precisely we have

$$\dim \theta^3_{\text{null}} \cap X_g \leq \max_{i=0,\ldots,g-2} \left(i + \dim\{(B,\Xi) \in \mathcal{A}_{g-1} \mid \dim 2_B(\overline{\Sigma}_1(\gamma_\Xi)) \geq i\}\right)\,. \tag{4.4.8}$$

Since the multiplication $2_B\colon B \to B$ is a finite map, we can replace $\dim 2_B(\overline{\Sigma}_1(\gamma_\Xi)) \geq i$ by $\dim \overline{\Sigma}_1(\gamma_\Xi) \geq i$, and if we rephrase the previous inequality in terms of the codimension, we get exactly what we want. □

Remark 4.4.7. *When $g > 5$, Lemma 4.4.6 requires that the set*

$$\{(B,\Xi) \in \mathcal{A}_{g-1} \,|\, \dim \overline{\Sigma}_1(\gamma_\Xi) \geq 0\} = \{(B,\Xi) \in \mathcal{A}_{g-1} \,|\, \overline{\Sigma}_1(\gamma_\Xi) \neq \emptyset\} \qquad (4.4.9)$$

is a proper subset of $\mathcal{A}_{g-1}$. However, this cannot happen; indeed, if $(B,\Xi) \in \mathcal{A}_{g-1}$ is a general ppav, then Ξ contains $2^{g-1}(2^g-1)$ odd two-torsion points, corresponding to the odd characteristics. If Ξ is cut out by a theta function $\Xi = \{\theta'(z',\tau') = 0\}$ and z' is an odd two-torsion point, then one can see that $\operatorname{rk} D\gamma(z',\tau') \leq 2$, so $z' \in \Sigma_1(\gamma_\Xi)$.

However, when $g = 5$ the hypotheses of Lemma 4.4.6 are satisfied.

Proposition 4.4.8. *It holds that*

$$\operatorname{codim}_{X_5}(\theta^3_{null} \cap X_5) \geq 3\,. \qquad (4.4.10)$$

Proof. According to Lemma 4.4.6, we need to prove that

$$\operatorname{codim}_{\mathcal{A}_4}\{(B,\Xi) \,|\, \dim \overline{\Sigma}_1(\gamma_\Xi) \geq i\} \geq i\,, \qquad \text{for } i = 0,1,2,3\,. \qquad (4.4.11)$$

- For $i = 0$, this is immediate, though as observed in Remark 4.4.7, it is crucial that $g = 5$.

- For $i = 1$, we need to show that for a general $(B,\Xi) \in \mathcal{A}_4$, the Thom-Boardman locus $\overline{\Sigma}_1(\gamma_\Xi)$ is finite dimensional. This is proved by Adams, McCrory, Shifrin and Varley in [2], where they show that the locus consists exactly of the odd two-torsion points of Remark 4.4.7.

For the cases where $i > 1$, we start with a general observation. Assume that the Gauss map $\gamma_\Xi\colon \Xi^{sm} \to \mathbb{P}^3$ has finite fibers, then $\dim \Sigma_1(\gamma_\Xi) \leq 1$. Indeed, let $Z \subseteq \Sigma_1(\gamma_\Xi)$ be an irreducible component of positive dimension. By construction, the differential of the induced map $\gamma_{\Xi|Z}\colon Z \to \mathbb{P}^3$ has rank at most one at a general point of Z, so $\dim \gamma_\Xi(Z) \leq 1$ by generic smoothness. Since the map has finite fibers, it follows that $\dim Z \leq 1$. Hence if $i > 1$, we can have $\dim \overline{\Sigma}_1(\gamma_\Xi) \geq i$ if and only if the locus $\{z' \in \Xi^{sing} \,|\, \operatorname{rank} Q_{z'}\Xi \leq 3\}$ has dimension at least i.

- For $i = 2$, let $(B,\Xi) \in \mathcal{A}_4$ be such that Ξ is smooth. Then the Gauss map $\gamma_\Xi\colon \Xi \to \mathbb{P}^3$ is finite and the singular locus is empty, so the previous observation implies $\dim \overline{\Sigma}_1(\gamma_\Xi) \leq 1$. This proves that the locus $\{(B,\Xi) \,|\, \dim \overline{\Sigma}_1(\gamma_\Xi) \geq 2\}$ is contained in the divisor $N_{0,4} = \{(B,\Xi) \,|\, \Xi^{sing} \neq \emptyset\}$. This divisor has two irreducible components, which are exactly the theta null divisor $\theta_{\text{null},4}$ and the Jacobian locus $\mathcal{J}_4$ [20]. Now, let (B,Ξ) be the Jacobian of a hyperelliptic curve of genus 4. Then $(B,\Xi) \in \theta_{\text{null},4} \cap \mathcal{J}_4$ [20], and since it is a Jacobian, we know that the Gauss map $\gamma_\Xi\colon \Xi^{sm} \to \mathbb{P}^3$ has finite fibers [10]. Moreover, the singular locus of Ξ has dimension 1, so the previous observation gives $\dim \overline{\Sigma}(\gamma_\Xi) \leq 1$. This proves that the locus $\{(B, \Xi) \mid \dim \overline{\Sigma}_1(\gamma_\Xi) \geq 2\}$ does not contain the intersection $\theta_{\text{null},4} \cap \mathcal{J}_4$; in particular, it does not coincide with any of the two components, so it has codimension at least two.

- For $i = 3$, let $(B, \Xi) \in \mathcal{A}_4$ be such that Ξ is irreducible. Then $\dim \overline{\Sigma}_1(\gamma_\Xi) \geq 3$ if and only if $\overline{\Sigma}_1(\gamma_\Xi) = \Xi$, but this is impossible because the Gauss map is dominant, so its differential at a general point is an isomorphism. Hence, the locus $\{(B, \Xi) \mid \dim \overline{\Sigma}_1(\gamma_\Xi) \geq 3\}$ is contained in the locus of decomposable abelian varieties, which has codimension 3.

□

Proof of main theorem

We can finally prove our main theorem, and we rewrite the argument here for clarity.

Proof of Theorem 4.1.1. We want to show that $\mathcal{J}_5 \cap \theta_{\text{null}}$ is an irreducible component of θ^3_{null}. As remarked before, we know that $\mathcal{J}_5 \cap \theta_{\text{null}}$ is irreducible of dimension 11, thus if $\mathcal{Z}_5 \subseteq \theta^3_{\text{null}}$ is the irreducible component containing $\mathcal{J}_5 \cap \theta_{\text{null}}$, we need to show that $\dim \mathcal{Z}_5 \leq 11$, or equivalently, $\operatorname{codim}_{\theta_{\text{null}}} \mathcal{Z}_g \geq 3$. We consider the intersection with X_5 inside the partial compactification $\overline{\mathcal{A}_5}^1$; we know from Proposition 4.4.5 that $\mathcal{Z}_5$ and X_5 intersect in a smooth point of θ_{null}, hence $\operatorname{codim}_{\theta_{\text{null}}} \mathcal{Z}_5 \geq \operatorname{codim}_{X_5}(\mathcal{Z}_5 \cap X_5)$. It is enough to prove that this is at least 3, or more generally, that $\operatorname{codim}_{X_5}(\theta^3_{\text{null}} \cap X_5) \geq 3$. This is precisely the bound of Proposition 4.4.8. □

Example 4.4.9. *As we have observed in Section 4.1, this solution to the Schottky problem is effective, since the condition of having a vanishing theta null with a quadric cone of rank at most three can be checked explicitly. We present here an explicit example, where we use the Julia package for theta functions presented in Section 2. We use the same curve and period matrix $\tau \in \mathbb{H}_5$ from Section 2.3, given by*

$$\begin{pmatrix}
0.40243 + 0.68413i & -0.18138 + 0.21894i & 0.24323 - 0.13416i & 0.00403 + 0.05085i & -0.31818 + 0.14383i \\
-0.18137 + 0.21894i & 0.27914 + 1.01836i & -0.09799 + 0.46222i & -0.06566 + 0.60959i & -0.14647 + 0.37006i \\
0.24323 - 0.13416i & -0.09799 + 0.46222i & 0.16663 + 0.68136i & -0.28606 + 0.02038i & 0.18558 - 0.15061i \\
0.00403 + 0.05085i & -0.06566 + 0.60959i & -0.28606 + 0.02038i & 0.04136 + 1.40560i & 0.19025 + 0.82885i \\
-0.31818 + 0.14384i & -0.14647 + 0.37006i & 0.18558 - 0.15061i & 0.19025 + 0.82885i & 0.74873 + 1.01168i
\end{pmatrix}$$

We can computationally check that the theta constant with even characteristic

$$m = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \end{bmatrix} \tag{4.4.12}$$

vanishes at τ. Moreover, we can compute the corresponding Hessian matrix

$$\begin{pmatrix}
-2.79665 + 5.29764i & -9.57825 - 9.04671i & 7.36305 + 2.28697i & 7.58338 + 5.34729i & 6.15667 - 1.90199i \\
-9.57825 - 9.04671i & 18.9738 + 8.34582i & -23.1027 - 3.10545i & -9.31944 - 0.822821i & 0.524289 - 3.64991i \\
7.36305 + 2.28697i & -23.1027 - 3.10545i & 16.8441 - 1.15986i & 13.9363 - 4.56541i & -3.32248 + 4.10698i \\
7.58338 + 5.34729i & -9.31944 - 0.822821i & 13.9363 - 4.56541i & 2.89309 + 1.21773i & 3.86617 - 0.546202i \\
6.15667 - 1.90199i & 0.524289 - 3.64991i & -3.32248 + 4.10698i & 3.86617 - 0.546202i & -12.9726 - 1.928i
\end{pmatrix}$$

The Hessian has the following eigenvalues:

$$\begin{gathered}
47.946229109152995 + 9.4919321440352 98i \\
-15.491689246713147 + 3.3401255907497958i \\
-9.512858919129267 - 1.0587349322052013i \\
-2.7271385943272036 \times 10^{-15} - 1.1117459994936022i \times 10^{-14} \\
-5.698014266322794 \times 10^{-15} + 6.342925068807627i \times 10^{-15}
\end{gathered}$$

so it is natural to expect that $\tau \in \theta^3_{null}$. Indeed, τ is the Jacobian of the genus five curve C obtained as the normalization of the singular plane octic

$$\{x^6y^2-4x^4y^2-2x^3y^3-2x^4y+2x^3y+4x^2y^2+3xy^3+y^4+4x^2y+2xy^2+x^2-4xy-2y^2-2x+1=0\}\,.$$

Using Macaulay2, we can write the equations of C in the canonical embedding and check that it is contained in a quadric of rank 3, so it has a vanishing theta null. To compute τ from C, we use the package [35] in Sage [103].

4.5 Conclusion

In this chapter, we presented a solution to a variant of the weak Schottky problem in genus five, for Jacobians with a vanishing theta null. In the next chapter, we will discuss the tropical Schottky problem, which is the analogue of the Schottky problem in tropical geometry.

Chapter 5

Tropical Schottky problem

In this chapter, we describe the tropical Schottky problem, which is the analogue of the Schottky problem in the combinatorial setting of tropical geometry. The material in this chapter is from the paper “From Curves to Tropical Jacobians and Back” authored with Barbara Bolognese and Madeline Brandt, which is published in Combinatorial Algebraic Geometry [27], and the paper “Schottky Algorithms: Classical meets Tropical” authored with Mario Kummer and Bernd Sturmfels, which is published in Mathematics of Computation [43].

5.1 Introduction

The Schottky problem also exists in tropical geometry [91]. The *tropical Siegel space* $\mathbb{H}_g^{trop}$ is the cone of positive definite $g \times g$-matrices, endowed with the fan structure given by the second Voronoi decomposition. The *tropical Schottky locus* $\mathcal{J}_g^{trop}$ is the subfan indexed by cographic matroids [32, Theorem 5.2.4]. A detailed analysis for $g \leq 5$ is found in [37, Theorem 6.4]. It is known, e.g. by [32, §6.3], that the inclusion $\mathcal{J}_g^{trop} \subset \mathbb{H}_g^{trop}$ correctly tropicalizes the complex-analytic inclusion $\mathcal{J}_g \subset \mathbb{H}_g$. However, it has been an open problem (suggested in [101, §9]) to find a direct link between the equations that govern these two inclusions.

We here solve this problem, and develop computational tools for the tropical Schottky problem. We distinguish between the *Schottky Decision Problem* and the *Schottky Recovery Problem.* For the former, the input is a matrix τ in $\mathbb{H}_g^{trop}$, possibly depending on parameters, and we must decide whether τ lies in $\mathcal{J}_g^{trop}$. For the latter, τ already passed that test, and we compute a curve whose Jacobian is given by τ.

Our main results in Section 5.2 are Algorithms 5.3.3 and 5.3.5. Based on the work in [56, 57, 118, 120], these furnish a computational solution to the tropical Schottky problem. Key ingredients are cographic matroids and the f-vectors of Voronoi polytopes.

Section 5.4 links the classical and tropical Schottky scenarios. Theorem 5.4.2 expresses the edge lengths of a metric graph in terms of tropical theta constants, and Theorem 5.4.9 explains what happens to the Schottky–Igusa modular form in the tropical limit. We found it especially gratifying to discover how the cographic locus is encoded in the classical theory.

The software we describe in this paper is made available at the supplementary website

$$\texttt{http://eecs.berkeley.edu/\~{}chualynn/schottky} \tag{5.1.1}$$

5.2 Tropical Jacobians

Curves, their Jacobians, and the Schottky locus have natural counterparts in the combinatorial setting of tropical geometry. We review the basics from [27, 32, 37, 91]. The role of a curve is played by a connected metric graph $\Gamma = (V, E, l, w)$. This has vertex set V, edge set E, a length function $l : E \to \mathbb{R}_{>0}$, and a weight function $w : V \to \mathbb{Z}_{\geq 0}$. The genus of Γ is

$$g \;=\; |E| - |V| + 1 + \sum_{v \in V} w(v). \tag{5.2.1}$$

The moduli space $\mathcal{M}_g^{trop}$ comprises all metric graphs of genus g. This is a stacky fan of dimension $3g-3$. See [37, Figure 4] for a colorful illustration. The tropical Torelli map $\mathcal{M}_g^{trop} \to \mathbb{H}_g^{trop}$ takes Γ to its (symmetric and positive semidefinite) Riemann matrix Q_Γ.

Fix a basis for the integral homology $H_1(\Gamma, \mathbb{Z}) \simeq \mathbb{Z}^g$. Beside the usual cycles in Γ, this group has $w(v)$ generators for the virtual cycles at each vertex v. Let B denote the $g \times |E|$ matrix whose columns record the coefficients of each edge in the basis vectors. Let D be the $|E| \times |E|$ diagonal matrix whose entries are the edge lengths. The *Riemann matrix* of Γ is

$$Q_\Gamma \;=\; B \cdot D \cdot B^t. \tag{5.2.2}$$

One way to choose a basis is to fix an orientation and a spanning tree of Γ. Each edge not in that tree then determines a cycle with ±1-coefficients. Changing the basis of $H_1(\Gamma, \mathbb{Z})$ corresponds to the action of $GL_g(\mathbb{Z})$ on Q_Γ by conjugation.

Example 5.2.1. *Consider the complete graph on 4 vertices in Figure 5.1.*

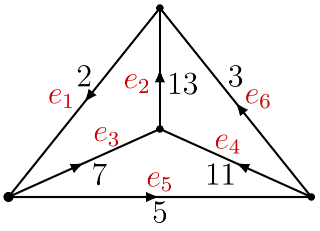


Figure 5.1: The metric graph and edge orientation used in Example 5.2.1.

We indicate in the figure an arbitrary choice of the edge orientations, and we choose the spanning tree consisting of the edges $T = \{e_2, e_3, e_4\}$. This corresponds to the cycle basis

$\omega_1 = e_1 + e_3 + e_2$, $\omega_2 = -e_3 + e_5 + e_4$, and $\omega_3 = -e_2 - e_4 + e_6$. Next, we compute the matrix B as

$$B = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & -1 & 1 & 0 & 1 & 0 \\ -1 & 0 & -1 & 0 & 0 & 1 \end{pmatrix} . \tag{5.2.3}$$

Let D be the 6×6 diagonal matrix with entries $13, 7, 11, 2, 5, 3$ along the diagonal. The period matrix is then

$$Q_\Gamma = BDB^T = \begin{pmatrix} 22 & -7 & -13 \\ -7 & 23 & -11 \\ -13 & -11 & 27 \end{pmatrix} . \tag{5.2.4}$$

The matrix Q_Γ has rank $g - \sum_{v \in V} w(v)$. We defined $\mathbb{H}_g^{trop}$ with positive definite matrices. Those have rank g. For that reason, we now restrict to graphs with zero weights, i.e. $w \equiv 0$.

The *tropical Schottky locus* $\mathcal{J}_g^{trop}$ is the set of all matrices (5.2.2), where $\Gamma = (V, E, l)$ runs over graphs of genus g, and B runs over their cycle bases. This set is known as the *cographic locus* in $\mathbb{H}_g^{trop}$, because the $g \times |E|$ matrix B is a representation of the *cographic matroid* of Γ.

The Schottky Decision Problem asks for a test of membership in $\mathcal{J}_g^{trop}$. To be precise, given a positive definite matrix Q, does there exist a metric graph Γ such that $Q = Q_\Gamma$?

To address this question, we need the polyhedral fan structures on $\mathcal{J}_g^{trop}$ and $\mathbb{H}_g^{trop}$. Let $G = (V, E)$ be the graph underlying Γ, with $E = \{e_1, e_2, \ldots, e_m\}$. Fix a cycle basis as above. Let $b_1, b_2, \ldots, b_m$ be the column vectors of the $g \times m$-matrix B. Formula (5.2.2) is equivalent to

$$Q_\Gamma \;=\; l(e_1) b_1 b_1^t + l(e_2) b_2 b_2^t + \cdots + l(e_m) b_m b_m^t. \tag{5.2.5}$$

The cone of all Riemann matrices for the graph G, allowing the edge lengths to vary, is

$$\sigma_{G,B} \;=\; \mathbb{R}_{>0} \bigl\{ b_1 b_1^t,\, b_2 b_2^t,\, \ldots\, ,\, b_m b_m^t \bigr\} . \tag{5.2.6}$$

This is a relatively open rational convex polyhedral cone, spanned by matrices of rank 1. The collection of all cones $\sigma_{G,B}$ is a polyhedral fan whose support is the Schottky locus $\mathcal{J}_g^{trop}$.

This fan is a subfan of the *second Voronoi decomposition* of the cone $\mathbb{H}_g^{trop}$ of positive definite matrices. The latter fan is defined as follows. Fix a Riemann matrix $Q \in \mathbb{H}_g^{trop}$ and consider its quadratic form $\mathbb{Z}^g \to \mathbb{R}$, $x \mapsto x^t Q x$. The values of this quadratic form define a regular polyhedral subdivision of $\mathbb{R}^g$ with vertices at $\mathbb{Z}^g$. This is denoted $\mathrm{Del}(Q)$ and known as the *Delaunay subdivision* of Q.

Example 5.2.2. *Consider the matrix $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$. The function $l_Q : \mathbb{Z}^2 \to \mathbb{Z}^2 \times \mathbb{R}$ is given by $(x, y) \mapsto (x, y, x^2)$. If we now take the convex hull of the points in the image of l_Q, we obtain the picture in Figure 5.2 on the left, together with the Delaunay subdivision on the right.*

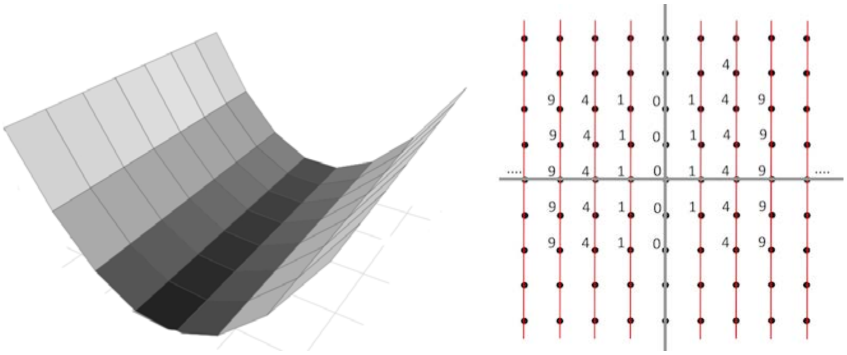


Figure 5.2: The weight function induced by the quadratic form in Example 5.2.2 on the left, and the corresponding Delaunay subdivision on the right.

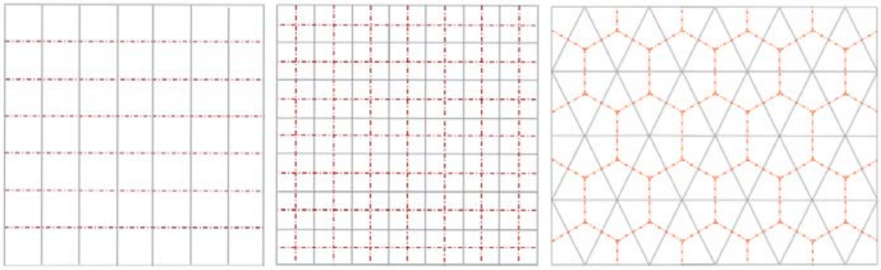


Figure 5.3: Delaunay decompositions of $\mathbb{R}^2$ (solid lines) and their associated Voronoi decompositions (dotted lines).

Dual to $\mathrm{Del}(Q)$ is the *Voronoi decomposition* of $\mathbb{R}^g$. This is illustrated in Figure 5.3 for $g = 2$. The cells of the Voronoi decomposition of Q are the lattice translates of the *Voronoi polytope*

$$\left\{\, p \in \mathbb{R}^g \;:\; 2p^tQx \leq x^tQx \;\text{ for all } x \in \mathbb{Z}^g \,\right\}. \tag{5.2.7}$$

This is the set of points in $\mathbb{R}^g$ for which the origin is the closest lattice point, in the norm given by Q. If Q is generic then the Delaunay subdivision is a triangulation and the Voronoi polytope (5.2.7) is simple. It is dual to the link of the origin in the simplicial complex $\mathrm{Del}(Q)$.

The structures above represent principally polarized abelian varieties in tropical geometry. A tropical abelian variety is the torus $\mathbb{R}^g/\mathbb{Z}^g$ together with a quadratic form $Q \in \mathbb{H}_g^{trop}$. The *tropical theta divisor* is given by the codimension one cells in the induced Voronoi decomposition of $\mathbb{R}^g/\mathbb{Z}^g$.

It is possible to give a more manageable description of the tropical theta divisor in virtue of Theorem 5.2.3, as we are about to explain. Let $\Gamma = (G, w, l)$ be a weighted metric graph, and let $p_0 \in \Gamma$ be a fixed basepoint. Let $\omega_1, \ldots, \omega_g$ be a basis of $H_1(G, \mathbb{Z})$. For any point p in Γ, let $c(p) = \sum_i a_i e_i$ describe any path from p_0 to p. Then, take the inner product of $c(p)$ with each element of the cycle basis to obtain a point of $\mathbb{R}^g/\Lambda$, which does not depend on the choice of path from p_0 to p. By the identification with $\mathbb{R}^g/\mathbb{Z}^g$ induced by the choice of cycle basis, this defines a point $\mu(p)$ of the tropical Jacobian. We may extend this map linearly so that it is defined on all divisors on Γ. By a *divisor* on Γ, we mean a finite formal integer linear combination of points in Γ. Then the map μ is called the *tropical Abel-Jacobi map* [91].

Given a divisor $D = \sum_i a_i p_i$, where $a_i \in \mathbb{Z}$ and $p_i \in \Gamma$, define the *degree* of D as $\sum_i a_i$. We say that D is *effective* if $a_i \geq 0$ for all i. Let W_{g-1} be the image of degree $g-1$ effective divisors under the tropical Abel-Jacobi map.

Theorem 5.2.3 (Corollary 8.6, [91])**.** *The set W_{g-1} is the tropical theta divisor up to translation.*

Example 5.2.4 (Example 5.2.1, Continued)**.** *Delaunay subdivisions also arise in many other branches of mathematics, for example in lattice packing or covering problems. In this context, Sikirić wrote a* `GAP` *[66] software package* `polyhedral` *[56]. Using this package, we compute that the Delaunay subdivision of the quadratic form in Equation 5.2.4 is given by six tetrahedra in the unit cube, all of which share the great diagonal as an edge. We also compute using* `polyhedral` *the Voronoi decomposition dual to this Delaunay subdivision, which gives a tiling of $\mathbb{R}^3$ by permutohedra as illustrated in Figure 5.4. This is the tropical theta divisor, with f-vector $(6, 12, 7)$. In Figure 5.5, we illustrate the correspondence described by Theorem 5.2.3 between W_2 and the tropical theta divisor.*

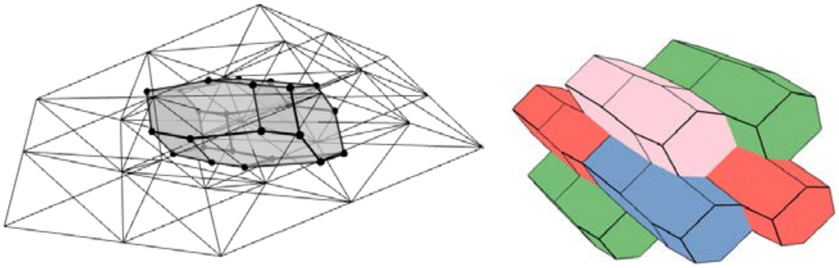


Figure 5.4: The left figure shows the Delaunay subdivision by tetrahedra and a dual permutohedron in grey. The right figure illustrates a tiling of $\mathbb{R}^3$ by permutohedra. The polytopes were computed using the `polyhedral` package of `GAP` [56] and the figures were created using `polymake` [67].

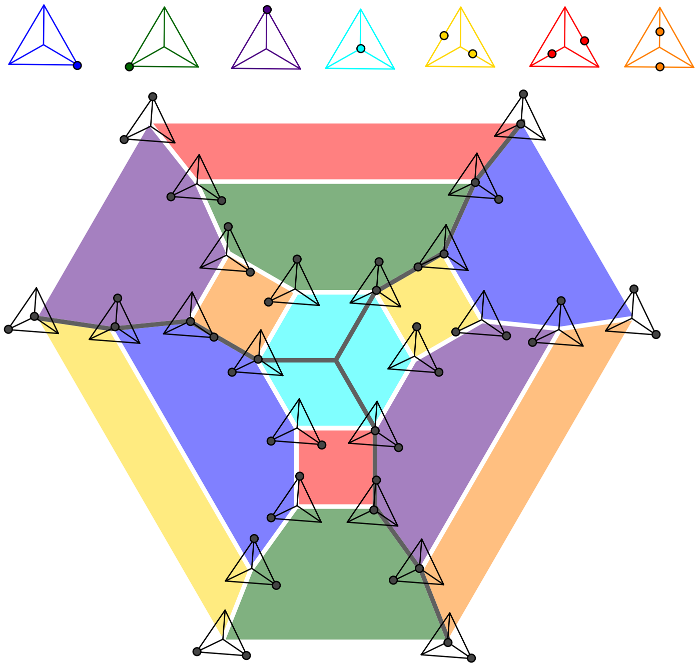


Figure 5.5: Each vertex of the permutohedron corresponds to a divisor supported on the vertices of Γ. The square faces correspond to divisors supported on the interiors of edges of Γ which do not meet in a vertex. Each hexagonal face corresponds to divisors which are supported on edges of Γ which are adjacent to a fixed vertex. Then, the edges correspond to keeping one point of the divisor fixed, and moving the other point along an edge of Γ. The grey curve depicted above represents the embedding of Γ into its Jacobian under the Abel-Jacobi map, which, under the identifications, is again K_4.

5.3 Tropical Schottky problem

We now fix an arbitrary Delaunay subdivision D of $\mathbb{R}^g$. Its *secondary cone* is defined as

$$\sigma_D \;=\; \left\{ Q \in \mathbb{H}_g^{trop} \;|\; \mathrm{Del}(Q) = D \right\}. \tag{5.3.1}$$

This is a relatively open convex polyhedral cone. It consists of positive definite matrices Q whose Voronoi polytopes (5.2.7) have the same normal fan. The group $\mathrm{G}L_g(\mathbb{Z})$ acts on the set of secondary cones. In his classical reduction theory for quadratic forms, Voronoi [120] proved that the cones σ_D form a polyhedral fan, now known as the *second Voronoi decomposition* of $\mathbb{H}_g^{trop}$, and that there are only finitely many secondary cones σ_D up to the action of $\mathrm{G}L_g(\mathbb{Z})$. The following summarizes characteristic features for matrices in the Schottky locus $\mathcal{J}_g^{trop}$.

Proposition 5.3.1. *Fix a graph G with metric D, homology basis B, and Riemann matrix $Q = BDB^t$. The Voronoi polytope (5.2.7) is affinely isomorphic to the zonotope $\sum_{i=1}^m [-b_i, b_i]$. The secondary cone $\sigma_{\mathrm{Del}(Q)}$ is spanned by the rank one matrices $b_i b_i^t$: it equals $\sigma_{G,B}$ in (5.2.6).*

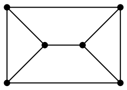
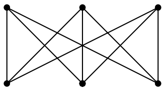
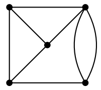
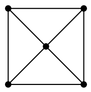
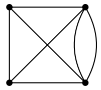
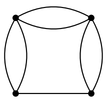
Proof. This can be extracted from Vallentin's thesis [118]. The affine isomorphism is given by the invertible matrix Q, as explained in item iii) of [118, §3.3.1]. The Voronoi polytope being the zonotope $\sum_{i=1}^m [-b_i, b_i]$ follows from the discussion on cographic lattices in [118, §3.5]. The result for the secondary cone is derived from [118, §2.6]. See [118, §4] for many examples. □

We now fix $g = 4$. Vallentin [118, §4.4.6] lists all 52 combinatorial types of Delaunay subdivisions of $\mathbb{Z}^4$. His table contains the f-vectors of all 52 Voronoi polytopes. Precisely 16 of these types are cographic, and these comprise the Schottky locus $\mathcal{J}_4^{trop}$. These are described in rows 3 to 18 of the table in [118, §4.4.6]. We reproduce the relevant data in Table 5.1. The following key lemma is found by inspecting Vallentin's list of f-vectors.

Lemma 5.3.2. *The f-vectors of the* 16 *Voronoi polytopes representing the Schottky locus $\mathcal{J}_4^{trop}$ are distinct from the f-vectors of the other* 36 *Voronoi polytopes, corresponding to $\mathbb{H}_4^{trop} \backslash \mathcal{J}_4^{trop}$.*

This lemma gives rise to the following method for the tropical Schottky decision problem.

Algorithm 5.3.3 (Tropical Schottky Decision)**.** *Input: $Q \in \mathbb{H}_4^{trop}$. Output: Yes, if $Q \in \mathcal{J}_4^{trop}$.*
1. Compute the Voronoi polytope in (5.2.7) for the quadratic form Q.
2. Determine the f-vector (f_0, f_1, f_2, f_3) of this 4-dimensional polytope.
3. Check whether this f-vector appears in our Table 5.1. Output "Yes" if this holds.

Graph G	Riemann matrix Q_Γ	f_0	f_1	f_2	f_3	Dimension of σ_D
	$\begin{pmatrix} 3 & 1 & -1 & 0 \\ 1 & 4 & 1 & 1 \\ -1 & 1 & 4 & -1 \\ 0 & 1 & -1 & 3 \end{pmatrix}$	96	198	130	28	9
	$\begin{pmatrix} 4 & 2 & -2 & -1 \\ 2 & 4 & -1 & -2 \\ -2 & -1 & 4 & 2 \\ -1 & -2 & 2 & 4 \end{pmatrix}$	102	216	144	30	9
	$\begin{pmatrix} 2 & 0 & -1 & 0 \\ 0 & 3 & 1 & 1 \\ -1 & 1 & 4 & -1 \\ 0 & 1 & -1 & 3 \end{pmatrix}$	72	150	102	24	8
	$\begin{pmatrix} 3 & 2 & 1 & -1 \\ 2 & 4 & 2 & -1 \\ 1 & 2 & 4 & 1 \\ -1 & -1 & 1 & 3 \end{pmatrix}$	78	168	116	26	8
	$\begin{pmatrix} 3 & 1 & -1 & -1 \\ 1 & 3 & 1 & 1 \\ -1 & 1 & 3 & 2 \\ -1 & 1 & 2 & 3 \end{pmatrix}$	60	134	98	24	7
	$\begin{pmatrix} 2 & 0 & -1 & -1 \\ 0 & 2 & -1 & -1 \\ -1 & -1 & 4 & 3 \\ -1 & -1 & 3 & 4 \end{pmatrix}$	54	116	84	22	7

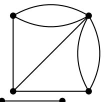
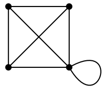
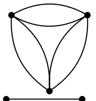
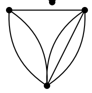
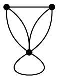
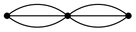
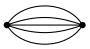
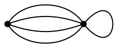
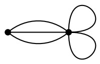
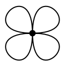
	$\begin{pmatrix} 2 & 0 & -1 & 0 \\ 0 & 2 & 0 & -1 \\ -1 & 0 & 3 & 1 \\ 0 & -1 & 1 & 3 \end{pmatrix}$	54	114	80	20	7
	$\begin{pmatrix} 3 & 1 & -1 & 0 \\ 1 & 3 & 1 & 0 \\ -1 & 1 & 3 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	48	96	64	16	7
	$\begin{pmatrix} 2 & 0 & -1 & -1 \\ 0 & 2 & 1 & 1 \\ -1 & 1 & 3 & 2 \\ -1 & 1 & 2 & 3 \end{pmatrix}$	46	108	84	22	6
	$\begin{pmatrix} 2 & -1 & -1 & -1 \\ -1 & 3 & 2 & 2 \\ -1 & 2 & 3 & 2 \\ -1 & 2 & 2 & 3 \end{pmatrix}$	42	94	72	20	6
	$\begin{pmatrix} 2 & 1 & 1 & 0 \\ 1 & 3 & 2 & 0 \\ 1 & 2 & 3 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	36	74	52	14	6
	$\begin{pmatrix} 2 & 1 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 1 & 2 \end{pmatrix}$	36	72	48	12	6
	$\begin{pmatrix} 2 & 1 & 1 & 1 \\ 1 & 2 & 1 & 1 \\ 1 & 1 & 2 & 1 \\ 1 & 1 & 1 & 2 \end{pmatrix}$	30	70	60	20	5
	$\begin{pmatrix} 2 & 1 & 1 & 0 \\ 1 & 2 & 1 & 0 \\ 1 & 1 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	28	62	48	14	5
	$\begin{pmatrix} 2 & 1 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	24	48	34	10	5
	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	16	32	24	8	4

Table 5.1: The tropical Schottky locus for $g = 4$

We implemented Algorithm 5.3.3 using existing software for polyhedral geometry, namely the `GAP` package `polyhedral` due to Dutour Sikirić [56, 57], as well as Joswig's `polymake` [67].

The first column of Table 5.1 shows all relevant graphs G of genus 4. The second column gives a representative Riemann matrix. Here all edges have length 1 and a cycle basis B was chosen. Using (5.2.6), we also precomputed the secondary cones $\sigma_{G,B}$ for the 16 representatives.

Example 5.3.4. *Using the `GAP` package `polyhedral` [56] we compute the Voronoi polytope of*

$$Q = \begin{pmatrix} 14 & -9 & 11 & 0 \\ -9 & 11 & -2 & 1 \\ 11 & -2 & 21 & 11 \\ 0 & 1 & 11 & 14 \end{pmatrix}.$$

Its f-vector is $(62, 142, 104, 24)$. This does not appear in Table 5.1. Hence Q is not in $\mathcal{J}_4^{trop}$.

We now address the Schottky Recovery Problem. The input is a matrix $Q \in \mathcal{J}_4^{trop}$. From Algorithm 5.3.3 we know the f-vector of the Voronoi polytope. Using Table 5.1, this uniquely identifies the graph G. Note that our graphs G are dual to those in [118, §4.4.4]. From our precomputed list, we also know the secondary cone $\sigma_{G,B}$ for some choice of basis B.

Algorithm 5.3.5 (Tropical Schottky Recovery)**.** *Input:* $Q \in \mathcal{J}_4^{trop}$.
Output: A metric graph Γ *whose Riemann matrix* Q_Γ *equals* Q.
1. Identify the underlying graph G *from Table 5.1. Retrieve the basis* B *and the cone* $\sigma_{G,B}$.
2. Let $D = \mathrm{Del}(Q)$ *and compute the secondary cone* σ_D *as in (5.3.1).*
3. The cones σ_D *and* $\sigma_{G,B}$ *are related by a linear transformation* $X \in GL_4(\mathbb{Z})$. *Compute* X.
4. The matrix X^tQX *lies in* $\sigma_{G,B}$. *Compute* $\ell_1, \ldots, \ell_m$ *such that* $X^tQX = \sum_{i=1}^m \ell_i b_i b_i^t$.
5. Output the graph G *with length* ℓ_i *for its i-th edge, corresponding to the column* b_i *of* B.

We implemented this algorithm as follows. Step 2 can be done using `polyhedral` [56]. This code computes the secondary cone σ_D containing a given positive definite matrix Q. The matrix $X \in \mathrm{G}L_4(\mathbb{Z})$ in Step 3 is also found by `polyhedral`, but with external calls to the package `isom` due to Plesken and Souvignier [98]. We refer to [57, §4] for details. For Step 4 we note that the rank 1 matrices $b_1b_1^t, \ldots, b_mb_m^t$ are linearly independent [118, §4.4.4]. Indeed, the two 9-dimensional secondary cones $\sigma_{G,B}$ at the top of Table 5.1 are simplicial, and so are their faces. Hence the multipliers $\ell_1, \ldots, \ell_m$ found in Step 4 are unique and positive. These ℓ_i must agree with the desired edge lengths $l(e_i)$, by the formula for $Q = Q_\Gamma$ in (5.2.5).

Example 5.3.6. *Consider the Schottky Recovery Problem for the matrix*

$$Q \;=\; \begin{pmatrix} 17 & 5 & 3 & 5 \\ 5 & 19 & 7 & 11 \\ 3 & 7 & 23 & 16 \\ 5 & 11 & 16 & 29 \end{pmatrix}. \tag{5.3.2}$$

Using `polyhedral`, *we find that the f-vector of its Voronoi polytope is* $(96, 198, 130, 28)$. *This matches the first row in Table 5.1. Hence* $Q \in \mathcal{J}_4^{trop}$, *and* G *is the triangular prism. Using* `polyhedral` *and* `isom`, *we find a matrix that maps* Q *into our preprocessed secondary cone:*

$$X = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ -1 & -1 & 0 & 0 \end{pmatrix} \in GL_4(\mathbb{Z}) \qquad \textit{gives} \qquad Q' = X^tQX = \begin{pmatrix} 26 & 9 & -9 & 0 \\ 9 & 20 & 7 & -2 \\ -9 & 7 & 23 & 3 \\ 0 & -2 & 3 & 17 \end{pmatrix} \in \sigma_{G,B}.$$

This Q' *is the Riemann matrix of the metric graph in Figure 5.6, with basis cycles* $e_2+e_6-e_3$, $-e_1-e_4+e_7+e_2$, $-e_1-e_5+e_8+e_3$, *and* $e_4+e_9-e_5$. *These are the rows of the* 4×9*-matrix* B. *In Step 4 of Algorithm 5.3.5 we compute* $D = diag(\ell_1, \ldots, \ell_9) = diag(7, 9, 9, 2, 3, 8, 2, 4, 12)$. *In Step 5 we output the metric graph in Figure 5.6. Its Riemann matrix equals* $Q = BDB^t$.

Example 3.2.3 explored the classical Schottky locus in a two-parameter family of Riemann matrices. In the tropical setting, it is natural to intersect $\mathbb{H}_g^{trop}$ with an affine-linear space L

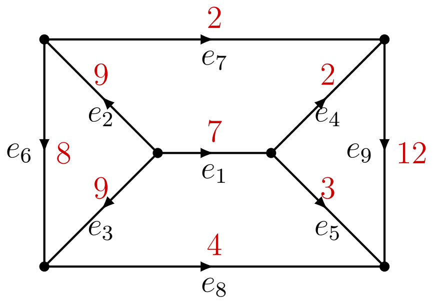


Figure 5.6: Metric graph with edge lengths in red. Its Riemann matrix matches (5.3.2).

of symmetric matrices. The intersection $\mathbb{H}_g^{trop} \cap L$ is a *spectrahedron*. By the *Schottky locus of a spectrahedron* we mean $\mathcal{J}_g^{trop} \cap L$. This is an infinite periodic polyhedral complex inside the spectrahedron. For quartic spectrahedra [95], when $g = 4$, this locus has codimension one.

Example 5.3.7 (The Schottky locus of a quartic spectrahedron)**.** *We consider the matrix*

$$Q = \begin{bmatrix} 1589 - 2922s + 960t & 789 - 1322s & -820 + 660s - 1350t & -820 + 3260s + 2550t \\ 789 - 1322s & 1589 - 2922s - 960t & -820 + 3260s - 2550t & -820 + 660s + 1350t \\ -820 + 660s - 1350t & -820 + 3260s - 2550t & 1665 + 450s + 3120t & -25 - 2930s \\ -820 + 3260s + 2550t & -820 + 660s + 1350t & -25 - 2930s & 1665 + 450s - 3120t \end{bmatrix}.$$

Here s and t are parameters. This defines a plane L in the space of symmetric 4×4-matrices. The left diagram in Figure 5.7 shows the hyperbolic curve $\{det(Q) = 0\}$. The spectrahedron $\mathbb{H}_g^{trop} \cap L$ is bounded by its inner oval. The right diagram shows the second Voronoi decomposition. The Schottky locus $\mathcal{J}_g^{trop} \cap L$ is a proper subgraph of its edge graph. It is shown in red. Note that the graph has infinitely many edges and regions.

Remark 5.3.8. *We described some computations in* `GAP` *and in* `polymake` *that realize Algorithms 5.3.3 and 5.3.5. The code for these implementations is made available on our website (5.1.1).*

5.4 Tropical meets classical

In this section we present a second solution to the tropical Schottky problem. It is new and different from the one in Section 5.2, as it works for every genus, and it links directly to the classical solution in Section 3.2.

Let $Q \in \mathbb{H}_g^{trop}$ be a positive definite matrix for arbitrary g. Mikhalkin and Zharkov [91, §5.2] define the following analogue to the Riemann theta function in the max-plus algebra:

$$\Theta(Q, x) \ := \ \max_{\lambda \in \mathbb{Z}^g} \{\lambda^t Q x - \frac{1}{2}\lambda^t Q \lambda\}. \tag{5.4.1}$$

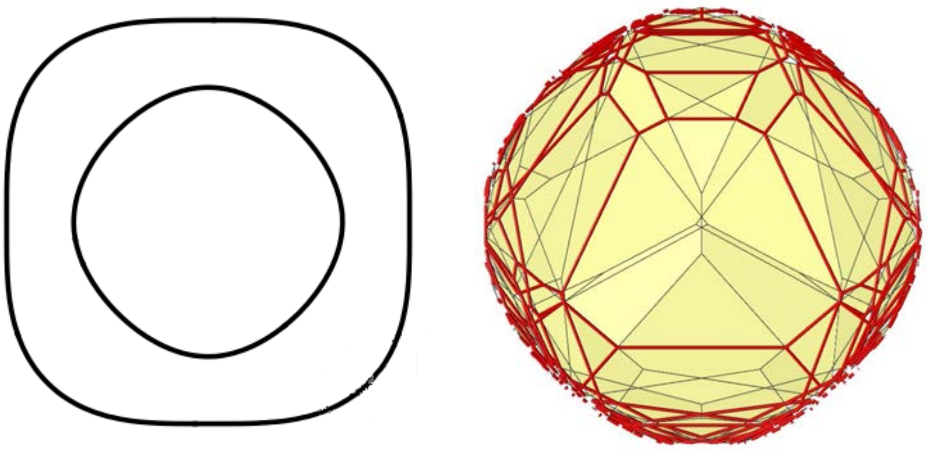


Figure 5.7: A quartic spectrahedron (left) and its second Voronoi decomposition (right). The Schottky locus of that spectrahedron consists of those edges that are highlighted in red.

This *tropical theta function* describes the asymptotic behavior of the classical Riemann theta function with Riemann matrix $t\cdot\tau$ when t goes to infinity, as long as there are no cancellations. This is made precise in Proposition 5.4.6. Here, the real matrix Q is the imaginary part of τ.

Analogously, for $u \in \mathbb{Z}^g$, we define the *tropical theta constant with characteristic* u to be

$$\Theta_u(Q) \;:=\; 2\cdot\Theta(Q,\frac{u}{2}) - \frac{1}{4}u^tQu. \tag{5.4.2}$$

In the classical case, characteristics are vectors $m = (m', m'')$ in $\mathbb{Z}^{2g}$. But, only $u = m'$ contributes to the aforementioned asymptotics. Note that $\Theta_u(Q)$ depends only on u modulo 2.

Definition 5.4.1. *For any $v \in \mathbb{Z}^g$ consider the following signed sum of tropical theta constants:*

$$\vartheta_v(Q) \;:=\; \sum_{u\in(\mathbb{Z}/2\mathbb{Z})^g} (-1)^{u^tv}\cdot\Theta_u(Q). \tag{5.4.3}$$

The theta matroid $M(Q)$ is the binary matroid represented by the collection of vectors

$$\big\{v \in (\mathbb{Z}/2\mathbb{Z})^g : \vartheta_v(Q) \neq 0\big\}. \tag{5.4.4}$$

The tropical theta constants and the theta matroid are invariant under basis changes $S \in \mathrm{GL}_g(\mathbb{Z})$. We have $\vartheta_u(Q) = \vartheta_{S^{-1}u}(S^tQS)$ for all $u \in \mathbb{Z}^g$, and therefore $M(Q) = M(S^tQS)$.

Here is the promised new approach to the Schottky problem. If Q lies in the tropical Schottky locus then $M(Q)$ is the desired cographic matroid and (5.4.3) furnishes edge lengths.

Theorem 5.4.2. *If $Q \in \mathcal{J}_g^{trop}$ then the matroid $M(Q)$ is cographic. In that graph, we assign the length $2^{3-g}\cdot\vartheta_v(Q)$ to the edge labeled v. The resulting metric graph has Riemann matrix Q.*

This says, in particular, that $\vartheta_v(Q)$ is non-negative when Q comes from a metric graph.

Proof. Since $Q \in \mathcal{J}_g^{trop}$, there exists a unimodular matrix $B = (b_1, \ldots, b_m) \in \{-1, 0, +1\}^{g\times m}$ and a diagonal matrix $D = diag(\ell_1, \ldots, \ell_m)$ such that $Q = BDB^t = \sum_{i=1}^m \ell_i b_i b_i^t$. We claim

$$\Theta_u(Q) \;=\; -\frac{1}{4} \cdot \sum_{b_i^t u \text{ is odd}} \ell_i \qquad \text{for all } \; u \in \mathbb{Z}^g. \tag{5.4.5}$$

Here the ℓ_i are positive real numbers. First, we note that

$$\Theta_u(Q) \;=\; \max_{\lambda\in\mathbb{Z}^g} \bigl\{ -(\lambda + \frac{u}{2})^t Q (\lambda + \frac{u}{2}) \bigr\} \;\;\leq\;\; \sum_{i=1}^m -\ell_i \cdot \min_{\lambda\in\mathbb{Z}^g} \Bigl\{ \bigl(b_i^t \cdot (\lambda + \frac{u}{2}) \bigr)^2 \Bigr\}.$$

If $b_i^t u$ is even, then $b_i^t \cdot (\lambda + \frac{u}{2}) = 0$ for some $\lambda \in \mathbb{Z}^g$. Otherwise, the absolute value of $b_i^t \cdot (\lambda + \frac{u}{2})$ is at least $1/2$. This shows that $\Theta_u(Q) \leq -\frac{1}{4} \cdot \sum_{b_i^t u \text{ is odd}} \ell_i$. To derive the reverse inequality, let $I = \bigl\{ i \,:\, u_i \text{ is odd} \bigr\} \subset \{1, \ldots, g\}$. By a result of Ghouila-Houri [68] on unimodular matrices, we can find $w \in \mathbb{Z}^g$ with $w_i = \pm 1$ if $i \in I$ and $w_i = 0$ otherwise, such that $b_i^t \cdot w \in \{0, \pm 1\}$ for all $1 \leq i \leq m$. The vector $\lambda_0 = \frac{1}{2}(w - u)$ lies in $\mathbb{Z}^g$. One checks that

$$-(\lambda_0 + \frac{u}{2})^t Q (\lambda_0 + \frac{u}{2}) \;=\; \sum_{i=1}^m -\ell_i \cdot (b_i^t \cdot (\lambda_0 + \frac{u}{2}))^2 \;=\; -\frac{1}{4} \sum_{i=1}^m \ell_i \cdot (b_i^t \cdot w)^2 \;=\; -\frac{1}{4} \cdot \sum_{b_i^t u \text{ is odd}} \ell_i.$$

Therefore, we also have $\Theta_u(Q) \geq -\frac{1}{4} \cdot \sum_{b_i^t u \text{ is odd}} \ell_i$. This establishes the assertion in (5.4.5).

We next claim that, under the same hypotheses as above, the function in (5.4.3) satisfies

$$\vartheta_v(Q) \;=\; 2^{g-3} \sum_{b_i \equiv v \bmod 2} \ell_i \qquad \text{for all } v \in \mathbb{Z}^g. \tag{5.4.6}$$

Indeed, substituting the right hand side of (5.4.5) for $\Theta_u(Q)$ into (5.4.3), we find that

$$\vartheta_v(Q) \;=\; -\frac{1}{4} \cdot \sum_{u \in (\mathbb{Z}/2\mathbb{Z})^g} \sum_{b_i^t u \text{ is odd}} (-1)^{u^t v} \cdot \ell_i \;=\; -\frac{1}{4} \cdot \sum_{i=1}^m \ell_i \cdot (|E_i| - |O_i|),$$

where $E_i = \{u \in (\mathbb{Z}/2\mathbb{Z})^g : b_i^t u \textit{ odd}, \, u^t v \textit{ even}\}$ and $O_i = \{u \in (\mathbb{Z}/2\mathbb{Z})^g : b_i^t u \textit{ odd}, \, u^t v \textit{ odd}\}$. If $b_i \equiv v \bmod 2$ then $E_i = \emptyset$ and $|O_i| = 2^{g-1}$. Otherwise, $|E_i| = |O_i| = 2^{g-2}$. This proves (5.4.6).

Since $Q \in \mathcal{J}_g^{trop}$, this matrix comes from a graph G. We may assume that G has no 2-valent vertices. This ensures that any pair is independent in the cographic matroid of G.

The column b_i of the matrix B records the coefficients of the i-th edge in a cycle basis of the graph G. The residue class of b_i modulo 2 is unique. For $v \in \mathbb{Z}^g$ with $b_i \equiv v \bmod 2$, the sum in (5.4.6) has only term ℓ_i, and we have $\ell_i = 2^{3-g} \vartheta_v(Q)$. If $v \in \mathbb{Z}^g$ is not congruent to b_i for any i then $\vartheta_v(Q) = 0$. This proves that the theta matroid $M(Q)$ equals the cographic matroid of G, and the edge lengths ℓ_i are recovered from Q by the rule in Theorem 5.4.2. □

By Theorem 5.4.2, the non-negativity of $\vartheta_v(Q)$ is a necessary condition for Q to be in $\mathcal{J}_g^{trop}$.

Example 5.4.3. *For the matrix Q in Example 5.3.4, we find $\vartheta_{0001}(Q) = -\frac{1}{2}$. Hence $Q \notin \mathcal{J}_4^{trop}$.*

This necessary (but not sufficient) condition translates into the following algorithm:

Algorithm 5.4.4 (Tropical Schottky Recovery)**.** *Input: $Q \in \mathcal{J}_g^{trop}$.*
Output: A metric graph Γ whose Riemann matrix Q_Γ equals Q.
1. Compute the theta matroid $M(Q)$. It is cographic and determines a unique graph G.
2. Compute all edge lengths using the formula $\ell_i = 2^{3-g}\vartheta_v(Q)$. Set $D = diag(\ell_1, \ldots, \ell_m)$.
3. Output the metric graph (G, D).
4. (Optional) As in Algorithm 5.3.5, find a basis B such that $BDB^t = Q$.

Example 5.4.5. *Let Q be the matrix in Example 5.3.6. For each $u \in (\mathbb{Z}/2\mathbb{Z})^4$, we list the theta constant $\Theta_u(Q)$, the weight $2^{-1}\vartheta_u(Q)$ and the label of the corresponding edge in Figure 5.3.6:*

u	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
$-\Theta_u$	$\frac{29}{4}$	$\frac{23}{4}$	5	$\frac{19}{4}$	$\frac{13}{2}$	7	$\frac{31}{4}$	$\frac{17}{4}$	9	$\frac{17}{2}$	$\frac{33}{4}$	$\frac{13}{2}$	$\frac{43}{4}$	$\frac{41}{4}$	$\frac{21}{2}$
$2^{-1}\vartheta_u$	9	7	9	8	2	0	4	12	0	0	0	0	2	0	3
Edge	e_2	e_1	e_3	e_6	e_7	$-$	e_8	e_9	$-$	$-$	$-$	$-$	e_4	$-$	e_5

We now explain the connection between the classical and tropical theta functions. In particular, we will show how the process of tropicalization relates Theorems 3.2.1 and 5.4.2.

In order to tropicalize the Schottky–Igusa modular form, we must study the order of growth of the theta constants when the entries of the Riemann matrix grow. This information is captured by the tropical theta constants. The following proposition makes that precise.

Proposition 5.4.6. *Fix $Q \in \mathbb{H}_g^{trop}$, and let $P(t)$ be any real symmetric $g \times g$-matrix that depends on a parameter $t \in \mathbb{R}$. For every $m \in (\mathbb{Z}/2\mathbb{Z})^{2g}$ there is a constant $C \in \mathbb{R}$ such that*

$$0 \;\le\; \frac{|\,\theta[m](P(t) + t \cdot \mathrm{i}Q, 0)\,|}{|\,\exp(t \cdot \pi \cdot \Theta_{m'}(Q))\,|} \le\; C \quad \textit{for all } t \geq 0. \tag{5.4.7}$$

Moreover, we can choose $P(t)$ such that the ratio above does not approach zero for $t \to \infty$.

Here $\theta[m](\tau, 0)$ is the classical theta constant from (2.1.3), and $\Theta_{m'}(Q)$ is the tropical theta constant defined in (5.4.2). We use the notation $m = (m', m'')$ for vectors in $\mathbb{Z}^{2g}$, where $m', m'' \in \mathbb{Z}^{2g}$.

Proof. Consider the lattice points λ where the maximum in (5.4.1) for $x = m'/2$ is attained. The corresponding summands in (2.1.2) with $\lambda = n$ have the same asymptotic behavior as $\exp(t \cdot \pi\Theta_{m'}(Q))$ for $t \to \infty$. The sum over the remaining exponentials tends to zero since it can be bounded by a sum of finitely many Gaussian integrals with variance going to zero for $t \to \infty$. We can choose the real symmetric matrix $P(t)$ in such a way that no cancellation of highest order terms happens. Then the expression in (5.4.7) is bounded away from zero. $\square$

Remark 5.4.7. *On the Siegel upper-half space $\mathbb{H}_g$ we have an action by the symplectic group $\mathrm{Sp}_{2g}(\mathbb{Z})$. Two matrices from the same orbit under this action correspond to the same abelian variety. However their tropicalizations may vary drastically. Consider for example the case $g = 1$: $\begin{pmatrix} 0 & -1 \\ 1 & k \end{pmatrix} \in \mathrm{Sp}_2(\mathbb{Z})$ sends $\tau = \mathrm{i}$ to a complex number with imaginary part $\frac{1}{1+k^2}$.*

We now assume that $g = 4$. For any subset $M \subset (\mathbb{Z}/2\mathbb{Z})^8$ we write $M' = \{m' : m \in M\}$ and similarly for M''. The following lemma concerns the possible choices for Theorem 3.2.1.

Lemma 5.4.8. *For any azygetic triple $\{m_1, m_2, m_3\}$ and any matching subgroup $N \subset (\mathbb{Z}/2\mathbb{Z})^8$,*

(1) there exist indices $1 \leq i < j \leq 3$ such that $(m_i + N)' = (m_j + N)'$, and

(2) if $\dim N' = 3$ and $(m_1 + N)' = (m_2 + N)' \neq (m_3 + N)'$, then $m_1', m_2' \in N'$.

Proof. This purely combinatorial statement can be proved by exhaustive computation. $\square$

For instance, consider the specific choice of m_1, m_2, m_3, N made prior to Example 3.2.2. This has $\dim N' = 2$, and Lemma 5.4.8 (1) holds with $i = 2$, $j = 3$. If we exchange the first four coordinates with the last four coordinates, then $\dim N' = 3$, $m_1', m_3' \in N'$ and $m_2' \notin N'$.

Recall from Theorem 3.2.1 that a matrix $\tau \in \mathbb{H}_4$ is in the Schottky locus if and only if $\pi_1^2 + \pi_2^2 + \pi_3^2 - 2(\pi_1\pi_2 + \pi_1\pi_3 + \pi_2\pi_3)$ vanishes. The tropicalization of this expression equals

$$\max_{i,j=1,2,3} (\pi_i^{\mathrm{trop}} + \pi_j^{\mathrm{trop}}), \tag{5.4.8}$$

where $\pi_i^{\mathrm{trop}} = \sum_{m \in m_i + N} \Theta_{m'}(Q)$ is the tropicalization of the product (3.2.2), with $Q = \mathrm{i}m(\tau)$.

The *tropical Schottky–Igusa modular form* (5.4.8) defines a piecewise-linear convex function $\mathbb{H}_4^{trop} \to \mathbb{R}$. Its breakpoint locus is the set of Riemann matrices Q for which the maximum in (5.4.8) is attained twice. That set depends on our choice of m_1, m_2, m_3, N. That choice is called *admissible* if $N \subset (\mathbb{Z}/2\mathbb{Z})^8$ has rank three, the triple $\{m_1, m_2, m_3\} \subset (\mathbb{Z}/2\mathbb{Z})^8$ is azygetic, all elements of $m_i + N$ are even, and the group $N' \subset (\mathbb{Z}/2\mathbb{Z})^4$ also has rank three. We define the *tropical Igusa locus* in $\mathbb{H}_g^{trop}$ to be the intersection, over all admissible choices m_1, m_2, m_3, N, of the breakpoint loci of the tropical modular forms (5.4.8).

Theorem 5.4.9. *A matrix $Q \in \mathbb{H}_4^{trop}$ lies in the tropical Igusa locus if and only if $\vartheta_v(Q) \geq 0$ for all $v \in \mathbb{Z}^4$. That locus contains the tropical Schottky locus $\mathcal{J}_4^{trop}$, but they are not equal.*

Proof. We are interested in how the maximum in (5.4.8) is attained. By Lemma 5.4.8 (1), after relabeling, $\pi_1^{\mathrm{trop}} = \pi_2^{\mathrm{trop}}$. The maximum is attained twice if and only if $\pi_1^{\mathrm{trop}} \geq \pi_3^{\mathrm{trop}}$.

The condition in Lemma 5.4.8 (2) then holds, and substituting the definition of π_i^{trop}, this is equivalent to

$$\sum_{u \in N'} \Theta_u(Q) \;\geq\; \sum_{u \notin N'} \Theta_u(Q). \tag{5.4.9}$$

Let v be the non-zero vector in $(\mathbb{Z}/2\mathbb{Z})^4$ that is orthogonal to N'. Then (5.4.9) is equivalent to

$$\vartheta_v(Q) \;=\; \sum_{u \in (\mathbb{Z}/2\mathbb{Z})^4} (-1)^{u^t v} \Theta_u(Q) \;\geq\; 0.$$

This proves the first assertion, if we knew that every v arises from some admissible choice.

We saw in Theorem 5.4.2 that $\vartheta_v(Q) \geq 0$ for all v whenever $Q \in \mathcal{J}_4^{trop}$. Hence the tropical Schottky locus $\mathcal{J}_4^{trop}$ is contained in the tropical Igusa locus. The two loci are not equal because the latter contains the *zonotopal locus* of $\mathbb{H}_4^{trop}$. This consists of matrices $Q = BDB^t$ where B represents any unimodular matroid, not necessarily cographic. By [118, §4.4.4], the second Voronoi decomposition of $\mathbb{H}_4^{trop}$ has a non-cographic 9-dimensional cone in its zonotopal locus. It is unique modulo $\mathrm{G}L_4(\mathbb{Z})$. We verified that all 16 tropical modular forms ϑ_v are non-negative on that cone. This establishes the last assertion in Theorem 5.4.9.

To finish the proof, we still need that every $v \in (\mathbb{Z}/2\mathbb{Z})^4 \backslash \{0\}$ is orthogonal to N' for some admissible choice m_1, m_2, m_3, N. By permuting coordinates, it suffices to show this for

$$v \;\in\; \{(1,0,0,0)^t, (1,1,0,0)^t, (1,1,1,0)^t, (1,1,1,1)^t\}.$$

For $v = (1,0,0,0)^t$ we take

$$m_1 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \\ 0 & 0 \\ 0 & 1 \end{pmatrix},\; m_2 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{pmatrix},\; m_3 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \\ 1 & 0 \\ 1 & 0 \end{pmatrix},\; n_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{pmatrix},\; n_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \\ 1 & 0 \\ 1 & 1 \end{pmatrix},\; n_3 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

For $v = (1,1,0,0)^t$ we take

$$m_1 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \\ 0 & 0 \\ 0 & 1 \end{pmatrix},\; m_2 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 1 & 1 \\ 0 & 0 \end{pmatrix},\; m_3 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 1 \end{pmatrix},\; n_1 = \begin{pmatrix} 1 & 1 \\ 1 & 1 \\ 0 & 1 \\ 1 & 0 \end{pmatrix},\; n_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 0 \end{pmatrix},\; n_3 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 0 & 0 \\ 1 & 1 \end{pmatrix}.$$

For $v = (1,1,1,0)^t$ we take

$$m_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 0 \\ 1 & 0 \end{pmatrix},\; m_2 = \begin{pmatrix} 0 & 1 \\ 0 & 1 \\ 0 & 1 \\ 1 & 0 \end{pmatrix},\; m_3 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 1 & 0 \end{pmatrix},\; n_1 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 1 & 1 \end{pmatrix},\; n_2 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 1 & 0 \\ 1 & 1 \end{pmatrix},\; n_3 = \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

For $v = (1,1,1,1)^t$ we take

$$m_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ 0 & 0 \end{pmatrix},\; m_2 = \begin{pmatrix} 0 & 1 \\ 0 & 1 \\ 1 & 0 \\ 1 & 0 \end{pmatrix},\; m_3 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \\ 0 & 1 \\ 0 & 1 \end{pmatrix},\; n_1 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 0 \\ 0 & 1 \end{pmatrix},\; n_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ 1 & 0 \end{pmatrix},\; n_3 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \\ 1 & 1 \\ 0 & 0 \end{pmatrix}.$$

This completes the proof of Theorem 5.4.9. □

We have shown that the tropicalization of the classical Schottky locus satisfies the constraints coming from the tropical Schottky–Igusa modular forms in (5.4.8). However, these constraints are not yet tight. The tropical Igusa locus, as we have defined it, is strictly larger than the tropical Schottky locus. It would be desirable to close this gap, at least for $g = 4$. One approach might be a more inclusive definition of which choices are "admissible".

Question 5.4.10. *Can the tropical Schottky locus $\mathcal{J}_4^{trop}$ be cut out by additional tropical modular forms, notably those obtained in (5.4.8) by allowing choices m_1, m_2, m_3, N with $\dim N' \leq 2$?*

The next question concerns arbitrary genus g. We ask whether just computing the theta matroid $M(Q)$ solves the Tropical Schottky Decision problem. Note that we did not address this subtle issue in Algorithm 5.4.4 because we had assumed that the input Q lies in $\mathcal{J}_g^{trop}$.

Question 5.4.11. *Let Q be a positive definite $g \times g$ matrix such that the matroid $M(Q)$ is cographic with positive weights. Does this imply that Q is in the tropical Schottky locus?*

If the answer is affirmative then we can use Tutte's classical algorithm [117] as a subroutine for Schottky Decision. That algorithm can decide whether the matroid $M(Q)$ is cographic. We close with a question that pertains to classical Schottky Reconstruction as in Section 3.2.

Question 5.4.12. *How to generalize the results in [48] from $g = 3$ to $g = 4$? Is there a nice* tritangent matrix*, written explicitly in theta constants, for canonical curves of genus four?*

5.5 Conclusion

In this chapter, we discussed the tropical Schottky problem, and presented algorithms for solving it in genus four. We also relate the classical and tropical solutions to the genus four Schottky problem. This chapter concludes the first part of this thesis. In the next part, we discuss two works relating to cryptography.

Part II

Elliptic curve and lattice-based cryptography

Chapter 6

On cycles of pairing-friendly elliptic curves

This part of the thesis relates to cryptography. In this chapter, we study cycles of pairing-friendly elliptic curves, for an application in pairing-based cryptography. The material in this chapter is from the paper "On Cycles of Pairing-Friendly Elliptic Curves" authored with Alessandro Chiesa and Matthew Weidner, and published in the SIAM Journal on Applied Algebra and Geometry [41].

6.1 Introduction

A cycle of elliptic curves is a list of elliptic curves defined over finite fields in which the number of points on one curve equals the size of the field of definition of the next, cyclically.

Definition 6.1.1. *An* m-cycle of elliptic curves *is a list of* m *distinct elliptic curves* $E_1/\mathbb{F}_{q_1},\ldots,$ $E_m/\mathbb{F}_{q_m}$*, where* $q_1,\ldots,q_m$ *are prime, such that the numbers of points on these curves satisfy*

$$\#E_1(\mathbb{F}_{q_1}) = q_2\,, \ldots, \#E_i(\mathbb{F}_{q_i}) = q_{i+1}\,, \ldots, \#E_m(\mathbb{F}_{q_m}) = q_1\,. \tag{6.1.1}$$

This notion was introduced in [111] with the name of *aliquot cycles*. The case of 2-cycles of ordinary curves, also called *amicable pairs*, was introduced in the context of primality proving by [89, 90] under the equivalent notion of *dual elliptic primes*.

Silverman and Stange [111] showed that cycles of arbitrary lengths exist, and gave conjectural estimates, for any elliptic curve $E/\mathbb{Q}$, of the number of prime pairs (q_1, q_2) such that reducing E modulo q_1 and q_2 gives an amicable pair. Cycles of elliptic curves were further studied in [15, 76, 96, 97], and some of these works refined and proved on average the conjectured estimates, showing that amicable pairs are asymptotically common.

In [21] the notion of cycles of elliptic curves was extended for applications to pairing-based cryptography.

Definition 6.1.2. *A* pairing-friendly m-cycle of elliptic curves *is an m-cycle such that every elliptic curve in the cycle is ordinary and has a small embedding degree.*

Pairing-friendly cycles were used in [21] to achieve recursive composition of *zkSNARKs* (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge). A zkSNARK is a cryptographic scheme that allows one party (the prover) to convince another party (the verifier) that the prover knows a certain secret, via a short proof that is cheap to verify and reveals no information about the secret. Efficient zkSNARK constructions are obtained via pairing-friendly elliptic curves, and the cycle condition in Eq. (6.1.1) enables their recursive composition, while avoiding expensive modular arithmetic across fields of different characteristics. (See [21] for details.)

Practitioners are interested in recursive composition of zkSNARKs, because it can be used to boost the scalability of distributed ledger technologies [33]. For example, there are commercial efforts in this space whose core technology *is* recursive composition [45], and such technology thus rests on properties of cycles of pairing-friendly elliptic curves.

This motivates the question: *what types of pairing-friendly cycles exist?* A pairing-friendly 2-cycle can be obtained from pairing-friendly prime-order curves of embedding degrees 4 and 6 [79, 21]. Beyond this, there are *no* other known constructions, and very little is known about pairing-friendly cycles. Indeed, requiring a small embedding degree as in Definition 6.1.2 is a strong restriction and techniques used in previous work to study aliquot cycles do not seem to apply to pairing-friendly cycles.

This is unfortunate because the aforementioned MNT cycle is not ideal for applications: its unequal embedding degrees make one curve less secure than the other and, moreover, the fact that both embedding degrees are so small implies that using the cycle at high security levels is inefficient. It would be desirable, e.g., to have a 2-cycle with embedding degrees $(12, 12)$ or $(20, 20)$ and, more generally, to understand this mathematical object better.

Overview of results

The stark difference in the current understanding of pairing-friendly cycles when compared to aliquot cycles, as well as applications to pairing-friendly cryptography in the real world, motivates a systematic study of pairing-friendly cycles. In this paper we initiate such a study, and our main results are the following.

1. Prior to this work, the *only* construction of pairing-friendly cycles was a 2-cycle from a family of curves called *MNT curves*, named after Miyaji, Nakabayashi, and Takano [92]. A natural question to ask is: can one construct other cycles consisting of MNT curves? In this work, we construct a new pairing-friendly cycle of length 4 using MNT curves. We also characterize *all* the possibilities for cycles consisting of MNT curves, showing that any MNT cycle must have length 2 or 4, and that the curves must have embedding degrees alternating between 4 and 6. See Section 6.4 for details.

2. We then study *arbitrary* pairing-friendly 2-cycles (not derived from a particular family). We prove that 2-cycles of elliptic curves with embedding degrees $(5, 10)$, $(8, 8)$, or $(12, 12)$ do *not* exist. The technique that we use relies on the fact that the cyclotomic polynomials of these embedding degrees have degree 4. In particular, we do not know how to extend this result to any other embedding degrees (k_1, k_2). See Section 6.5 for details.

3. We move to study pairing-friendly cycles of arbitrary length. One strategy to construct cycles could be to pick a parametrized family of elliptic curves and try to construct cycles consisting of curves from the same family (like for MNT curves). What must the parameters of the family satisfy for such constructions to be possible? We prove that if the curves have the same discriminant for complex multiplication $D > 3$, then we cannot construct cycles of length greater than 2 (Section 6.6). This implies that to construct elliptic curve cycles, we must use curves from families of varying discriminants.

4. So far we discussed cycles consisting of elliptic curves of *prime* order. What if we relax the definition of cycles to allow *composite* (non-prime) order elliptic curves in which the number of points on one curve is a multiple of (but not necessarily equal to) the size of the field of definition of the next? We prove that composite-order cycles *cannot exist* (see Section 6.7). This is a strong restriction as it implies that we must construct cycles using pairing-friendly elliptic curves of *prime* order. Unfortunately, there are very few constructions of families of such curves in the literature, *regardless of cycles*.

5. Lastly, we study the other known families of pairing-friendly elliptic curves of prime order (apart from MNT curves): the Freeman curves [61] and the Barreto–Naehrig curves [19]. We prove that cycles within each of these families do not exist (Section 6.8). This means that, if one wants to obtain cycles from curve families, one must consider combinations of current families (or study future constructions of prime-order elliptic curves).

Overall, cycles of pairing-friendly elliptic curves seem much harder to understand, and to construct, than cycles of arbitrary elliptic curves. While our results have for the most part established limitations of pairing-friendly cycles, our outlook is optimistic. Our work demonstrates that studying pairing-friendly cycles is tractable and, moreover, points the way to concrete research questions that could lead to more tools for studying these cycles. We thus conclude the introduction with a selection of open problems.

Open problems

1. Do there exist cycles consisting of elliptic curves with the *same* embedding degree? The varying embedding degrees in current constructions of cycles is inconvenient because, in practice, curves in the cycle have different security levels.

2. Can we construct cycles of embedding degrees greater than 6? All known pairing-friendly cycles involve embedding degrees at most 6, which means that it is inefficient to use such cycles at high security levels (e.g., 128 bits of security). It would be desirable to construct, or rule out, cycles of higher embedding degrees (say, 20).

3. In particular, can we construct 2-cycles of higher embedding degrees? Our technique for ruling out pairs with embedding degrees $(5, 10)$, $(8, 8)$, or $(12, 12)$ sheds some light on other pairs (k_1, k_2) for which $\Phi_{k_1}(x) = \Phi_{k_2}(-x)$, but it does not seem to extend to the case $\deg \Phi_{k_1}(x) > 4$. We believe that it would be especially interesting to study pairs with embedding degrees $(16, 16)$, which have cyclotomic polynomial $x^8 + 1$.

4. Do there exist cycles consisting of elliptic curves with the same discriminant and the same embedding degrees? Our work demonstrates that sharing the same discriminant is already quite limiting, and it would be interesting to understand how this requirement interacts with that of sharing the same embedding degree.

5. Are there cycles from combinations of MNT, Freeman, and Barreto–Naehrig curves? Our preliminary investigations via Gröbner bases suggest small cycles are unlikely, but the question remains open for arbitrary-length cycles.

6.2 Preliminaries

Elliptic curves and pairings

Let E be an elliptic curve over a finite field $\mathbb{F}_q$, where q is a prime. We denote this by $E/\mathbb{F}_q$, and we denote by $E(\mathbb{F}_q)$ the group of points of E over $\mathbb{F}_q$, with order $n = \#E(\mathbb{F}_q)$. The *trace* of $E/\mathbb{F}_q$ is $t = q + 1 - n$. By Hasse's theorem [110, Theorem V.1.1], t satisfies $|t| \leq 2\sqrt{q}$. We say that E is *supersingular* if $\gcd(q, t) \neq 1$, otherwise E is *ordinary*.

The *endomorphism ring* $\mathrm{End}(E)$ of E consists of morphisms from E to itself that are also group homomorphisms on its points. If E is supersingular, then $\mathrm{End}(E)$ is an order in a quaternion algebra. If E is ordinary, then $\mathrm{End}(E)$ is an order in an imaginary quadratic field $\mathbb{Q}(\sqrt{-D})$, for some positive squarefree integer D. We call D the *discriminant*, and we say that E has *complex multiplication* in $\mathbb{Q}(\sqrt{-D})$.[1]

Let $r \geq 2$ be an integer relatively prime to q. We denote the r-torsion points of E by $E[r]$, and we denote the group of r-th roots of unity in the algebraic closure of $\mathbb{F}_q$ by μ_r. The *Weil pairing* is a bilinear non-degenerate map

$$e_r \colon E[r] \times E[r] \to \mu_r \, . \tag{6.2.1}$$

The *embedding degree* with respect to r is the smallest integer k such that r divides $q^k - 1$. In the case of prime-order curves, if $r = n$ we simply say that E has embedding degree k.

[1] Some works use the convention that D is negative. Throughout this work we take D to be positive.

The Weil pairing was first used in cryptography to reduce the discrete logarithm problem on $E[r]$ to a discrete logarithm problem in μ_r, which is contained in $\mathbb{F}_{q^k}^*$ [87, 63]. Subsequently, starting with the work of [28, 77], the Weil pairing was used to achieve numerous cryptographic capabilities. For security, it is necessary to choose the embedding degree k such that the discrete logarithm problem in $\mathbb{F}_{q^k}^*$ is computationally infeasible. On the other hand, the embedding degree cannot be too large, or the computation of the Weil pairing (which grows linearly in k) would not be efficient enough for cryptographic applications.

We say that an elliptic curve $E/\mathbb{F}_q$ is *pairing-friendly* if $E(\mathbb{F}_q)$ has a large prime-order subgroup, and if the embedding degree is small (see [62] for a more precise definition). A random elliptic curve has a large embedding degree and thus is not pairing-friendly. Constructing pairing-friendly curves with specified parameters is a difficult problem with strong practical motivations that has been extensively studied. It was shown in [87] that supersingular elliptic curves can have embedding degree at most 6, and if the characteristic of q is not 2 or 3, the embedding degree is at most 3. As we are interested in large values of q and higher values of k for applications in cryptography, we focus on ordinary elliptic curves.

The known methods to construct ordinary pairing-friendly curves proceed by first finding parameters q, r, t, k such that there exists an elliptic curve $E/\mathbb{F}_q$ with trace t, a prime-order subgroup of size r, and embedding degree k. The *complex multiplication method* is then used to find the equation of the curve. This works if the *CM equation* $4q - t^2 = Dy^2$ has a solution with $y \in \mathbb{Z}$ and small positive discriminant $D \in \mathbb{Z}$. Indeed, state-of-the-art algorithms run in time $O(D \operatorname{polylog} D)$ and are only feasible for D of size up to 10^{16} [113].

It is useful to view the condition on the embedding degree via cyclotomic polynomials. Let Φ_m be the m-th cyclotomic polynomial (the minimal polynomial over the rationals of an irreducible m-th root of unity). It is known that (see for example [121])

$$x^m - 1 = \prod_{d|m} \Phi_d(x)\,. \tag{6.2.2}$$

Lemma 6.2.1. *Let $E/\mathbb{F}_q$ have prime order n. Then E has embedding degree k if and only if k is minimal such that n divides $\Phi_k(q)$.*

Proof. The condition that k is the embedding degree implies that k is minimal such that $q^k \equiv 1 \pmod{n}$. Using basic results on cyclotomic polynomials (see [121, Lemma 2.9]), this is equivalent to the condition that $n|\Phi_k(q)$. □

This can be converted into a result relating n to the trace t.

Lemma 6.2.2 ([18])**.** *The elliptic curve $E/\mathbb{F}_q$ has embedding degree k if and only if $n|\Phi_k(t-1)$ and $n \nmid \Phi_i(t-1)$ for all $0 < i < k$.*

To construct ordinary pairing-friendly elliptic curves, one need only consider embedding degrees $k \geq 3$, because of the following lemma.

Lemma 6.2.3. *Let $E/\mathbb{F}_q$ be an elliptic curve of prime order with embedding degree $k = 2$. Then E is supersingular.*

Proof. By Lemma 6.2.1, the condition that $k = 2$ implies that $q + 1 - t \,|\, q + 1$, since $\Phi_2(x) = x + 1$. Thus we can write $q + 1 - t = d(q + 1)$ for some integer $d \geq 1$. From the Hasse bound, we have $|t| = (d - 1)(q + 1) \leq 2\sqrt{q}$. Thus we have the inequality

$$(d - 1)q - 2\sqrt{q} + d - 1 \leq 0\,. \tag{6.2.3}$$

This has a solution if the discriminant $4 - 4(d - 1)^2$ is nonnegative, which simplifies to $d \leq 2$. If $d = 1$, then $t = 0$ and E is supersingular. If $d = 2$, then $t = -q - 1$. Using the Hasse bound, we have $q + 1 \leq 2\sqrt{q}$, or $(\sqrt{q} - 1)^2 \leq 0$, which has only the trivial solution $q = 1$. □

Families of pairing-friendly elliptic curves

We consider families of pairing-friendly elliptic curves with a fixed embedding degree, whose parameters are defined by polynomials. These are useful for generating curves for applications, where curves of arbitrary size are desired. Each family is parametrized by polynomials $(q_k(x), n_k(x), t_k(x))$, representing the field of definition, number of rational points, and trace respectively, where k is the embedding degree. These have to satisfy that $n_k(x) = q_k(x) + 1 - t_k(x)$, $n_k(x)$ divides $\Phi_k(t_k(x) - 1)$, and there must be infinitely many integer solutions (x, y) to the CM equation $4q_k(x) - t_k(x)^2 = Dy^2$, for some small positive discriminant $D \in \mathbb{Z}$.

Miyaji, Nakabayashi, and Takano [92] characterized all families of ordinary prime-order elliptic curves with embedding degrees $k = 3, 4, 6$. For these embedding degrees, the cyclotomic polynomial is quadratic, and the CM equation can be transformed into a generalized Pell equation. These families are parametrized by the polynomials in Table 6.1. We refer to elliptic curves belonging to the MNT families in Table 6.1 as *MNT curves*.

Table 6.1: MNT curves.

k	$q_k(x)$	$n_k(x)$	$t_k(x)$
3	$12x^2 - 1$	$12x^2 - 6x + 1$	$6x - 1$
4	$x^2 + x + 1$	$x^2 + 2x + 2,\ x^2 + 1$	$-x,\ x + 1$
6	$4x^2 + 1$	$4x^2 + 2x + 1$	$-2x + 1$

For other embedding degrees, there is no analogous characterization of all elliptic curves with a given embedding degree. Moreover, there is currently no method to construct families of prime-order elliptic curves of arbitrary embedding degrees. (If we allow for composite orders, there are algorithms to construct elliptic curves of arbitrary embedding degrees [44, 55].) There are two other constructions of prime-order families, stated below.

Freeman [61] has constructed a family of prime-order elliptic curves with $k = 10$, which is parametrized by the following polynomials:

$$q_{10}(x) = 25x^4 + 25x^3 + 25x^2 + 10x + 3\,, \tag{6.2.4a}$$

$$n_{10}(x) = 25x^4 + 25x^3 + 15x^2 + 5x + 1\,, \tag{6.2.4b}$$

$$t_{10}(x) = 10x^2 + 5x + 3\,. \tag{6.2.4c}$$

Barreto and Naehrig [19] have another construction with $k = 12$, parametrized by

$$q_{12}(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1\,, \tag{6.2.5a}$$

$$n_{12}(x) = 36x^4 + 36x^3 + 18x^2 + 6x + 1\,, \tag{6.2.5b}$$

$$t_{12}(x) = 6x^2 + 1\,. \tag{6.2.5c}$$

Other constructions of pairing-friendly elliptic curves have *composite* orders. These include the families of Brezing and Weng [34] and of Barreto, Lynn, and Scott [18].

6.3 Cycles of pairing-friendly elliptic curves

In this paper we study cycles of pairing-friendly elliptic curves. This notion was introduced in [21] for applications in cryptography. We re-state Definition 6.1.1 below.

Definition 6.3.1. *An* m-cycle of elliptic curves *is a list of* m *distinct elliptic curves* $E_1/\mathbb{F}_{q_1}$,…, $E_m/\mathbb{F}_{q_m}$*, where* $q_1, \ldots, q_m$ *are prime, such that the numbers of points on these curves satisfy*

$$\#E_1(\mathbb{F}_{q_1}) = q_2\,, \ldots, \#E_i(\mathbb{F}_{q_i}) = q_{i+1}\,, \ldots, \#E_m(\mathbb{F}_{q_m}) = q_1\,. \tag{6.3.1}$$

Cryptographic applications require curves in the cycle to have small embedding degree.

Definition 6.3.2. *A* $(k_1, \ldots, k_m)$-cycle *is an* m*-cycle of distinct ordinary elliptic curves* $E_1/\mathbb{F}_{q_1}$, …, $E_m/\mathbb{F}_{q_m}$ *such that* $E_i/\mathbb{F}_{q_i}$ *has embedding degree* k_i*, for each* $i = 1, \ldots, m$*. A* $(k_1, \ldots, k_m)$*-cycle is* pairing-friendly *if all the* k_i*'s are small (recall Definition 6.1.2).*

An m-cycle is a special case of a $(k_1, \ldots, k_m)$-cycle where the k_i's are arbitrary positive integers (or possibly infinity). If we require that $q_1, \ldots, q_m$ are *distinct* primes, Definition 6.3.1 is equivalent to the notion of *aliquot cycles* for elliptic curves $E/\mathbb{Q}$ by Silverman and Stange [111]. An aliquot m-cycle for $E/\mathbb{Q}$ is a sequence of distinct primes $(q_1, \ldots, q_m)$ such that E has good reduction at each prime and, if we denote the reduction of E at q_i by $\tilde{E}_{q_i}$, then

$$\#\tilde{E}_{q_1}(\mathbb{F}_{q_1}) = q_2\,, \ldots, \#\tilde{E}_{q_i}(\mathbb{F}_{q_i}) = q_{i+1}\,, \ldots, \#\tilde{E}_{q_m}(\mathbb{F}_{q_m}) = q_1\,. \tag{6.3.2}$$

Given an aliquot m-cycle, we can construct an m-cycle of elliptic curves by setting $E_i := \tilde{E}_{q_i}$ for each i. Conversely, given an m-cycle where $q_1, \ldots, q_m$ are distinct, we can construct a curve $E/\mathbb{Q}$ by computing its coefficients via the Chinese Remainder Theorem in such a way that E's reduction at each q_i is E_i. It is known that cycles of arbitrary lengths exist, based just on the Hasse bound and the fact that every trace in the Hasse bound is realized by an elliptic curve [53].

Proposition 6.3.3 ([111, Theorem 5.1])**.** *For every $m \geq 1$ there exists an elliptic curve $E/\mathbb{Q}$ with an aliquot m-cycle.*

However, the foregoing result does not take into account the embedding degrees of the curves. In particular, it is not known if pairing-friendly cycles of arbitrary lengths exist.

The focus of this paper is the study of *pairing-friendly* cycles of elliptic curves. This is a significantly more restrictive notion than the aliquot cycles introduced in [111], since a random elliptic curve would not have a small embedding degree. Moreover, there are only few known families of prime-order elliptic curves with small embedding degrees (see Section 6.2 for a list of all such families). Even without the condition that the curves form a cycle, it is already a difficult problem to construct pairing-friendly elliptic curves of prime order.

We list below a few observations that we will use in this paper. First, the lemma below implies that to construct cycles of elliptic curves for applications (where the size of the finite fields tend to be large), we need only consider *ordinary* elliptic curves.

Lemma 6.3.4. *Let $E_1/\mathbb{F}_{q_1}$,…, $E_m/\mathbb{F}_{q_m}$ be an m-cycle of elliptic curves, where $q_1, \dots, q_m \geq 5$ are prime. Then all the curves must be ordinary elliptic curves.*

Proof. It is known that for any elliptic curve $E/\mathbb{F}_q$ with $q \geq 5$ prime, E is supersingular if and only if $\#E(\mathbb{F}_q) = q + 1$, see for example [110, Exercise 5.10]. Suppose $E_i/\mathbb{F}_{q_i}$ is supersingular for some i, then $\#E(\mathbb{F}_{q_i}) = q_i + 1 = q_{i+1}$. But since q_i is prime, $q_i + 1$ is even, hence this cannot hold. □

Next, we present a necessary condition for m elliptic curves to form an m-cycle. This condition is *not* sufficient as every trace in the Hasse interval can be realized by an elliptic curve [53], hence this condition is not a strong restriction on the curves in the cycle.

Lemma 6.3.5. *Let $E_1/\mathbb{F}_{q_1}$,…, $E_m/\mathbb{F}_{q_m}$ be an m-cycle of elliptic curves, with traces $t_1, \dots, t_m$ respectively. Then the sum of their traces satisfies*

$$t_1 + \cdots + t_m = m\,. \tag{6.3.3}$$

Proof. Let $n_i = \#E_i(\mathbb{F}_{q_i})$, for each $i = 1, \dots, m$. Since the curves form a cycle, we have the constraints $n_1 = q_2$, …, $n_i = q_{i+1}$, …, $n_m = q_1$. If we sum up these m equations, we get $n_1 + \cdots + n_m = q_1 + \cdots + q_m$. Using the fact that $n_i = q_i + 1 - t_i$, we get $t_1 + \cdots + t_m = m$. □

6.4 MNT cycles

We consider pairing-friendly cycles consisting of MNT curves (see Table 6.1), which are the ordinary prime-order elliptic curves of embedding degrees $3, 4, 6$. For brevity, we use the term *MNT cycles* for cycles where every curve is an MNT curve. In [79, 21], MNT curves were used to give the first construction of pairing-friendly 2-cycles. In this section, we construct MNT 4-cycles, and characterize the possible MNT cycles.

Proposition 6.4.1. *All MNT cycles have lengths 2 or 4, and they are either* $(6, 4)$*-cycles or* $(6, 4, 6, 4)$*-cycles.*

The proof of this result proceeds in a few steps. First in Lemma 6.4.2 we show that no curve in an MNT cycle can have embedding degree 3. Then in Lemmas 6.4.4 and 6.4.5 we show that no two consecutive curves in an MNT cycle can both have embedding degree 4 or 6. Finally we consider MNT cycles with alternating embedding degrees 4 and 6, and we show that these can only have lengths 2 or 4.

Lemma 6.4.2. *Let* $E_1/\mathbb{F}_{q_{k_1}(x_1)}, \dots, E_m/\mathbb{F}_{q_{k_m}(x_m)}$ *be an MNT cycle, with* $x_1, \dots, x_m \in \mathbb{Z}$ *and embedding degrees* $k_1, \dots, k_m \in \{3, 4, 6\}$*. Then none of the embedding degrees can be 3.*

To show Lemma 6.4.2, we make use of the following result.

Lemma 6.4.3 ([121, Proposition 2.10])**.** *Let* q *be a prime such that* $q \nmid k$*. Then* q *divides* $\Phi_k(a)$ *for some* $a \in \mathbb{Z}$ *if and only if* $q \equiv 1 \pmod{k}$*.*

Proof of Lemma 6.4.2. By Lemma 6.2.1, the condition that $E_i/\mathbb{F}_{q_{k_i}(x_i)}$ has embedding degree k_i implies that $n_{k_i}(x_i) \mid \Phi_{k_i}(q_{k_i}(x_i))$. Since $n_{k_i}(x_i) = q_{k_{i+1}}(x_{i+1})$, Lemma 6.4.3 implies

$$q_{k_{i+1}}(x_{i+1}) \equiv 1 \pmod{k_i}\,. \tag{6.4.1}$$

Suppose that $k_j = 3$ for some j. From Table 6.1,

$$q_3(x_j) = 12x_j^2 - 1 \equiv 1 \pmod{k_{j-1}}\,. \tag{6.4.2}$$

However, this is not possible since $12x_j^2 - 1 \equiv -1 \pmod{3, 4, 6}$. □

We show that for any MNT cycle, no two consecutive curves can both have embedding degree 4 or 6.

Lemma 6.4.4. *Let* $E_1/\mathbb{F}_{q_{k_1}(x_1)}, \dots, E_m/\mathbb{F}_{q_{k_m}(x_m)}$ *be an MNT cycle, with* $x_1, \dots, x_m \in \mathbb{Z}$*. Then no two consecutive curves can both have embedding degree* 4*.*

Proof. Suppose to the contrary that $k_i = k_{i+1} = 4$ for some i. Then $n_4(x_i) = q_4(x_{i+1})$. From Table 6.1, $q_4(x_{i+1}) = x_{i+1}^2 + x_{i+1} + 1$, and there are two possibilities for $n_4(x_i)$.

Suppose $n_4(x_i) = x_i^2 + 2x_i + 2$. Then $x_i^2 + 2x_i + 2 = x_{i+1}^2 + x_{i+1} + 1$, which implies

$$(x_i + 1)^2 = x_{i+1}(x_{i+1} + 1)\,. \tag{6.4.3}$$

This is a contradiction if $x_i \neq -1$, since the product of two consecutive nonzero integers is not a square.[2] But if $x_i = -1$, then $n_4(x_i) = 1$ would not be prime.

Suppose $n_4(x_i) = x_i^2 + 1$. Then $x_i^2 + 1 = x_{i+1}^2 + x_{i+1} + 1$, which implies

$$x_i^2 = x_{i+1}(x_{i+1} + 1)\,. \tag{6.4.4}$$

This is a contradiction by the same argument as above. □

[2] Suppose that for some nonzero $x, y \in \mathbb{Z}$, $x(x+1) = y^2$. If $x > 0$, then $x^2 < y^2 < (x+1)^2$, which has no integer solutions for x, y. If $x < 0$, then $x^2 > y^2 > (x+1)^2$, which also has no integer solutions for x, y.

Lemma 6.4.5. *Let $E_1/\mathbb{F}_{q_{k_1}(x_1)}, \ldots, E_m/\mathbb{F}_{q_{k_m}(x_m)}$ be an MNT cycle with $x_1, \ldots, x_m \in \mathbb{Z}$. Then no two consecutive curves can both have embedding degree* 6.

Proof. Suppose to the contrary that $k_i = k_{i+1} = 6$ for some i. Then $n_6(x_i) = q_6(x_{i+1})$. From Table 6.1, $q_6(x_{i+1}) = 4x_{i+1}^2 + 1$, and $n_6(x_i) = 4x_i^2 + 2x_i + 1$. Thus $4x_i^2 + 2x_i + 1 = 4x_{i+1}^2 + 1$, which implies

$$2x_i(2x_i + 1) = (2x_{i+1})^2 . \tag{6.4.5}$$

This is a contradiction if $x_{i+1} \neq 0$, since the product of two consecutive nonzero integers is not a square. But if $x_{i+1} = 0$, then $q_6(x_{i+1}) = 1$ would not be prime. □

We now consider MNT cycles consisting of elliptic curves with alternating embedding degrees 4 and 6.

Lemma 6.4.6. *Let $E_i/\mathbb{F}_{q_4}(x_i)$, $E_{i+1}/\mathbb{F}_{q_6}(x_{i+1})$ be consecutive curves in an MNT cycle. Then $2|x_{i+1}| = |x_i|$ or $2|x_{i+1}| = |x_i + 1|$.*

Proof. We have the condition $n_4(x_i) = q_6(x_{i+1})$. By Table 6.1, $q_6(x_{i+1}) = 4x_{i+1}^2 + 1$, and there are two possibilities for $n_4(x_i)$. If $n_4(x_i) = x_i^2 + 2x_i + 2$, then $x_i^2 + 2x_i + 2 = 4x_{i+1}^2 + 1$, which we simplify to $(x_i + 1)^2 = (2x_{i+1})^2$. Thus $2|x_{i+1}| = |x_i + 1|$. If instead $n_4(x_i) = x_i^2 + 1$, then $x_i^2 + 1 = 4x_{i+1}^2 + 1$, which we simplify to $x_i^2 = (2x_{i+1})^2$. Thus $2|x_{i+1}| = |x_i|$. □

Lemma 6.4.7. *Let $E_i/\mathbb{F}_{q_6}(x_i)$, $E_{i+1}/\mathbb{F}_{q_4}(x_{i+1})$ be consecutive curves in an MNT cycle. Then $x_{i+1} = 2x_i$.*

Proof. We have the condition $n_6(x_i) = q_4(x_{i+1})$. By Table 6.1, this gives $4x_i^2 + 2x_i + 1 = x_{i+1}^2 + x_{i+1} + 1$, or $2x_i(2x_i + 1) = x_{i+1}(x_{i+1} + 1)$. This implies $x_{i+1} = 2x_i$. □

We now show Proposition 6.4.1 that all MNT cycles are $(6, 4)$-cycles or $(6, 4, 6, 4)$-cycles.

Proof of Proposition 6.4.1. By Lemma 6.4.2, Lemma 6.4.4 and Lemma 6.4.5, all MNT cycles consist of curves with embedding degrees alternating between 4 and 6, and have even lengths. Let $E_1/\mathbb{F}_{q_6}(x_1), E_2/\mathbb{F}_{q_4}(x_2), \ldots, E_{2m}/\mathbb{F}_{q_4}(x_{2m})$ be an MNT cycle. We first observe that Lemma 6.4.6 and Lemma 6.4.7 imply that $|x_1| = |x_3| = \cdots = |x_{2m-1}|$. Thus $q_6(x_1) = q_6(x_3) = \cdots = q_6(x_{2m-1})$. As there are only two possibilities for $n_6(x_1), n_6(x_3), \ldots, n_6(x_{2m-1})$, for the curves to be distinct we must have $m \leq 4$, and if $m = 4$ then we must have $x_3 = -x_1$. Let $x := x_1$. Then Lemma 6.4.7 implies $x_2 = 2x$. By Lemma 6.4.6, either $x_3 = x$, in which case we have a $(6, 4)$-cycle, or $x_3 = -x$. For the latter case, Lemma 6.4.7 implies that $x_4 = -2x$, which gives us a $(6, 4, 6, 4)$-cycle.

By substituting the possible parameter values for x into the polynomials in Table 6.1, we obtain the parametrizations of the possible families of MNT $(6, 4)$-cycles in Table 6.2 and $(6, 4, 6, 4)$-cycles in Table 6.3. These cycles can be constructed by substituting integer values of x and checking if all the $n(x)$'s and $q(x)$'s are prime. □

Table 6.2: MNT $(6,4)$-cycles.

	E_1	E_2
k	6	4
$q(x)$	$4x^2+1$	$4x^2+2x+1$
$n(x)$	$4x^2+2x+1$	$4x^2+1$
$t(x)$	$-2x+1$	$2x+1$

Table 6.3: MNT $(6,4,6,4)$-cycles.

	E_1	E_2	E_3	E_4
k	6	4	6	4
$q(x)$	$4x^2+1$	$4x^2+2x+1$	$4x^2+1$	$4x^2-2x+1$
$n(x)$	$4x^2+2x+1$	$4x^2+1$	$4x^2-2x+1$	$4x^2+1$
$t(x)$	$-2x+1$	$2x+1$	$2x+1$	$-2x+1$

The MNT $(6,4,6,4)$-cycles in Table 6.3 are unions of two MNT $(6,4)$-cycles. Indeed, the pairs (E_1,E_2) and (E_3,E_4) each form $(6,4)$-cycles. Furthermore, E_1,E_3 are defined over the same finite field. Interestingly, these are the only possible MNT 4-cycles, and no longer cycles consisting of distinct elliptic curves can be obtained by taking unions of MNT 2-cycles.

Example 6.4.8. *We give an example of an MNT $(6,4)$-cycle, using the parametrization in Table 6.2. If $x=1$, we check that $4x^2+1=5$ and $4x^2-2x+1=3$ are prime. We compute each of the two curves in the cycle using the CM method and Sage [103].*

$$E_1/\mathbb{F}_5 \;:\; y^2 = x^3+4x+2\,, \tag{6.4.6a}$$
$$E_2/\mathbb{F}_3 \;:\; y^2 = x^3+2x^2+1\,. \tag{6.4.6b}$$

We list all the points of these curves in Table 6.4.

Example 6.4.9. *We give an example of an MNT $(6,4,6,4)$-cycle, using the parametrization in Table 6.3. If $x=3$, we check that $4x^2+1=37$, $4x^2+2x+1=43$ and $4x^2-2x+1=31$ are all prime. We compute the curves using Sage [103].*

$$E_1/\mathbb{F}_{37} \;:\; y^2 = x^3+24x+16\,, \tag{6.4.7a}$$
$$E_2/\mathbb{F}_{43} \;:\; y^2 = x^3+36x+5\,, \tag{6.4.7b}$$
$$E_3/\mathbb{F}_{37} \;:\; y^2 = x^3+22x+27\,, \tag{6.4.7c}$$
$$E_4/\mathbb{F}_{31} \;:\; y^2 = x^3+26x+21\,. \tag{6.4.7d}$$

We list all the points of these curves in Table 6.5.

Table 6.4: Example of an MNT $(6, 4)$-cycle.

	E_1	E_2
	$y^2 = x^3 + 4x + 2$	$y^2 = x^3 + 2x^2 + 1$
(q, n, t, k, D)	$(5, 3, 3, 6, 11)$	$(3, 5, -1, 4, 11)$
points (excluding point at infinity)	(3,1) (3,4)	(0,1) (0,2) (1,1) (1,2)

Table 6.5: Example of an MNT $(6, 4, 6, 4)$-cycle.

	E_1	E_2	E_3	E_4
	$y^2 = x^3 + 24x + 16$	$y^2 = x^3 + 36x + 5$	$y^2 = x^3 + 22x + 27$	$y^2 = x^3 + 26x + 21$
(q, n, t, k, D)	$(37, 43, -5, 6, 123)$	$(43, 37, 7, 4, 123)$	$(37, 31, 7, 6, 11)$	$(31, 37, -5, 4, 11)$
points (excluding point at infinity)	(0,4) (18,29) (0,33) (23,9) (1,2) (23,28) (1,35) (26,7) (3,2) (26,30) (3,35) (27,16) (4,18) (27,21) (4,19) (28,12) (7,3) (28,25) (7,34) (31,10) (9,6) (31,27) (9,31) (32,17) (12,16) (32,20) (12,21) (33,2) (13,3) (33,35) (13,34) (34,18) (14,5) (34,19) (14,32) (35,16) (17,3) (35,21) (17,34) (36,18) (18,8) (36,19)	(3,21) (23,10) (3,22) (23,33) (4,16) (29,5) (4,27) (29,38) (5,3) (30,7) (5,40) (30,36) (7,16) (31,9) (7,27) (31,34) (8,17) (32,16) (8,26) (32,27) (12,12) (33,8) (12,31) (33,35) (13,2) (38,1) (13,41) (38,42) (18,11) (41,21) (18,32) (41,22) (19,18) (42,21) (19,25) (42,22)	(0,8) (23,34) (0,29) (25,12) (3,3) (25,25) (3,34) (27,18) (5,15) (27,19) (5,22) (28,5) (8,7) (28,32) (8,30) (30,14) (10,10) (30,23) (10,27) (31,7) (11,3) (31,30) (11,34) (35,7) (12,13) (35,30) (12,24) (36,2) (23,3) (36,35)	(2,9) (18,11) (2,22) (18,20) (3,8) (20,4) (3,23) (20,27) (5,11) (21,1) (5,20) (21,30) (7,9) (22,9) (7,22) (22,22) (8,11) (23,13) (8,20) (23,18) (10,14) (26,13) (10,17) (26,18) (13,13) (27,15) (13,18) (27,16) (15,2) (28,3) (15,29) (28,28) (16,10) (30,5) (16,21) (30,26)

6.5 Two-cycles of specific embedding degrees

In this section we prove the following result.

Proposition 6.5.1. *There are no* $(5, 10)$-, $(8, 8)$-, *or* $(12, 12)$-*cycles.*

The pairs $(5, 10), (8, 8), (12, 12)$ are precisely the pairs (k_1, k_2) whose cyclotomic polynomials satisfy $\Phi_{k_1}(x) = \Phi_{k_2}(-x)$ and $\deg \Phi_{k_1}(x) = 4$. To prove Proposition 6.5.1, we first use these conditions to reduce from the problem of classifying (k_1, k_2)-cycles to that of finding integral points on a few quartic curves, with finitely many exceptions, in Lemma 6.5.3. We then classify all integral points on these quartic curves and the finitely many exceptions using computational tools, yielding no actual (k_1, k_2)-cycles. Note that in the case of 2-cycles, when we require nontrivial embedding degrees, the two curves cannot have equal field sizes.[3]

We first prove the following more general result, which we hope will also have applications to other kinds of 2-cycles.

Lemma 6.5.2. *Let (k_1, k_2) satisfy $\Phi_{k_1}(x) = \Phi_{k_2}(-x)$. Let $E_1/\mathbb{F}_{q_1}, E_2/\mathbb{F}_{q_2}$ be a (k_1, k_2)-cycle with $q_1 > q_2$, and let $c = q_1 - q_2$. Then $q_1 q_2 \mid \Phi_{k_1}(c)$. Additionally, for some integer d whose prime divisors are all congruent to $1 \pmod{k_1}$, there is an integer y such that*

$$y^2 = c^2 d^2 + 4d\Phi_{k_1}(c)\,. \tag{6.5.1}$$

Proof. By Lemma 6.2.1, the condition that $E_1/\mathbb{F}_{q_1}$ has embedding degree k_1 implies that $q_2 \mid \Phi_{k_1}(q_1)$. Then $q_2 \mid \Phi_{k_1}(q_1 - q_2)$ as well. Similarly, $q_1 \mid \Phi_{k_2}(q_2 - q_1) = \Phi_{k_1}(q_1 - q_2)$. It follows that $q_1 q_2 \mid \Phi_{k_1}(q_1 - q_2) = \Phi_{k_1}(c)$ as q_1 and q_2 are distinct primes. Then $dq_1q_2 = \Phi_{k_1}(c)$ for some integer d. Using $q_1 = q_2 + c$, we can rewrite this as

$$dq_2^2 + cdq_2 - \Phi_{k_1}(c) = 0\,. \tag{6.5.2}$$

For this quadratic equation in q_2 to have an integral solution, the discriminant

$$c^2 d^2 + 4d\Phi_{k_1}(c) \tag{6.5.3}$$

must be a perfect square, so that there is a y satisfying Eq. (6.5.1). Also, for any prime $p \mid d$, the above relation $dq_1q_2 = \Phi_{k_1}(c)$ implies that $p \mid \Phi_{k_1}(c)$. Hence $p \equiv 1 \pmod{k_1}$ by Lemma 6.4.3. □

Lemma 6.5.3. *In the situation of Lemma 6.5.2, additionally let* $\deg \Phi_{k_1}(x) = 4$*. Equivalently, let $(k_1, k_2) \in \{(5, 10), (8, 8), (10, 5), (12, 12)\}$. Then $c \le 82$ or $1 \le d \le 16$.*

Proof. Let $c \ge 83$. Then $\Phi_{k_1}(c) > 0$, so the relation $dq_1q_2 = \Phi_{k_1}(c)$ implies $d \ge 1$. Next, because $E_2/\mathbb{F}_{q_2}$ has q_1 points, the Hasse bound implies $|q_1 - (q_2 + 1)| \le 2\sqrt{q_2}$. Substituting $c = q_1 - q_2$ and rearranging shows $q_2 \ge (c - 1)^2/4$. The same holds for q_1 since $q_1 > q_2$. Then $dq_1q_2 = \Phi_{k_1}(c)$ implies

$$d < 16\frac{\Phi_{k_1}(c)}{(c-1)^4}\,. \tag{6.5.4}$$

For each $k_1 \in \{5, 8, 10, 12\}$, we find that for $c \ge 83$, the right-hand side is at most 17. Thus either $c \le 82$ or $1 \le d \le 16$. □

[3] Even when allowed, curves $E/\mathbb{F}_q$ with $q = \sharp E(\mathbb{F}_q)$, known as *anomalous*, are undesirable because discrete logarithms can be computed in polynomial time via the SSSA attack [108, 112, 104].

For each (k_1, k_2) listed in Lemma 6.5.3, using the fact $q_1, q_2 \mid \Phi_{k_1}(c)$ from Lemma 6.5.2, one can see that the case $c \leq 82$ yields only finitely many (k_1, k_2)-cycles. Also, for each $1 \leq d \leq 16$ whose prime divisors are congruent to $1 \pmod{k_1}$, one can show that Eq. (6.5.1) defines a plane curve of genus 1 in the coordinates (c, y). Siegel's Theorem [84, Theorem 8.2.4] implies that such a curve has only finitely many integral points, hence there are only finitely many (k_1, k_2)-cycles.

We now use computational tools to show that there are in fact no (k_1, k_2)-cycles.

Proof of Proposition 6.5.1. Using the fact $q_1, q_2 \mid \Phi_{k_1}(c)$ from Lemma 6.5.2, it is easy to enumerate all (k_1, k_2)-cycles which have $c \leq 82$, for $(k_1, k_2) \in \{(5, 10), (8, 8), (10, 5), (12, 12)\}$. Doing so using Sage [103] reveals no such examples.

We now consider the case $d \leq 16$. Restricting to values of d whose prime factors are all congruent to $1 \pmod{k_1}$, we are left with the cases shown in Table 6.6.

Table 6.6: Cases $((k_1, k_2), d)$ satisfying Lemma 6.5.3 when $c \geq 83$.

(k_1, k_2)	d
$(5, 10)$	11
$(10, 5)$	13
$(12, 12)$	13

In the case $(k_1, k_2) = (12, 12)$, $d = 13$, we can enumerate the integral points of Eq. (6.5.1) using Magma's `IntegralQuarticPoints` function [29]. Doing so gives no examples with $c \geq 83$.

When $(k_1, k_2) = (5, 10)$ or $(10, 5)$ and $d = 11$, Sage [103] finds that Eq. (6.5.1) has no solutions over the ring of integers modulo 16, hence it has no integral solutions. Thus these cases also give no examples. □

When $\deg \Phi_{k_1}(x) > 4$, the bound on d in Eq. (6.5.4) no longer converges to a finite value as $c \to \infty$, so we cannot reduce to finding integral points on a finite number of curves as above. It would be interesting to find more general arguments which work for higher-degree cyclotomic polynomials, such as the case of $(16, 16)$-cycles, where $\Phi_{k_1}(x) = \Phi_{k_2}(x) = x^8 + 1$.

6.6 Cycles with the same discriminant

In this section we show that if we construct cycles from elliptic curves of the same discriminant D, then the length of the cycle must be small. This implies that to construct elliptic curves from polynomial families, we cannot use families with a fixed discriminant. The results in this section are *independent* of the embedding degrees of the elliptic curves.

We first show that any 2-cycle of ordinary elliptic curves consists of curves with the same discriminant.

Proposition 6.6.1. *Let $E_1/\mathbb{F}_{q_1}, E_2/\mathbb{F}_{q_2}$ be a 2-cycle of ordinary elliptic curves. Then they both have the same discriminant for complex multiplication.*

Proof. Let t_i be the trace of E_i for each i. Then $q_2 = q_1 + 1 - t_1$ and $q_1 = q_2 + 1 - t_2$. This implies $t_1 + t_2 = 2$, and

$$4q_2 - t_2^2 = 4(q_1 + 1 - t_1) - (2 - t_1)^2 = 4q_1 - t_1^2\,.$$

The discriminant of E_i is the squarefree part of $4q_i - t_i^2$, so the two curves have the same discriminant. □

The converse is also true if $D > 3$, as shown in [111, Corollary 6.2] and [15, Theorem 3.4]. We present an adapted version of the proof below.

Proposition 6.6.2. *Let $D > 3$ be a squarefree integer such that $-D \equiv 0, 1 \pmod 4$. Suppose that we have an m-cycle of ordinary elliptic curves $E_1/\mathbb{F}_{q_1}, \ldots, E_m/\mathbb{F}_{q_m}$ such that each elliptic curve has discriminant D and $q_1, \ldots, q_m$ are distinct primes. Then $m \leq 2$.*

Proof. For each $i = 1, \ldots, m$, let $y_i \in \mathbb{Z}$ be such that the CM equation $4q_i - t_i^2 = Dy_i^2$ is satisfied. Firstly, we note that if we fix q_i and D, the solution (t_i, y_i) to the CM equation is unique up to sign. This follows from the fact that, under our assumptions on D, the units in the ring of integers of $\mathbb{Q}(\sqrt{-D})$ are ±1, hence if two elements have the same norm, then they differ by a multiple of ±1.

Now let $E_i/\mathbb{F}_{q_i}$, $E_{i+1}/\mathbb{F}_{q_{i+1}}$ be two consecutive curves in the cycle. Since

$$4q_{i+1} - (t_i - 2)^2 = 4(q_{i+1} - 1 + t_i) - t_i^2 = 4q_i - t_i^2 = Dy_i^2\,, \tag{6.6.1}$$

thus $t_i - 2 = \pm t_{i+1}$, and $y_i = \pm y_{i+1}$, by the uniqueness of the solution to the CM equation.

Suppose that $m \geq 3$. Without loss of generality, assume that q_2 is the smallest prime in the cycle. Then $q_2 < q_1, q_3$. From the previous paragraph we also have $t_1 - 2 = \pm t_2$. We consider the two cases separately.

If $t_1 - 2 = t_2$, then $q_2 = q_1 - 1 - t_2$. So we have the inequalities $q_1 = q_2 + 1 + t_2 > q_2$, and $q_3 = q_2 + 1 - t_2 > q_2$. Hence $1 > t_2 > -1$ so $t_2 = 0$. But this implies that $q_1 = q_3$, which contradicts the assumption that the q_i's are distinct.

If $t_1 - 2 = -t_2$, then $q_2 = q_1 - 1 + t_2$, so $q_1 = q_2 + 1 - t_2 = q_3$. This again contradicts the assumption that the q_i's are distinct. □

For the case where $D = 3$, we cite the following result from [15].

Proposition 6.6.3 ([15, Theorem 3.4])**.** *Suppose that we have an m-cycle of ordinary elliptic curves $E_1/\mathbb{F}_{q_1}, \ldots, E_m/\mathbb{F}_{q_m}$ such that each elliptic curve has discriminant D and $q_1, \ldots, q_m$ are distinct primes. If $m \geq 3$, then $m = 6$ and $D = 3$.*

The results in this section show that to construct m-cycles of elliptic curves with a fixed discriminant D, either $m \leq 2$ or $m = 6$ and $D = 3$. This places a strong restriction on possible cycles, and implies that we cannot construct long cycles from a single family of elliptic curves with a fixed discriminant. For example, the Barreto–Naehrig curves [19] all have discriminant $D = 3$.

We also note that the results in this section do not depend on the embedding degrees of the elliptic curves. It remains an open question to understand how restricting the embedding degrees places further restrictions on the possible cycles.

6.7 Cycles with cofactors

Allowing for non-prime orders gives greater flexibility in constructing elliptic curves, while still having relevance to cryptographic applications. While there are few embedding degrees that can be achieved by current constructions of prime-order curves, there are methods that achieve *arbitrary* embedding degrees for composite-order curves [44, 55]. While composite-order curves tend to be less preferable than prime-order curves in applications, they can still be practical and sometimes even preferable.[4]

Nevertheless, we show in this section that allowing for non-prime orders does not give us greater flexibility in constructing cycles. Our arguments in this section rely only on the Hasse bound and the constraints on the orders of the elliptic curves posed by the cycle condition.

Definition 6.7.1. *An m-*cycle of elliptic curves with cofactors *consists of m distinct elliptic curves $E_1/\mathbb{F}_{q_1}$,..., $E_m/\mathbb{F}_{q_m}$ such that for positive integer cofactors $h_1, \ldots, h_m$,*

$$\#E_1(\mathbb{F}_{q_1}) = h_1 q_2\,, \ldots, \#E_i(\mathbb{F}_{q_i}) = h_i q_{i+1}\,, \ldots, \#E_m(\mathbb{F}_{q_m}) = h_m q_1\,. \tag{6.7.1}$$

If all the cofactors are 1, then Definition 6.7.1 reduces to Definition 6.1.1. We show that, for any $m > 1$, we cannot have m-cycles of elliptic curves with any nontrivial cofactor (and large orders). We deduce this by considering only the Hasse bound on the orders of the curves.

Proposition 6.7.2. *For all $m > 1$, there exists no m-cycle of elliptic curves having at least one nontrivial cofactor (greater than 1), if $q_1, \ldots, q_m > 12m^2$.*

Proof. We first prove this for the simpler case where $m = 2$. Suppose that we have a 2-cycle of elliptic curves $E_1/\mathbb{F}_{q_1}, E_2/\mathbb{F}_{q_2}$ with cofactors such that $\#E_1(\mathbb{F}_{q_1}) = h_1 q_2$, $\#E_2(\mathbb{F}_{q_2}) = h_2 q_1$. The Hasse bound for E_1 implies

$$q_1 + 1 - 2\sqrt{q_1} \leq h_1 q_2 \leq q_1 + 1 + 2\sqrt{q_1}\,. \tag{6.7.2}$$

[4] For example, Barreto–Lynn-Scott curves [18] are composite-order curves that, thanks to their high embedding degrees, enable efficient implementations at high-security levels. As another example, Edwards curves [58, 22, 24] are composite-order curves that, thanks to their complete formulas for addition, enable efficient implementations that resist various side channels (e.g., [23]).

We can express this as $(\sqrt{q_1}-1)^2 \leq h_1q_2 \leq (\sqrt{q_1}+1)^2$. Applying the same argument to E_2, we get the following two inequalities

$$\sqrt{q_1}-1 \leq \sqrt{h_1q_2} \leq \sqrt{q_1}+1\,, \tag{6.7.3}$$

$$\sqrt{q_2}-1 \leq \sqrt{h_2q_1} \leq \sqrt{q_2}+1\,. \tag{6.7.4}$$

We can then bound q_2 as follows

$$\sqrt{h_1q_2} \leq \frac{1}{\sqrt{h_2}}(\sqrt{q_2}+1)+1\,. \tag{6.7.5}$$

If $h_1 > 1$ or $h_2 > 1$, this implies that

$$\sqrt{q_2} \leq \frac{\sqrt{h_2}+1}{\sqrt{h_1h_2}-1} \leq 1+\frac{2}{\sqrt{h_1h_2}-1} < 3\,. \tag{6.7.6}$$

The same argument applies for bounding q_1. Hence for any 2-cycle with nontrivial cofactors, the elliptic curves must have small orders.

We now extend the argument above to m-cycles with cofactors, for all $m > 2$. Suppose we have an m-cycle with cofactors $\#E_1(\mathbb{F}_{q_1}) = h_1q_2\,, \#E_2(\mathbb{F}_{q_2}) = h_2q_3\,, \ldots, \#E_m(\mathbb{F}_{q_m}) = h_mq_1$. Applying the same argument as before, we have the inequalities

$$\begin{aligned}
\sqrt{h_mq_1} &\leq \sqrt{q_m}+1 && \text{(6.7.7a)}\\
&\leq \frac{1}{\sqrt{h_{m-1}}}(\sqrt{q_{m-1}}+1)+1\\
&\leq \frac{1}{\sqrt{h_{m-1}h_{m-2}}}(\sqrt{q_{m-2}}+1)+\left(1+\frac{1}{\sqrt{h_{m-1}}}\right)\\
&\vdots\\
&\leq \frac{1}{\sqrt{h_{m-1}\cdots h_1}}(\sqrt{q_1}+1)+\left(1+\frac{1}{\sqrt{h_{m-1}}}+\cdots+\frac{1}{\sqrt{h_{m-1}\cdots h_2}}\right)\,. && \text{(6.7.7b)}
\end{aligned}$$

We simplify this to

$$\sqrt{q_1}\left(1-\frac{1}{\sqrt{h_m\cdots h_1}}\right) \leq \frac{1}{\sqrt{h_m}}+\frac{1}{\sqrt{h_mh_{m-1}}}+\cdots+\frac{1}{\sqrt{h_m\cdots h_1}}\,. \tag{6.7.8}$$

If at least one of $h_1, \ldots, h_m$ is greater than 1, then we can bound q_1 as follows.

$$\sqrt{q_1} \leq \frac{m}{1-\frac{1}{\sqrt{h_m\cdots h_1}}} \leq \frac{m}{1-\frac{1}{\sqrt{2}}} = (2+\sqrt{2})m\,. \tag{6.7.9}$$

The above argument applies for $q_2, \ldots, q_m$, hence $q_i \leq (2+\sqrt{2})^2m^2 < 12m^2$ for each i. For cryptographic applications, we would require the elliptic curves to be defined over much larger fields than the size of the cycle, contrary to this bound. □

6.8 Other cycles on parametrized families

We have shown in Section 6.7 that it is not possible to construct cycles of elliptic curves with nontrivial cofactors (and large orders relative to cycle length). Hence cycles of elliptic curves must be assembled from *prime*-order elliptic curves. At present the only known families of *pairing-friendly* prime-order elliptic curves are the MNT curves for $k = 3, 4, 6$, Freeman curves for $k = 10$ [61], and Barreto–Naehrig curves for $k = 12$ [19]. Now we prove that we cannot construct cycles from just Freeman curves or from just Barreto–Naehrig curves.

Proposition 6.8.1. *There do not exist cycles consisting only of Freeman curves.*

Proof. Lemma 6.3.5 poses a restriction on the sum of the traces in a cycle. The trace of the Freeman curves is parametrized by $t(x) = 10x^2 + 5x + 3$ (see Eq. (6.2.4)). We note that $t(x) > 1$ for all $x \in \mathbb{R}$, since the discriminant of $t(x) - 1$ is -55. Hence the condition in Lemma 6.3.5 cannot be satisfied for cycles consisting only of Freeman curves. □

Proposition 6.8.2. *There do not exist cycles consisting only of Barreto–Naehrig curves.*

Proof. We again use Lemma 6.3.5. The trace of the Barreto–Naehrig curves is parametrized by $t(x) = 6x^2 + 1$ (see Eq. (6.2.5)), hence if we have a family of elliptic curves consisting only of Barreto–Naehrig curves, then each trace has to be 1. So $x = 0$ and $q(x) = n(x) = 1$ for every curve in the cycle, which is impossible since $q(x)$ and $n(x)$ have to be prime. □

We remark that the proof of Lemma 6.4.2 also shows that there do not exist cycles consisting of just Barreto–Naehrig curves and MNT curves of embedding degree 3.

For combinations of MNT, Freeman, and Barreto–Naehrig curves, we did a preliminary investigation using Gröbner bases to find solutions to the following system of polynomial equations in m variables $x_1, \ldots, x_m$, where $k_1, \ldots, k_m \in \{3, 4, 6, 10, 12\}$.

$$n_{k_1}(x_1) = q_{k_2}(x_2)\,, n_{k_2}(x_2) = q_{k_3}(x_3), \ldots, n_{k_m}(x_m) = q_{k_1}(x_1)\,. \tag{6.8.1}$$

For $m \leq 4$ we found that the ideals generated by these polynomials have dimension 0 apart from the MNT cycles in Proposition 6.4.1, implying that we cannot construct other families of cycles of length up to 4. We leave it as an open problem to construct cycles from combinations of these families, or to show that they do not exist.

6.9 Conclusion

In this chapter, we studied cycles of pairing-friendly elliptic curves, for an application in pairing-based cryptography. In the next chapter, we will study the concrete security of lattice-based cryptography, based on the hardness of the Learning With Errors problem.

Chapter 7

On the concrete security of LWE with small secret

In this chapter, we study the concrete security of the Learning With Errors (LWE) problem in lattice-based cryptography, when sampling the secret from a non-uniform, small distribution. The material in this chapter is from the paper "On the Concrete Security of LWE with Small Secret" authored with Hao Chen, Kristin Lauter and Yongsoo Song, which has been submitted for publication [38]. This project was done during a summer internship at Microsoft Research, Redmond, in 2019.

7.1 Introduction

Lattice-based cryptography was proposed more than 20 years ago, and is currently used as the basis for Homomorphic Encryption schemes world-wide. Cryptosystems based on the hardness of lattice problems are also under consideration for standardization in the ongoing NIST PQC Post-Quantum Cryptography competition. Both applications rely specifically on the hardness of the *Learning with Errors (LWE)* problem [99]. Homomorphic encryption allows computations on encrypted data, with security parameters for practical applications specified in HES, the Homomorphic Encryption Standard [7]. For practical implementations of homomorphic encryption schemes, it is important to understand the concrete security levels of LWE. While there are various security estimates in the literature [6, 64], there is still a significant gap between our theoretical understanding of the performance of lattice reduction algorithms and their practical performance.

Most Homomorphic Encryption deployments use small secrets as an optimization, so it is important to understand the concrete security of LWE when sampling the secret from a non-uniform, small distribution. Although there are numerous heuristics used to estimate the running time and quality of lattice reduction algorithms such as BKZ2.0 [40], more work is needed to validate and test these heuristics in practice to provide concrete security parameter recommendations, especially in the case of small secret.

In this work, we introduce a new approach which uses concrete attacks on the LWE problem as a way to study the performance and quality of BKZ2.0 directly. We generate random LWE instances using secrets sampled from binary, ternary or discrete Gaussian distributions. We convert each LWE instance into a uSVP instance and run the BKZ2.0 algorithm to find an approximation to the shortest vector. When the attack is successful, we can deduce a bound on the Hermite factor achieved for the given blocksize. We find that the security levels for certain values of the modulus q and dimension n are smaller than predicted by the online LWE Estimator, due to unexpectedly high success probabilities for small blocksizes 30, 35, 40 and 45 on these uSVP lattices. We also ran our experiments on generated instances of the TU Darmstadt LWE challenges and observed significantly lower running times for successful attacks on those instances generated with the binary distribution for the secret vector. We observe that sampling the secret from the discrete Gaussian error distribution yields greater security than the binary or ternary distributions for the same set of parameters.

We conduct a systematic experimental study of the success probability of the BKZ2.0 algorithm on uSVP lattices. Our main motivation is to investigate the concrete security of the *Learning with Errors (LWE)* problem [99], specifically in the setting of homomorphic encryption [7].

For efficiency reasons, it is common in homomorphic encryption to sample the secret from special distributions, such that it has small entries [30]. For example, two common distributions are the *binary* or *ternary* distributions [31, 88], where the entries in the secret are in $\{0, 1\}$ or $\{0, \pm 1\}$ respectively. We also consider secrets sampled from the same small discrete gaussian distribution as the errors. In fact, the Homomorphic Encryption Standard [7] specifies tables of secure parameters for three possible distributions for the secret vector: uniform, ternary, and error distributions. When the secret has a small norm, we can embed such instances of LWE into instances of the *unique Shortest Vector Problem (uSVP)* [8, 16, 17]. To recover the shortest vector, we can then run lattice reduction algorithms, such as the BKZ2.0 algorithm [40] which is currently known to be the most effective.

In this work, we study experimentally the concrete Hermite factor of the BKZ2.0 algorithm on uSVP lattices. We construct instances of LWE in small dimensions, where the secrets are sampled from the binary, ternary and discrete gaussian distributions. We convert each instance into a uSVP instance, and run the BKZ2.0 algorithm to recover the shortest vector. We then compute the Hermite factor of the lattice and compare it with estimates from the literature. Our work demonstrates that the Hermite factor achieved by BKZ2.0 on uSVP lattices may be significantly smaller than the estimates for random lattices used in practice. Furthermore, the trend as we increase the lattice dimension is noticeably downward.

Our approach is similar to the approach taken in earlier work [83] for estimating the approximation factor for the LLL algorithm. Laine and Lauter found that the approximation factor for LLL is significantly better than expected in small dimensions, but it was not clear how that would extend to other lattice reduction algorithms such as BKZ. The attacks presented in [83] also cover the case of secrets sampled from the uniform distribution, but the attacks are only successful for very large moduli.

We also generated instances of the TU Darmstadt LWE challenges [36] with binary, ternary and discrete gaussian secrets, and we run our same attack on these instances. Although our experiments only cover blocksizes 30, 35, 40 and 45, these blocksizes are already large enough to attack all the solved LWE challenges in the online tables, for secrets sampled from the binary and ternary secret distributions. We observe that the discrete gaussian secret distribution yields greater security than the binary or ternary distributions for the same set of parameters, as the attack rarely succeeds. Furthermore, our attacks run in a matter of minutes (under an hour) for blocksizes 30, 35, 40 and in a matter of hours for blocksize 45, for the range of parameters where the actual challenges have been solved.

7.2 Preliminaries

Let $\mathbf{b}_1, \ldots, \mathbf{b}_d \in \mathbb{R}^d$ be d linearly independent vectors, and let $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_d) \in \mathbb{R}^{d\times d}$ be the matrix whose columns are formed by them. The lattice generated by $\mathbf{B}$ is

$$L(\mathbf{B}) = \left\{\mathbf{Bx} \,:\, \mathbf{x} \in \mathbb{Z}^d\right\} . \tag{7.2.1}$$

The *Shortest Vector Problem (SVP)* asks to find the shortest nonzero vector in the lattice, whose norm is the *first minimum*:

$$\lambda_1(L(\mathbf{B})) = \min_{\mathbf{v}\in L(\mathbf{B}),\mathbf{v}\neq 0} ||\mathbf{v}|| , \tag{7.2.2}$$

where we use $||\cdot||$ to denote the ℓ_2-norm. Similarly, the *second minimum* of the lattice is

$$\lambda_2(L(\mathbf{B})) = \min_{\mathbf{v}_1,\mathbf{v}_2\in L(\mathbf{B})} \left\{ \max\{||\mathbf{v}_1||, ||\mathbf{v}_2||\} \,:\, \mathbf{v}_1, \mathbf{v}_2 \text{ linearly independent}\right\} . \tag{7.2.3}$$

The *unique Shortest Vector Problem (uSVP)* with gap γ is a variant of the SVP where $\lambda_2 \geq \gamma \cdot \lambda_1$, for some $\gamma \geq 1$. While random lattices do not satisfy this condition, in Section 7.3 we describe a procedure for embedding an instance of LWE with small secrets to an instance of uSVP.

In this work, we use the BKZ2.0 lattice reduction algorithm [40] to solve instances of the uSVP. Let $\mathbf{b}_1^*, \ldots, \mathbf{b}_d^*$ denote the Gram-Schmidt orthogonalization of the basis vectors. For $1 \leq i \leq d$, let π_i be the orthogonal projection over $(\mathbf{b}_1, \ldots, \mathbf{b}_{i-1})^\perp$. For $1 \leq j \leq k \leq d$, let $B_{[j,k]}$ be the local projected block $(\pi_j(\mathbf{b}_j), \ldots, \pi_j(\mathbf{b}_k))$, and let $L_{[j,k]}$ be the lattice spanned by $B_{[j,k]}$, of dimension $k - j + 1$.

Definition 7.2.1. *A basis* $\mathbf{b}_1, \ldots, \mathbf{b}_d$ *is* BKZ-reduced *with blocksize* $\beta \geq 2$ *if it is LLL-reduced, and for each* $1 \leq j \leq d$, $||\mathbf{b}_j^*|| = \lambda_1(L_{[j,k]})$ *where* $k = \min(j + \beta - 1, d)$.

The BKZ algorithm works by iteratively reducing each local block $B_{[j,k]}$ of size up to β. Each block is first LLL-reduced, before being enumerated to find a vector that is the shortest in the projected lattice $L_{[j,k]}$. The BKZ2.0 algorithm [40] improves on BKZ by modifying the enumeration routine, incorporating the sound pruning technique by [65].

The volume of a lattice is $\mathrm{Vol}(L(\mathbf{B})) = |\det(\mathbf{B})|$. We use the root Hermite factor to measure the quality of the BKZ-reduced basis.

Definition 7.2.2. *The* root Hermite factor δ *of a basis* $\{\mathbf{b}_1, \ldots, \mathbf{b}_d\}$ *is defined by*

$$||\mathbf{b}_1|| = \delta^d \cdot \mathrm{Vol}(L(\mathbf{B}))^{1/d}. \tag{7.2.4}$$

For BKZ with block size β, Chen [39] gives the following estimate for δ which only depends on β.

$$\delta(\beta) \approx \left(\frac{\beta}{2\pi e}(\pi\beta)^{1/\beta}\right)^{\frac{1}{2(\beta-1)}}. \tag{7.2.5}$$

For a large β, we can approximate this by $\beta^{1/2\beta}$.

7.3 Reduction from LWE to uSVP

In this work, we study the uSVP attack on LWE, which is currently the most effective attack if the LWE secret has small entries [8, 17]. There are two known estimates for the conditions under which uSVP can be solved by lattice reduction, which are known as the *2008 estimate* [64] and the *2016 estimate* [9]. In this section, we describe the reduction from LWE to uSVP, which proceeds by first reducing LWE to BDD and then reducing BDD to uSVP. We also describe the 2008 and 2016 estimates, and calculate the optimal parameters for the uSVP attack under these estimates, as well as the predicted values of the Hermite factor.

The LWE Problem

We first define the search variant of the LWE problem.

Definition 7.3.1. *Let* $n \geq 1$*,* $q \geq 2$ *be a prime modulus and let* D_σ *be a discrete gaussian distribution over* $\mathbb{Z}$ *with standard deviation* σ*. Let* $A \in \mathbb{Z}_q^{m\times n}$ *be a matrix with entries uniformly sampled from* $\mathbb{Z}_q$*, let* $\mathbf{s} \in \mathbb{Z}_q^n$ *be a secret vector, and let* $\mathbf{e} \in \mathbb{Z}_q^m$ *be an error vector with entries sampled independently from* D_σ*. Let* $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \pmod{q}$*. The goal of the LWE problem is to find* $\mathbf{s}$*, given* $(\mathbf{A}, \mathbf{b})$*.*

We consider the following distributions for the secret:

- *Binary*: Secret has entries sampled uniformly at random from $\{0, 1\}$.
- *Ternary*: Secret has entries sampled uniformly at random from $\{-0, \pm 1\}$.
- *Gaussian*: Secret has entries sampled from the same discrete gaussian distribution as the error.

Reduction from LWE to BDD

Assuming that the secret has a small norm, we can transform the LWE problem into the *Bounded Distance Decoding (BDD)* problem. Specifically, given a lattice $L(\mathbf{B})$ and a target vector $\mathbf{t}$, such that the distance of $\mathbf{t}$ from $L(\mathbf{B})$ is bounded by a factor of λ_1, the BDD problem asks to find a lattice vector $\mathbf{v} \in L(\mathbf{B})$ close to $\mathbf{t}$. Consider the lattice generated by

$$\mathbf{B}_0 = \begin{pmatrix} \mathbf{I}_n & \mathbf{0} \\ \mathbf{A} & q \cdot \mathbf{I}_m \end{pmatrix} . \tag{7.3.1}$$

Since $\mathbf{As} + \mathbf{e} = \mathbf{b} \pmod{q}$, we can write $\mathbf{b} = \mathbf{As} + \mathbf{e} + q \cdot \mathbf{c}$ for some $\mathbf{c} \in \mathbb{Z}^m$. Hence the lattice contains the vector $\mathbf{B}_0 \begin{pmatrix} \mathbf{s} \\ \mathbf{c} \end{pmatrix} = \begin{pmatrix} \mathbf{s} \\ \mathbf{As} + q\mathbf{c} \end{pmatrix} = \begin{pmatrix} \mathbf{s} \\ \mathbf{b} - \mathbf{e} \end{pmatrix}$. Thus if we solve the BDD problem in the lattice generated by $\mathbf{B}_0$, with respect to the target point $\mathbf{t} = \begin{pmatrix} \mathbf{0} \\ \mathbf{b} \end{pmatrix}$, then we obtain $\begin{pmatrix} \mathbf{s} \\ -\mathbf{e} \end{pmatrix}$, allowing us to recover the secret.

Reduction from BDD to uSVP

We can reduce the BDD problem to an instance of uSVP using Kannan's embedding technique [78]. Consider the basis matrix obtained by adding one row and column to (7.3.1):

$$\mathbf{B}_1 = \begin{pmatrix} \mathbf{B}_0 & \mathbf{t} \\ \mathbf{0} & 1 \end{pmatrix} = \begin{pmatrix} \mathbf{I}_n & \mathbf{0} & \mathbf{0} \\ \mathbf{A} & q \cdot \mathbf{I}_m & \mathbf{b} \\ 0 & 0 & 1 \end{pmatrix} . \tag{7.3.2}$$

The lattice generated by the columns of $\mathbf{B}_1$ contains the unique shortest vector

$$\mathbf{B}_1 \begin{pmatrix} \mathbf{s} \\ \mathbf{c} \\ -1 \end{pmatrix} = \begin{pmatrix} \mathbf{B}_0 \begin{pmatrix} \mathbf{s} \\ \mathbf{c} \end{pmatrix} - \mathbf{t} \\ -1 \end{pmatrix} = \begin{pmatrix} \mathbf{s} \\ -\mathbf{e} \\ -1 \end{pmatrix} . \tag{7.3.3}$$

Assuming that the gap between λ_1 and λ_2 in this lattice is sufficiently large, we can solve for the unique shortest vector using lattice reduction algorithms such as BKZ2.0. We further optimize this by balancing the lengths of the secret and error vectors, scaling the secret by some constant factor ω. If the secret is sampled from the same discrete gaussian distribution as the error, then we set $\omega = 1$. For the binary or ternary secret distributions, consider the matrix

$$\mathbf{B} = \begin{pmatrix} \omega \cdot \mathbf{I}_n & \mathbf{0} & \mathbf{0} \\ \mathbf{A} & q \cdot \mathbf{I}_m & \mathbf{b} \\ 0 & 0 & 1 \end{pmatrix} . \tag{7.3.4}$$

The lattice $L(\mathbf{B})$ generated by (7.3.4) has dimension

$$d = n + m + 1 \tag{7.3.5}$$

and contains a short vector

$$\mathbf{B}\begin{pmatrix}\mathbf{s}\\ \mathbf{c}\\ -1\end{pmatrix} = \begin{pmatrix}\omega\cdot\mathbf{s}\\ \mathbf{A}\mathbf{s}+q\mathbf{c}-\mathbf{b}\\ -1\end{pmatrix} = \begin{pmatrix}\omega\cdot\mathbf{s}\\ -\mathbf{e}\\ -1\end{pmatrix}\,. \tag{7.3.6}$$

Since this is the shortest vector of this lattice, we approximate the first minimum of the lattice by its expected norm:

$$\lambda_1 = \sqrt{\omega^2\cdot||\mathbf{s}||^2+||\mathbf{e}||^2+1} \approx \sqrt{\omega^2\cdot h+m\sigma^2+1}\,, \tag{7.3.7}$$

where σ is the standard deviation of the discrete Gaussian distribution and h is the expected value of $||\mathbf{s}||^2$. We have $h=\frac{n}{2}$ for the binary distribution and $h=\frac{2}{3}n$ for the ternary distribution.

We estimate the second minimum λ_2 to be the same as the first minimum of a random lattice with the same dimension using the *Gaussian Heuristic*. Since the lattice is q-ary, it also contains vectors of norm q, so we have

$$\lambda_2 \approx \min\left\{q, \sqrt{\frac{d}{2\pi e}}\omega^{n/d}q^{m/d}\right\}\,. \tag{7.3.8}$$

We can solve the uSVP using lattice reduction algorithms if λ_2 is sufficiently larger than λ_1. We choose ω to maximize the ratio $\frac{\lambda_2}{\lambda_1}$ as follows. First we write

$$\gamma = \frac{\lambda_2}{\lambda_1} \approx \frac{\min\left\{q, \sqrt{\frac{d}{2\pi e}}\omega^{n/d}q^{m/d}\right\}}{\sqrt{\omega^2h+m\sigma^2}}\,. \tag{7.3.9}$$

We choose the parameters to optimize the second term in the minimum, since the Gaussian Heuristic would asymptotically be smaller than q. Differentiating the expression in (7.3.9) with respect to ω and setting the result to zero, we get

$$\omega^2 = \frac{nm}{h(d-n)}\sigma^2 \approx \frac{n}{h}\sigma^2\,. \tag{7.3.10}$$

This gives us $\omega=\sqrt{2}\sigma$ for the binary distribution and $\omega=\sqrt{\frac{3}{2}}\sigma$ for the ternary distribution. Substituting (7.3.10) into (7.3.7), we get

$$\lambda_1 \approx \sqrt{d}\sigma\,. \tag{7.3.11}$$

This also holds for the case where the secret is sampled from the same discrete gaussian distribution as the error. Notably, the shortest vector has the same ℓ_2-norm regardless of the secret distribution, whereas the ℓ_1-norm differs. Thus we have

$$\gamma = \frac{\min\left\{q, \sqrt{\frac{d}{2\pi e}}\omega^{n/d}q^{m/d}\right\}}{\sqrt{d}\sigma}\,. \tag{7.3.12}$$

Remark 7.3.2. *Another commonly used secret distribution is the* uniform *distribution on $\mathbb{Z}_q$, where the entries of the secret are sampled uniformly at random from $\{0, 1, \ldots, q-1\}$. Since the secret does not have a small norm, the uSVP attack would require a much larger q to succeed. To balance the norms of the secret and error vectors, we would have to choose the scaling factor to be $\omega \approx \frac{\sqrt{3}}{q}\sigma$. However, with the factor of q in the denominator of ω, the Gaussian heuristic would be greater than q, and so we would have $\lambda_2 = q$ from* (7.3.8)*. For the uSVP attack to be effective, λ_2 would have to be much greater than λ_1, which means that q would have to be much larger than in the case of the binary, ternary or gaussian secret distributions.*

There are two known ways for estimating the conditions under which uSVP can be solved using lattice reduction, which are called the *2008 estimate* and the *2016 estimate* in the literature. We study each of these in turn.

2008 estimate

From experiments by Gama and Nguyen [64], they claimed that the shortest vector can be recovered if

$$\gamma = \frac{\lambda_2}{\lambda_1} \geq \delta^d\,, \tag{7.3.13}$$

where δ is the root Hermite factor of the lattice reduction algorithm, up to a multiplicative constant.

In what follows, we will compute the estimate of δ based on the heuristic in (7.3.13) for our setting. We will fix n and q, while choosing the lattice dimension d to maximize γ. First we write

$$\gamma \approx \frac{\sqrt{\frac{d}{2\pi e}}\omega^{n/d}q^{m/d}}{\sqrt{d}\sigma} = \frac{1}{\sqrt{2\pi e}}\frac{\omega^{n/d}q^{m/d}}{\sigma} \approx \frac{1}{\sqrt{2\pi e}}\left(\frac{q}{\omega}\right)^{-n/d}\left(\frac{q}{\sigma}\right) \geq \delta^d\,. \tag{7.3.14}$$

We choose d to maximize the ratio in (7.3.14). Specifically, we maximize $\left(\frac{q}{\omega}\right)^{-n/d}\delta^{-d}$ by setting

$$d = \sqrt{\frac{n\log\left(\frac{q}{\omega}\right)}{\log\delta}}\,. \tag{7.3.15}$$

We solve for the largest possible value of δ as a function of n, q, ω, σ. First, we assume equality in (7.3.14) and take logarithms on both sides:

$$\log\left(\frac{q}{\sqrt{2\pi e}\sigma}\right) - \frac{n}{d}\log\left(\frac{q}{\omega}\right) = d\log\delta\,. \tag{7.3.16}$$

Substituting (7.3.15) and rearranging, we get the *2008 estimate* for δ:

$$\log\delta_{2008} = \frac{\log^2\left(\frac{q}{\sqrt{2\pi e}\sigma}\right)}{4n\log\left(\frac{q}{\omega}\right)}\,. \tag{7.3.17}$$

We substitute (7.3.17) into (7.3.15) to obtain

$$d_{2008} = \frac{2n \log\left(\frac{q}{\omega}\right)}{\log\left(\frac{q}{\sqrt{2\pi e}\sigma}\right)} . \tag{7.3.18}$$

This is the lattice dimension that we will use in our experiments to compute δ_{2008}. We observe that δ_{2008} increases with q. For fixed n, β, we experimentally find the smallest q such that the attack succeeds. Substituting the parameters into (7.3.17), we would then obtain a heuristic estimate of δ_{2008}, which we will compare with the actual value of δ from (7.2.4).

We remark that (7.3.17) only holds for large q, such that λ_2 is given by the Gaussian Heuristic. If $\lambda_2 = q$, then we compute δ_{2008} by using

$$\frac{\lambda_2}{\lambda_1} = \frac{q}{\sqrt{d}\sigma} = \delta_{2008}^d . \tag{7.3.19}$$

This gives us

$$\log \delta_{2008} = \frac{1}{d} \log\left(\frac{q}{\sqrt{d}\sigma}\right) , \tag{7.3.20}$$

where d is given by (7.3.18).

We also compare δ_{2008} with the actual value of δ that we expect from the experiments, using the definition in (7.2.4) and assuming that the shortest vector is successfully recovered, and that λ_2 is equal to the Gaussian Heuristic. We have

$$\delta_{2008}^d = \frac{\lambda_2}{\lambda_1} = \sqrt{\frac{d}{2\pi e}}\delta^{-d} . \tag{7.3.21}$$

This gives us the relation between the expected experimental δ and δ_{2008}.

$$\delta = \frac{1}{\delta_{2008}} \left(\frac{d}{2\pi e}\right)^{1/2d} . \tag{7.3.22}$$

Hence we expect δ to trend differently from δ_{2008}.

2016 estimate

The *2016 estimate* is given in the New Hope key exchange paper [9]. The authors consider the evolution of the Gram-Schmidt coefficients of the unique shortest vector in the BKZ tours, assuming that the Geometric Series Assumption [105] holds. This says that the norms of the Gram-Schmidt vectors after lattice reduction satisfy

$$||\mathbf{b}_i^*|| \approx \delta^{d-2i+2} \cdot \mathrm{Vol}(L(\mathbf{B}))^{1/d} . \tag{7.3.23}$$

The reasoning in [9] is that, if the projection of the unique shortest vector onto the space spanned by the last β Gram-Schmidt vectors is shorter than $\mathbf{b}_{d-\beta+1}^*$, then the SVP oracle in

BKZ would be able to find it when called on the last block of size β. The success condition is thus given by

$$\sqrt{\frac{\beta}{d}}\lambda_1 \leq ||\mathbf{b}^*_{d-\beta+1}|| \,. \tag{7.3.24}$$

Based on these heuristics, we compute the estimated value of δ in our setting. Substituting $\lambda_1 \approx \sqrt{d}\sigma$ and (7.3.23), we get

$$\sqrt{\beta}\sigma \leq \delta^{2\beta-d} \cdot \mathrm{Vol}(L(\mathbf{B}))^{1/d} = \delta^{2\beta-d}\omega^{n/d}q^{m/d} \,. \tag{7.3.25}$$

If we choose d to optimize this ratio, we obtain (7.3.15) again. Substituting (7.3.15) into (7.3.25) and taking logarithms, we get a quadratic equation in $\sqrt{\log\delta}$:

$$2\beta\log\delta - 2\sqrt{n\log\left(\frac{q}{\omega}\right)\log\delta} + \log\left(\frac{q}{\sqrt{\beta}\sigma}\right) = 0 \,. \tag{7.3.26}$$

We solve this equation to get the *2016 estimate* for δ:

$$\log\delta_{2016} = \frac{n\log\left(\frac{q}{\omega}\right)}{4\beta^2}\left(1-\sqrt{1-\frac{2\beta\log\left(\frac{q}{\sqrt{\beta}\sigma}\right)}{n\log\left(\frac{q}{\omega}\right)}}\right)^2 \,, \tag{7.3.27}$$

If the value inside the squareroot is negative, then we take $\log\delta_{2016} = \frac{n\log\left(\frac{q}{\omega}\right)}{4\beta^2}$. We obtain the lattice dimension d_{2016} by substituting (7.3.27) into (7.3.15). For large n, (7.3.27) is asymptotically

$$\log\delta_{2016} \approx \frac{\log^2\left(\frac{q}{\sqrt{\beta}\sigma}\right)}{4n\log\left(\frac{q}{\omega}\right)} \,. \tag{7.3.28}$$

We observe that (7.3.28) is similar to (7.3.17) except for the denominator of q in the numerator. The experiments in [8, 17] suggest that the 2016 estimate is more consistent with experiments than the 2008 estimate. In this paper, we will experimentally compare δ_{2008} and δ_{2016} with actual values of δ.

We compare δ_{2016} with the expected experimental value of δ, using the definition in (7.2.4) and assuming that the shortest vector is successfully recovered. We have

$$\delta_{2016}^{2\beta-d} = \sqrt{\frac{\beta}{d}}\frac{\lambda_1}{\mathrm{Vol}(L(\mathbf{B}))^{1/d}} = \sqrt{\frac{\beta}{d}}\delta^d \,. \tag{7.3.29}$$

Hence we have the relation

$$\delta = \delta_{2016}^{2\beta/d-1}\left(\frac{d}{\beta}\right)^{1/2d} \,. \tag{7.3.30}$$

We observe that δ trends differently from δ_{2016}, similarly to (7.3.22) for the case of δ_{2008}.

7.4 Experiments

Setup

We perform our experiments using a 2.4 GHz Intel® Xeon® E5-2673 v4 processor, with 48 virtual CPUs and 192 GB of RAM. We generate random instances of LWE, and convert them into instances of uSVP via (7.3.4). We sample the errors from a discrete gaussian distribution with standard deviation $\sigma = 3.2$, using the discrete gaussian sampler in [103], and we sample secrets uniformly from the binary, ternary and discrete gaussian distributions. To recover the shortest vector, we use the BKZ2.0 algorithm implemented in `fplll` [116], with the `bkzautoabort` option, and with blocksizes $\beta = 30, 35, 40, 45$. The `bkzautoabort` option causes the algorithm to terminate when the norms of the Gram-Schmidt vectors stop changing.

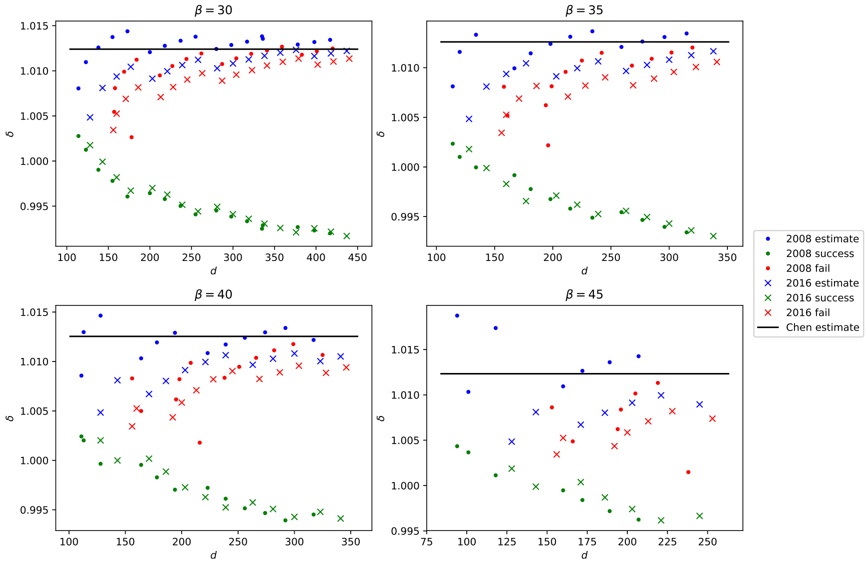
For $\beta = 30$, we choose n from 40 to 200 in steps of 10. For $\beta = 35, 40$, we choose n from 40 to 150, and for $\beta = 45$, we choose n from 40 to 100. We use a smaller range of values of n for higher β, since the running time of BKZ2.0 grows exponentially with β and so it is infeasible to run the experiments for high blocksizes with large n. For each set of parameters, we vary $\log q$ to determine the smallest value of $\log q$ such that BKZ2.0 succeeds in recovering the secret. We perform 10 trials per set of parameters, to account for the randomness in sampling the lattices.

The data are in Tables 7.1 to 7.6, where the rows in boldface contain the data for the smallest value of $\log(q)$ where the attack succeeds. For each set of parameters, we compute the values of the Hermite factor using the estimates in (7.3.17) and (7.3.27), which we tabulate as δ_{2008} and δ_{2016} respectively. Based on the estimates, we also compute the optimal values of the lattice dimensions from (7.3.15), which we tabulate as d_{2008} and d_{2016}. Since these dimensions are different, we conduct two sets of experiments for each set of parameters, where one set has lattice dimension d_{2008} and the other has dimension d_{2016}. We thus divide Tables 7.1 to 7.6 into two parts, where the left parts indicate the experiments for the 2008 estimate and the right for the 2016 estimate.

For each instance, we compute the actual values of δ using the definition in (7.2.4). We split the instances into cases where BKZ2.0 succeeds in recovering the secret, and cases where it fails, and we compute the average value of δ in each scenario. We tabulate these experimental values of δ under the columns labeled "Average successful δ" and "Average failed δ".

In Figures 7.1, 7.2, 7.3, we plot the values of δ against the lattice dimension for the binary, ternary and gaussian secret distributions respectively, with separate plots for each blocksize. In each plot, we plot the values of the 2008 and 2016 estimates for δ against the dimension of the lattice, using blue dots and crosses respectively. For comparison, we plot Chen's estimate (7.2.5) which only depends on the blocksize, using a black line. We also plot the average values of δ for the instances where BKZ2.0 succeeds and fails. The dots and crosses represent attacks run with the dimensions calculated from the 2008 and 2016 estimates respectively, and the green and red represent the successful and failed instances respectively. The data for

Figure 7.1: Plots of δ for binary secrets and $\beta = 30, 35, 40, 45$. The dots and crosses represent attacks run with the dimensions calculated from the 2008 and 2016 estimates respectively. The blue are estimates of δ, and the green and red are the experimental values of δ for the success and failure cases respectively. The black line represents Chen's estimate.



the successful cases is obtained from the smallest value of $\log(q)$ where the attack succeeds, which are the rows in boldface in the tables, while the data for the failed cases is obtained from the largest value of $\log(q)$ where the attack does not succeed, which are the rows directly above those in boldface.

Results

The main observation that we make is that the experimental values of δ for successful instances decrease as the lattice dimension increases, whereas the 2008 and 2016 estimates show increasing trends which seem to approach Chen's estimate. The differing trends is explained by the predicted relations between the successful experimental values and the estimates in (7.3.22) and (7.3.29).

We also observe that the experimental values of δ for failed instances closely follow the 2008 and 2016 estimates. The values of δ for failed instances are higher than for successful instances, which is expected since BKZ2.0 finds shorter vectors for the latter. Moreover, the values of δ for the successful instances decrease as the lattice dimension increases. In the cases where BKZ2.0 fails to recover the unique shortest vector, it recovers instead a vector with length close to the Gaussian Heuristic, and so the algorithm behaves like it would on a random lattice of the same dimension. In these cases, the experimental values of δ closely follow the 2008 and 2016 estimates. This indicates that the estimates accurately capture the behavior of BKZ2.0 on random lattices, but not on successful instances of uSVP.

Figure 7.2: Plots of δ for ternary secrets and $\beta = 30, 35, 40, 45$.

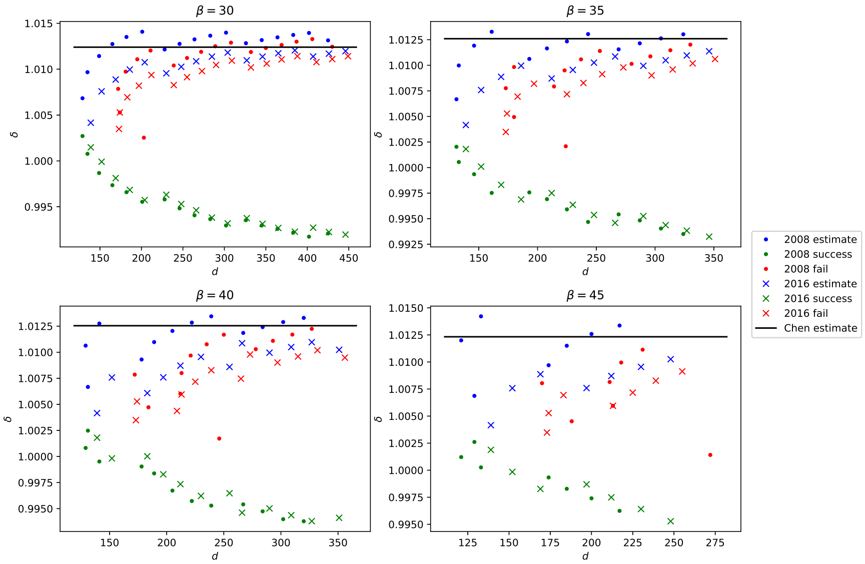
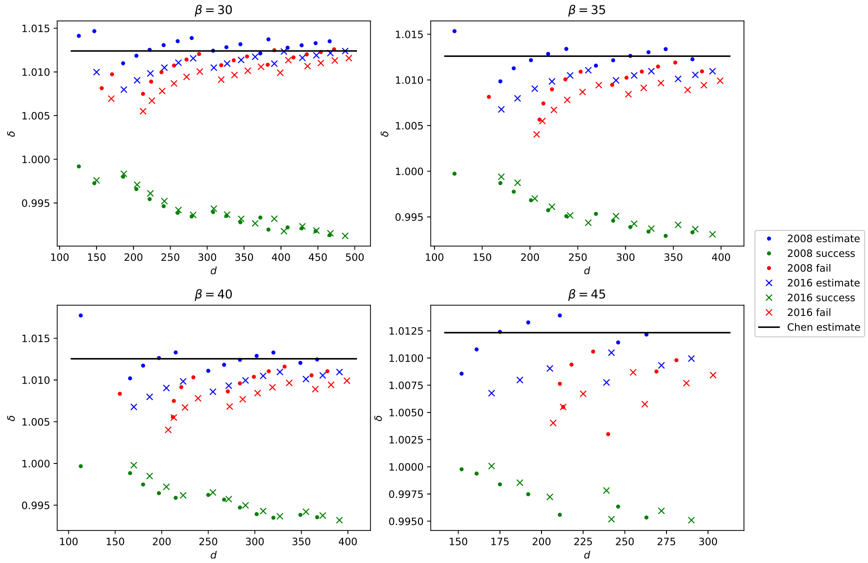


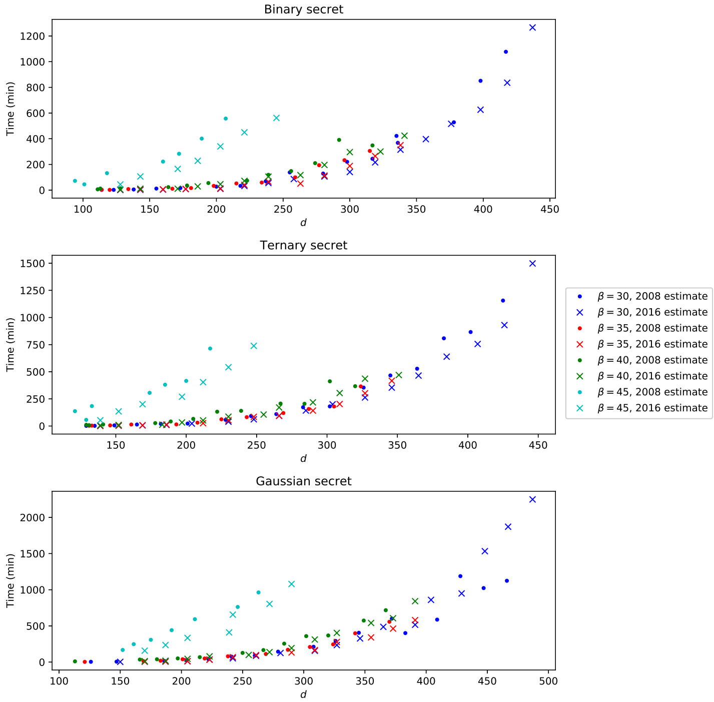
Figure 7.3: Plots of δ for gaussian secrets and $\beta = 30, 35, 40, 45$.



We also observe that the success rates for the 2008 and 2016 estimates are comparable, although the 2008 estimate generally predicts higher lattice dimensions which lead to longer running times. The 2008 estimate also generally predicts higher values of δ than the 2016 estimate, for fixed lattice dimensions.

Additionally, for fixed n and β, the values of $\log q$ and d required to recover the secret is significantly higher for the cases where the secret is sampled from the discrete gaussian

Figure 7.4: Plots of running times in minutes. The dots and crosses represent attacks run with the dimensions calculated from the 2008 and 2016 estimates respectively. The blue, red, green and cyan represent blocksizes 30, 35, 40, 45 respectively.



distribution, as compared to the binary and ternary distributions. The values for the binary and ternary distributions are comparable, though slightly higher for the ternary distribution. This indicates that gaussian secrets yield greater security levels, and would be recommended over binary or ternary secrets in practical applications. For all three secret distributions, the shortest vector has the same ℓ_2-norm, whereas the ℓ_1-norm is highest for the gaussian distribution, followed by the ternary and binary distributions. This indicates a trend of higher security level with increasing ℓ_1-norm, and it would be interesting to study this more systematically.

Due to the experimental nature of our work, we could only produce data for lattices of small dimensions, as the running time of BKZ2.0 grows exponentially with the parameters. We plot the average running times of BKZ2.0 for each set of parameters in Figure 7.4. In the plots, the dots and crosses represent attacks run with the dimensions calculated from the 2008 and 2016 estimates respectively. The blue, red, green and cyan represent blocksizes 30, 35, 40, 45 respectively.

It is infeasible to run our experiments for $\beta \geq 50$ and $n > 100$ within reasonable times. For comparison, with blocksize 50, it takes about 19 hours to run the experiment with binary secrets for $n = 40$ and $\log q = 6$, as compared to an hour for blocksize 45 with the same parameters. It would be desirable to conduct longer experimental studies with higher blocksizes and dimensions, to simulate the parameters used in practical cryptosystems. Nevertheless, our work represents a first step towards a systematic experimental understanding of the Hermite factor of BKZ2.0 on uSVP lattices, which we hope will motivate further studies on the topic.

TU Darmstadt LWE Challenge

Using the same experimental setup, we generate instances of the TU Darmstadt LWE challenges [36]. In the actual challenges, the secrets are sampled from uniform distributions on $\mathbb{Z}_q$; in our experiments we use instead the binary, ternary and gaussian secret distributions.

In the challenges, the discrete Gaussian error distributions have varying standard deviations $\sigma = \alpha q$, where α is a parameter. For each challenge, the parameters n, q, α are fixed. We generate instances with binary, ternary and Gaussian secrets, and we run the uSVP attack using the BKZ2.0 algorithm with blocksizes $\beta = 30, 35, 40, 45$. Due to resource limitations, we run only 3 trials for each set of parameters.

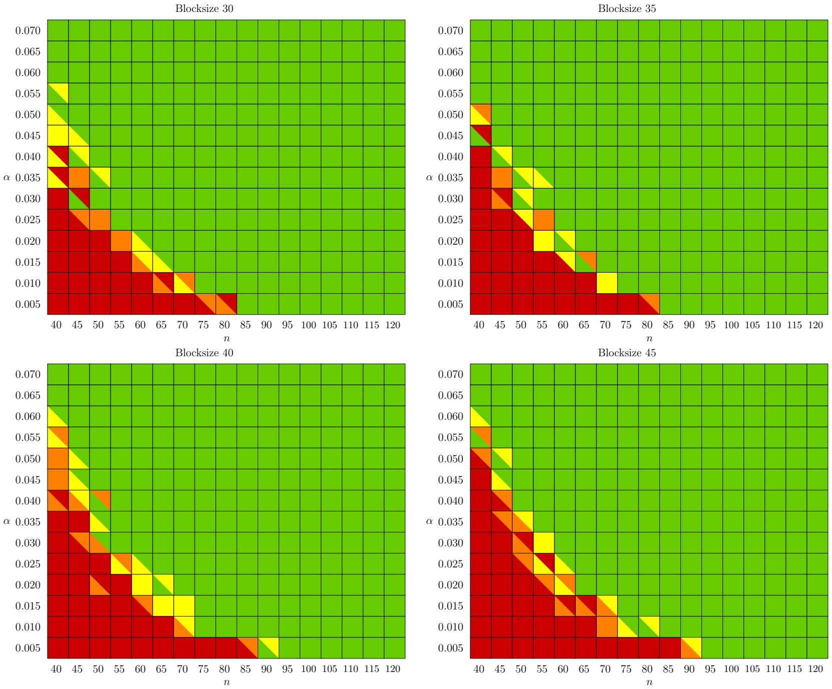
The data from our experiments are in Figures 7.5, 7.6, 7.7. In each figure, we plot a grid for each blocksize, where the columns are indexed by n and the rows by α. Each cell in the grid is colored based on the number of successful trials, where the colors red, orange, yellow and green indicate that the number of successful trials is 3, 2, 1 and 0 respectively. Moreover, the bottom diagonal of each divided cell indicates the 2008 estimate, while the top diagonal indicates the 2016 estimate.

We observe that there is a much higher success rate in solving the challenges for the binary and ternary secret distributions, as compared to the gaussian distribution. This indicates that gaussian secret distributions are more secure for practical applications. Moreover, our running times for the successful instances are significantly less than the records in the actual challenges, which use secrets from uniform distributions. Furthermore, we also observe that we are already able to attack all the solved LWE challenges in the online tables, for secrets sampled from the binary or ternary secret distributions. This indicates that uniform secrets offer much higher security than the secret distributions that we consider, and it would be promising to study the case of uniform secrets in our experimental framework, as a potential follow-up to this work.

7.5 Conclusion

In this chapter, we introduced the Learning With Errors (LWE) problem in lattice-based cryptography, and we studied experimentally the concrete security of LWE when sampling the secret from small distributions. With this chapter, we conclude this thesis, which brings together a collection of works at the interface of computer science and mathematics.

Figure 7.5: TU Darmstadt LWE challenges for binary secrets. Each cell is colored based on the number of successful trials, where the colors red, orange, yellow and green indicate that the number of successful trials is 3, 2, 1 and 0 respectively. The bottom diagonal of each divided cell indicates the 2008 estimate, while the top diagonal indicates the 2016 estimate.



Blocksize 30

Blocksize 35

Blocksize 40

Blocksize 45

Figure 7.6: TU Darmstadt LWE challenges for ternary secrets

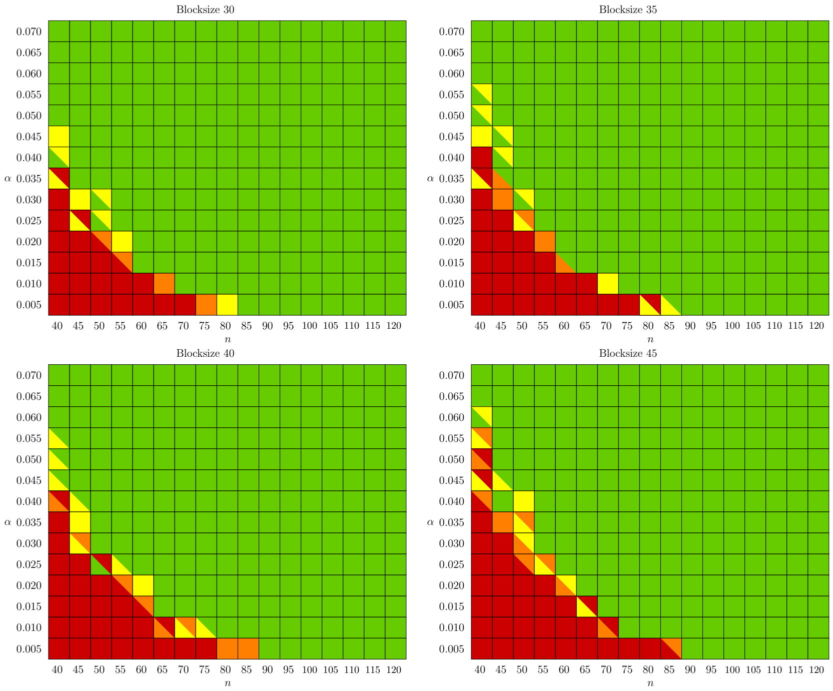


Figure 7.7: TU Darmstadt LWE challenges for gaussian secrets

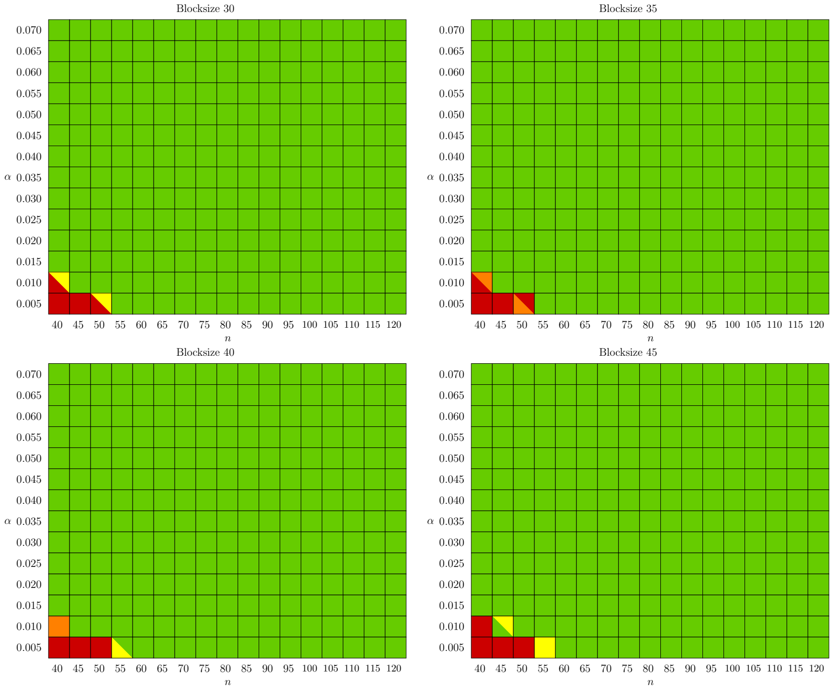


Table 7.1: Binary secrets

β	n	$\log(q)$	d_{2008}	δ_{2008}	Number of successes	Average time (min)	Average successful δ	Average failed δ	d_{2016}	δ_{2016}	Number of successes	Average time (min)	Average successful δ	Average failed δ
30	40	5	156	0.99952	0	1	-	1.00344	178	1.00255	0	2	-	1.00264
		6	**128**	**1.00484**	**5**	**1**	**1.00176**	**1.00661**	**114**	**1.00805**	**7**	**2**	**1.00277**	**1.00835**
		7	114	1.01014	10	1	0.99893	-	83	1.01933	10	1	1.00340	-
	50	6	160	1.00317	0	2	-	1.00525	157	1.00535	0	2	-	1.00545
		7	**143**	**1.00810**	**7**	**2**	**0.99992**	**1.00826**	**123**	**1.01096**	**8**	**2**	**1.00125**	**1.01118**
		8	133	1.01126	10	2	0.99722	-	105	1.01821	10	2	0.99952	-
	60	7	171	1.00671	0	3	-	1.00689	158	1.00793	0	3	-	1.00808
		8	**160**	**1.00937**	**8**	**4**	**0.99819**	**1.00950**	**138**	**1.01258**	**8**	**5**	**0.99903**	**1.01278**
		9	152	1.01219	10	4	0.99558	-	125	1.01808	10	4	0.99752	-
	70	8	186	1.00803	0	6	-	1.00816	169	1.00974	0	7	-	1.00990
		9	**177**	**1.01044**	**10**	**8**	**0.99672**	**-**	**155**	**1.01374**	**10**	**12**	**0.99780**	**-**
	80	8	213	1.00702	0	8	-	1.00709	200	1.00798	0	13	-	1.00805
		9	**203**	**1.00913**	**2**	**10**	**0.99701**	**1.00921**	184	1.01115	0	12	-	1.01123
		10	196	1.0112	10	12	0.99547	-	**173**	**1.01438**	**10**	**16**	**0.99607**	**-**
	90	9	228	1.00811	0	27	-	1.00820	212	1.00940	0	23	-	1.00949
		10	**221**	**1.00995**	**4**	**32**	**0.99628**	**1.01001**	**200**	**1.01207**	**6**	**27**	**0.99644**	**1.01224**
		11	215	1.01183	10	31	0.99452	-	192	1.01485	10	24	0.99525	-
	100	10	245	1.00895	0	45	-	1.00903	227	1.01041	0	42	-	1.01053
		11	**239**	**1.01064**	**7**	**55**	**0.99515**	**1.01073**	**218**	**1.01277**	**8**	**33**	**0.99579**	**1.01291**
		12	234	1.01235	10	54	0.99365	-	211	1.01520	10	35	0.99430	-
	110	11	263	1.00967	0	71	-	1.00973	244	1.01122	0	57	-	1.01131
		12	**258**	**1.01122**	**10**	**86**	**0.99442**	**-**	**237**	**1.01333**	**10**	**69**	**0.99504**	**-**
	120	11	287	1.00886	0	94	-	1.00890	270	1.01001	0	85	-	1.01006
		12	**281**	**1.01028**	**2**	**106**	**0.99492**	**1.01035**	262	1.01187	0	75	-	1.01192
		13	277	1.01172	10	122	0.99372	-	**255**	**1.01378**	**10**	**138**	**0.99409**	**-**
	130	12	304	1.00949	0	78	-	1.00957	287	1.01071	0	112	-	1.01075
		13	**300**	**1.01081**	**2**	**141**	**0.99411**	**1.01085**	**280**	**1.01242**	**2**	**129**	**0.99452**	**1.01247**
		14	296	1.01214	10	174	0.99297	-	274	1.01413	10	148	0.99324	-
	140	13	323	1.01003	0	206	-	1.01007	304	1.01130	0	121	-	1.01138
		14	**319**	**1.01126**	**3**	**216**	**0.99360**	**1.01130**	**298**	**1.01286**	**8**	**220**	**0.99385**	**1.01296**
		15	315	1.01250	10	258	0.99257	-	294	1.01443	10	122	0.99301	-
	150	14	341	1.01051	0	281	-	1.01058	322	1.01180	0	174	-	1.01188
		15	**338**	**1.01166**	**8**	**315**	**0.99306**	**1.01170**	**317**	**1.01323**	**10**	**244**	**0.99333**	**-**
		16	335	1.01282	10	347	0.99196	-	313	1.01467	10	268	0.99224	-
	160	15	360	1.01093	0	253	-	1.01099	341	1.01222	0	334	-	1.01226
		16	**357**	**1.01201**	**10**	**397**	**0.99258**	**-**	**336**	**1.01355**	**10**	**368**	**0.99288**	**-**
	170	16	379	1.01130	0	531	-	1.01136	359	1.01259	0	546	-	1.01267
		17	**376**	**1.01232**	**10**	**516**	**0.99210**	**-**	**335**	**1.01382**	**10**	**422**	**0.99250**	**-**
	180	16	402	1.01067	0	609	-	1.01069	383	1.01175	0	484	-	1.01178
		17	**398**	**1.01163**	**2**	**626**	**0.99254**	**1.01170**	**378**	**1.01291**	**2**	**528**	**0.99268**	**1.01298**
		18	396	1.01260	10	739	0.99167	-	375	1.01406	10	392	0.99179	-
	190	17	421	1.01102	0	761	-	1.01103	401	1.01210	0	392	-	1.01217
		18	**418**	**1.01193**	**9**	**836**	**0.99217**	**1.01196**	**398**	**1.01319**	**10**	**851**	**0.99231**	**-**
		19	415	1.01285	10	937	0.99129	-	394	1.01427	10	881	0.99156	-
	200	18	440	1.01133	0	1183	-	1.01135	420	1.01241	0	951	-	1.01247
		19	**437**	**1.01220**	**6**	**1266**	**0.99169**	**1.01225**	**417**	**1.01343**	**10**	**1077**	**0.99200**	**-**
		20	435	1.01307	10	1450	0.99090	-	414	1.01446	10	1107	0.99114	-
35	40	5	156	0.99952	0	1	-	1.00344	196	1.00210	0	2	-	1.00218
		6	**128**	**1.00484**	**8**	**2**	**1.00180**	**1.00661**	**114**	**1.00812**	**4**	**3**	**1.00234**	**1.00835**
		7	114	1.01014	10	2	0.99879	-	71	1.02702	10	0	1.00566	-
	50	6	160	1.00317	0	3	-	1.00525	161	1.00507	0	3	-	1.00518
		7	**143**	**1.00810**	**9**	**5**	**0.99989**	**1.00826**	**120**	**1.01159**	**10**	**2**	**1.00101**	**-**
		8	133	1.01126	10	4	0.99730	-	96	1.02173	10	2	0.99982	-
	60	7	171	1.00671	0	6	-	1.00689	158	1.00795	0	5	-	1.00808
		8	**160**	**1.00937**	**10**	**6**	**0.99829**	**-**	**134**	**1.01332**	**10**	**8**	**0.99996**	**-**
	70	7	200	1.00534	0	6	-	1.00585	194	1.00614	0	10	-	1.00622
		8	186	1.00803	0	7	-	1.00816	**167**	**1.00994**	**2**	**11**	**0.99917**	**1.01014**
		9	**177**	**1.01044**	**10**	**9**	**0.99656**	**-**	151	1.01447	10	10	0.99747	-
	80	8	213	1.00702	0	12	-	1.00709	199	1.00799	0	15	-	1.00813
		9	**203**	**1.00913**	**5**	**13**	**0.99712**	**1.00921**	**181**	**1.01145**	**6**	**16**	**0.99777**	**1.01160**
		10	196	1.01120	10	24	0.99545	-	170	1.01504	10	15	0.99620	-
	90	9	228	1.00811	0	29	-	1.00820	211	1.00952	0	26	-	1.00958
		10	**221**	**1.00995**	**5**	**41**	**0.99620**	**1.01001**	**198**	**1.01240**	**10**	**33**	**0.99676**	**-**
		11	215	1.01183	10	43	0.99468	-	189	1.01544	10	30	0.99545	-
	100	10	245	1.00895	0	50	-	1.00903	225	1.01058	0	44	-	1.01072
		11	**239**	**1.01064**	**10**	**66**	**0.99526**	**-**	**215**	**1.01312**	**10**	**52**	**0.99580**	**-**

Table 7.2: Binary secrets (continued)

β	n	$\log(q)$	d_{2008}	δ_{2008}	Number of successes	Average time (min)	Average successful δ	Average failed δ	d_{2016}	δ_{2016}	Number of successes	Average time (min)	Average successful δ	Average failed δ
35	110	10	269	1.00814	0	65	-	1.00823	253	1.00924	0	83	-	1.00931
		11	**263**	**1.00967**	**2**	**51**	**0.99557**	**1.00973**	242	1.01142	0	66	-	1.01150
		12	258	1.01122	10	95	0.99449	-	**234**	**1.01367**	**10**	**59**	**0.99489**	**-**
	120	11	287	1.00886	0	111	-	1.00890	268	1.01012	0	88	-	1.01021
		12	**281**	**1.01028**	**2**	**113**	**0.99495**	**1.01035**	**259**	**1.01209**	**3**	**99**	**0.99544**	**1.01220**
		13	277	1.01172	10	137	0.99362	-	252	1.01411	10	91	0.99391	-
	130	12	304	1.00949	0	155	-	1.00957	285	1.01085	0	156	-	1.01090
		13	**300**	**1.01081**	**7**	**188**	**0.99430**	**1.01085**	**277**	**1.01264**	**7**	**194**	**0.99466**	**1.01274**
		14	296	1.01214	10	203	0.99309	-	271	1.01445	10	180	0.99358	-
	140	13	323	1.01003	0	217	-	1.01007	302	1.01146	0	182	-	1.01153
		14	**319**	**1.01126**	**8**	**265**	**0.99361**	**1.01130**	**296**	**1.01309**	**10**	**233**	**0.99396**	**-**
		15	315	1.01250	10	289	0.99250	-	291	1.01473	10	132	0.99281	-
	150	14	341	1.01051	0	312	-	1.01058	320	1.01196	0	243	-	1.01203
		15	**338**	**1.01166**	**10**	**350**	**0.99304**	**-**	**315**	**1.01345**	**10**	**305**	**0.99341**	**-**
40	40	5	156	0.99952	0	3	-	1.00344	216	1.00173	0	6	-	1.00179
		6	**128**	**1.00484**	**6**	**4**	**1.00202**	**1.00661**	**111**	**1.00857**	**6**	**6**	**1.00242**	**1.00881**
		7	114	1.01014	10	5	0.99919	-	80	1.02062	10	3	1.00158	-
	50	6	160	1.00317	0	6	-	1.00525	164	1.00488	0	9	-	1.00499
		7	**143**	**1.00810**	**10**	**11**	**0.99999**	**-**	**113**	**1.01297**	**10**	**12**	**1.00202**	**-**
	60	6	192	1.00217	0	9	-	1.00435	211	1.00353	0	14	-	1.00360
		7	**171**	**1.00671**	**1**	**11**	**1.00017**	**1.00689**	156	1.00811	0	15	-	1.00829
		8	160	1.00937	9	14	0.99821	1.00950	**128**	**1.01464**	**10**	**14**	**0.99965**	**-**
	70	7	200	1.00534	0	17	-	1.00585	195	1.00609	0	21	-	1.00616
		8	**186**	**1.00803**	**5**	**29**	**0.99886**	**1.00816**	**164**	**1.01032**	**4**	**23**	**0.99954**	**1.01051**
		9	177	1.01044	10	32	0.99666	-	145	1.01562	10	17	0.99817	-
	80	8	213	1.00702	0	38	-	1.00709	198	1.00810	0	32	-	1.00821
		9	**203**	**1.00913**	**9**	**46**	**0.99727**	**1.00921**	**178**	**1.01193**	**8**	**36**	**0.99828**	**1.01200**
		10	196	1.01120	10	52	0.99552	-	164	1.01601	10	35	0.99651	-
	90	9	228	1.00811	0	54	-	1.00820	208	1.00974	0	64	-	1.00986
		10	**221**	**1.00995**	**10**	**72**	**0.99628**	**-**	**194**	**1.01290**	**10**	**55**	**0.99703**	**-**
	100	9	253	1.00730	0	79	-	1.00738	238	1.00825	0	82	-	1.00835
		10	245	1.00895	0	81	-	1.00903	**223**	**1.01085**	**2**	**74**	**0.99722**	**1.01091**
		11	**239**	**1.01064**	**10**	**105**	**0.99524**	**-**	212	1.01360	10	74	0.99599	-
	110	10	269	1.00814	0	111	-	1.00823	251	1.00939	0	109	-	1.00946
		11	**263**	**1.00967**	**8**	**117**	**0.99574**	**1.00973**	**239**	**1.01172**	**3**	**119**	**0.99612**	**1.01179**
		12	258	1.01122	10	147	0.99442	-	230	1.01413	10	121	0.99520	-
	120	11	287	1.00886	0	185	-	1.00890	266	1.01031	0	125	-	1.01037
		12	**281**	**1.01028**	**8**	**196**	**0.99508**	**1.01035**	**256**	**1.01240**	**7**	**148**	**0.99515**	**1.01249**
		13	277	1.01172	10	235	0.99374	-	249	1.01454	10	145	0.99409	-
	130	12	304	1.00949	0	235	-	1.00957	282	1.01105	0	195	-	1.01113
		13	**300**	**1.01081**	**10**	**296**	**0.99428**	**-**	**274**	**1.01295**	**10**	**210**	**0.99467**	**-**
	140	12	328	1.00881	0	242	-	1.00885	308	1.00998	0	260	-	1.01004
		13	**323**	**1.01003**	**1**	**300**	**0.99479**	**1.01007**	299	1.01167	0	295	-	1.01176
		14	319	1.01126	10	372	0.99361	-	**292**	**1.01339**	**10**	**391**	**0.99393**	**-**
	150	13	346	1.00936	0	402	-	1.00940	325	1.01063	0	521	-	1.01066
		14	**341**	**1.01051**	**6**	**424**	**0.99412**	**1.01058**	**317**	**1.01218**	**5**	**348**	**0.99452**	**1.01226**
		15	338	1.01166	10	420	0.99328	-	311	1.01375	10	361	0.99364	-
45	40	5	156	0.99952	0	23	-	1.00344	238	1.00142	0	31	-	1.00148
		6	**128**	**1.00484**	**10**	**44**	**1.00187**	**-**	**101**	**1.01033**	**10**	**45**	**1.00366**	**-**
	50	6	160	1.00317	0	69	-	1.00525	166	1.00474	0	64	-	1.00487
		7	**143**	**1.00810**	**10**	**106**	**0.99988**	**-**	**94**	**1.01874**	**10**	**72**	**1.00434**	**-**
	60	6	192	1.00217	0	104	-	1.00435	217	1.00334	0	164	-	1.00340
		7	**171**	**1.00671**	**3**	**165**	**1.00038**	**1.00689**	153	1.00846	0	137	-	1.00862
		8	160	1.00937	10	166	0.99804	-	**118**	**1.01737**	**10**	**132**	**1.00113**	**-**
	70	7	200	1.00534	0	167	-	1.00585	194	1.00611	0	149	-	1.00622
		8	**186**	**1.00803**	**6**	**228**	**0.99869**	**1.00816**	**160**	**1.01094**	**10**	**222**	**0.99947**	**-**
		9	177	1.01044	10	264	0.99667	-	137	1.01755	10	160	0.99959	-
	80	8	213	1.00702	0	284	-	1.00709	196	1.00831	0	320	-	1.00838
		9	**203**	**1.00913**	**10**	**340**	**0.99741**	**-**	**172**	**1.01265**	**10**	**283**	**0.99840**	**-**
	90	9	228	1.00811	0	418	-	1.00820	205	1.01007	0	384	-	1.01015
		10	**221**	**1.00995**	**10**	**450**	**0.99616**	**-**	**189**	**1.01360**	**10**	**401**	**0.99718**	**-**
	100	9	253	1.00730	0	411	-	1.00738	236	1.00841	0	512	-	1.00849
		10	**245**	**1.00895**	**4**	**562**	**0.99665**	**1.00903**	219	1.01123	0	496	-	1.01132
		11	239	1.01064	10	659	0.99520	-	**207**	**1.01426**	**10**	**557**	**0.99624**	**-**

Table 7.3: Ternary secrets

β	n	$\log(q)$	d_{2008}	δ_{2008}	Number of successes	Average time (min)	Average successful δ	Average failed δ	d_{2016}	δ_{2016}	Number of successes	Average time (min)	Average successful δ	Average failed δ
30	40	5	173	0.99927	0	1	-	1.00348	203	1.00218	0	2	-	1.00253
		6	**139**	**1.00416**	**2**	**1**	**1.00148**	**1.00667**	**129**	**1.00683**	**5**	**2**	**1.00271**	**1.00775**
		7	122	1.00949	10	2	0.99893	-	95	1.01570	10	1	1.00126	-
	50	6	174	1.00267	0	2	-	1.00528	174	1.00469	0	3	-	1.00528
		7	**152**	**1.00758**	**7**	**3**	**0.99991**	**1.00842**	**135**	**1.00967**	**3**	**2**	**1.00077**	**1.01069**
		8	141	1.01065	10	3	0.99729	-	115	1.01609	10	2	0.99900	-
	60	7	183	1.00608	0	4	-	1.00694	172	1.00714	0	5	-	1.00785
		8	**169**	**1.00887**	**10**	**6**	**0.99812**	**-**	**149**	**1.01143**	**7**	**6**	**0.99868**	**1.01235**
		9	159	1.01163	10	6	0.99574	-	134	1.01655	10	7	0.99634	-
	70	8	197	1.00759	0	7	-	1.00820	181	1.00895	0	9	-	1.00973
		9	**186**	**1.00996**	**10**	**10**	**0.99684**	**-**	**165**	**1.01274**	**10**	**14**	**0.99735**	**-**
	80	9	212	1.00871	0	16	-	1.00936	195	1.01040	0	27	-	1.01108
		10	**204**	**1.01075**	**10**	**23**	**0.99573**	**-**	**182**	**1.01351**	**10**	**20**	**0.99659**	**-**
	90	9	239	1.00774	0	30	-	1.00827	224	1.00881	0	33	-	1.00942
		10	**230**	**1.00955**	**4**	**40**	**0.99631**	**1.01012**	211	1.01138	0	21	-	1.01203
		11	223	1.01141	10	44	0.99468	-	**201**	**1.01408**	**10**	**23**	**0.99554**	**-**
	100	10	255	1.00859	0	58	-	1.00913	239	1.00985	0	69	-	1.01040
		11	**248**	**1.01026**	**7**	**62**	**0.99530**	**1.01080**	**228**	**1.01215**	**6**	**57**	**0.99580**	**1.01279**
		12	242	1.01195	10	69	0.99380	-	220	1.01452	10	50	0.99439	-
	110	11	273	1.00932	0	84	-	1.00979	255	1.01069	0	73	-	1.01122
		12	**266**	**1.01086**	**9**	**94**	**0.99462**	**1.01141**	**246**	**1.01276**	**10**	**92**	**0.99483**	**-**
		13	261	1.01241	10	100	0.99313	-	239	1.01487	10	93	0.99360	-
	120	12	290	1.00995	0	116	-	1.01046	272	1.01138	0	102	-	1.01189
		13	**285**	**1.01137**	**9**	**143**	**0.99382**	**1.01187**	**264**	**1.01325**	**10**	**110**	**0.99407**	**-**
		14	281	1.01280	10	159	0.99252	-	258	1.01514	10	137	0.99295	-
	130	13	309	1.01049	0	152	-	1.01093	289	1.01195	0	144	-	1.01250
		14	**304**	**1.01181**	**10**	**200**	**0.99319**	**-**	**283**	**1.01365**	**10**	**173**	**0.99366**	**-**
	140	13	332	1.00974	0	225	-	1.01019	314	1.01089	0	219	-	1.01139
		14	**327**	**1.01096**	**5**	**263**	**0.99376**	**1.01142**	308	1.01243	0	153	-	1.01289
		15	323	1.01219	10	286	0.99262	-	**302**	**1.01398**	**10**	**181**	**0.99296**	**-**
	150	14	351	1.01023	0	315	-	1.01061	332	1.01141	0	286	-	1.01187
		15	**346**	**1.01137**	**7**	**354**	**0.99314**	**1.01181**	**326**	**1.01283**	**10**	**354**	**0.99354**	**-**
		16	343	1.01252	10	386	0.99207	-	321	1.01426	10	288	0.99246	-
	160	15	369	1.01065	0	372	-	1.01106	350	1.01185	0	353	-	1.01231
		16	**365**	**1.01173**	**10**	**465**	**0.99269**	**-**	**345**	**1.01317**	**10**	**466**	**0.99296**	**-**
	170	16	388	1.01104	0	584	-	1.01142	369	1.01224	0	455	-	1.01264
		17	**385**	**1.01205**	**10**	**639**	**0.99228**	**-**	**364**	**1.01347**	**10**	**528**	**0.99259**	**-**
	180	16	411	1.01042	0	758	-	1.01077	393	1.01143	0	675	-	1.01179
		17	**407**	**1.01138**	**2**	**756**	**0.99272**	**1.01175**	387	1.01258	0	680	-	1.01300
		18	404	1.01234	10	855	0.99179	-	**383**	**1.01373**	**10**	**808**	**0.99218**	**-**
	190	17	430	1.01078	0	857	-	1.01110	411	1.01180	0	708	-	1.01216
		18	**426**	**1.01169**	**6**	**930**	**0.99225**	**1.01205**	406	1.01287	0	639	-	1.01328
		19	423	1.01260	10	986	0.99144	-	**402**	**1.01395**	**10**	**866**	**0.99174**	**-**
	200	18	449	1.01110	0	1320	-	1.01141	430	1.01212	0	1290	-	1.01245
		19	**446**	**1.01197**	**6**	**1498**	**0.99197**	**1.01228**	**425**	**1.01314**	**10**	**1156**	**0.99209**	**-**
		20	443	1.01284	10	1426	0.99106	-	422	1.01416	10	765	0.99116	-
35	40	5	173	0.99927	0	2	-	1.00348	224	1.00179	0	4	-	1.00208
		6	**139**	**1.00416**	**5**	**2**	**1.00181**	**1.00667**	**131**	**1.00668**	**5**	**3**	**1.00203**	**1.00751**
		7	122	1.00949	10	2	0.99901	-	85	1.01988	10	1	1.00321	-
	50	6	174	1.00267	0	3	-	1.00528	180	1.00441	0	4	-	1.00494
		7	**152**	**1.00758**	**5**	**4**	**1.00009**	**1.00842**	**133**	**1.00998**	**6**	**4**	**1.00054**	**1.01101**
		8	141	1.01065	10	4	0.99736	-	108	1.01816	10	2	0.99953	-
	60	7	183	1.00608	0	6	-	1.00694	173	1.00708	0	9	-	1.00776
		8	**169**	**1.00887**	**10**	**7**	**0.99831**	**-**	**146**	**1.01192**	**9**	**6**	**0.99935**	**1.01267**
	70	8	197	1.00759	0	10	-	1.00820	180	1.00906	0	12	-	1.00983
		9	**186**	**1.00996**	**10**	**14**	**0.99688**	**-**	**161**	**1.01328**	**10**	**14**	**0.99752**	**-**
	80	8	225	1.00664	0	21	-	1.00717	214	1.00735	0	23	-	1.00793
		9	**212**	**1.00871**	**2**	**26**	**0.99750**	**1.00936**	**193**	**1.01062**	**1**	**15**	**0.99757**	**1.01131**
		10	204	1.01075	10	29	0.99569	-	179	1.01403	10	25	0.99637	-
	90	9	239	1.00774	0	40	-	1.00827	223	1.00888	0	24	-	1.00950
		10	**230**	**1.00955**	**7**	**53**	**0.99636**	**1.01165**	**208**	**1.01165**	**8**	**31**	**0.99691**	**1.01238**
		11	223	1.01141	10	54	0.99473	-	198	1.01458	10	27	0.99554	-
	100	10	255	1.00859	0	65	-	1.00913	237	1.00997	0	51	-	1.01058
		11	**248**	**1.01026**	**10**	**85**	**0.99537**	**-**	**225**	**1.01234**	**10**	**62**	**0.99591**	**-**

Table 7.4: Ternary secrets (continued)

β	n	$\log(q)$	d_{2008}	δ_{2008}	Number of successes	Average time (min)	Average successful δ	Average failed δ	d_{2016}	δ_{2016}	Number of successes	Average time (min)	Average successful δ	Average failed δ
35	110	11	273	1.00932	0	48	-	1.00979	253	1.01085	0	62	-	1.01140
		12	**266**	**1.01086**	**10**	**95**	**0.99459**	**-**	**243**	**1.01305**	**10**	**82**	**0.99468**	**-**
	120	11	297	1.00854	0	136	-	1.00901	280	1.00964	0	118	-	1.01014
		12	**290**	**1.00995**	**1**	**142**	**0.99525**	**1.01046**	**269**	**1.01156**	**3**	**120**	**0.99542**	**1.01216**
		13	285	1.01137	10	168	0.99382	-	261	1.01354	10	113	0.99422	-
	130	12	315	1.00918	0	172	-	1.00959	296	1.01039	0	147	-	1.01087
		13	**309**	**1.01049**	**4**	**203**	**0.99437**	**1.01093**	**287**	**1.01215**	**4**	**157**	**0.99483**	**1.01268**
		14	304	1.01181	10	251	0.99313	-	280	1.01393	10	188	0.99371	-
	140	13	332	1.00974	0	260	-	1.01019	313	1.01102	0	218	-	1.01147
		14	**327**	**1.01096**	**8**	**302**	**0.99383**	**1.01142**	**305**	**1.01263**	**10**	**180**	**0.99404**	**-**
		15	323	1.01219	10	306	0.99256	-	299	1.01425	10	233	0.99289	-
	150	14	351	1.01023	0	352	-	1.01061	330	1.01155	0	303	-	1.01202
		15	**346**	**1.01137**	**10**	**417**	**0.99324**	**-**	**324**	**1.01303**	**10**	**365**	**0.99350**	**-**
40	40	5	173	0.99927	0	4	-	1.00348	246	1.00147	0	12	-	1.00172
		6	**139**	**1.00416**	**8**	**6**	**1.00180**	**1.00667**	**131**	**1.00667**	**6**	**8**	**1.00248**	**1.00751**
		7	122	1.00949	10	6	0.99880	-	81	1.02205	10	2	1.00269	-
	50	6	174	1.00267	0	7	-	1.00528	184	1.00418	0	13	-	1.00472
		7	**152**	**1.00758**	**7**	**10**	**0.99982**	**1.00842**	**129**	**1.01063**	**10**	**11**	**1.00082**	**-**
		8	141	1.01065	10	11	0.99731	-	94	1.02384	10	6	1.00122	-
	60	6	209	1.00179	0	18	-	1.00437	234	1.00310	0	24	-	1.00349
		7	**183**	**1.00608**	**1**	**12**	**1.00002**	**1.00694**	172	1.00713	0	16	-	1.00785
		8	169	1.00887	10	13	0.99811	-	**141**	**1.01275**	**10**	**15**	**0.99952**	**-**
	70	7	213	1.00487	0	28	-	1.00595	212	1.00546	0	34	-	1.00601
		8	**197**	**1.00759**	**1**	**33**	**0.99829**	**1.00820**	**178**	**1.00930**	**2**	**27**	**0.99904**	**1.01006**
		9	186	1.00996	10	35	0.99666	-	156	1.01412	10	23	0.99772	-
	80	8	225	1.00664	0	43	-	1.00717	213	1.00740	0	43	-	1.00800
		9	**212**	**1.00871**	**5**	**52**	**0.99735**	**1.00936**	**189**	**1.01097**	**2**	**42**	**0.99838**	**1.01179**
		10	204	1.01075	10	56	0.99566	-	174	1.01480	10	50	0.99665	-
	90	9	239	1.00774	0	63	-	1.00827	221	1.00903	0	60	-	1.00968
		10	**230**	**1.00955**	**8**	**86**	**0.99622**	**1.01012**	**205**	**1.01204**	**7**	**66**	**0.99673**	**1.01237**
		11	223	1.01141	10	93	0.99468	-	193	1.01527	10	76	0.99537	-
	100	9	265	1.00696	0	95	-	1.00746	253	1.00770	0	84	-	1.00819
		10	**255**	**1.00859**	**1**	**106**	**0.99648**	**1.00913**	235	1.01019	0	105	-	1.01076
		11	248	1.01026	10	124	0.99540	-	**222**	**1.01284**	**10**	**132**	**0.99573**	**-**
	110	11	273	1.00932	0	134	-	1.00979	250	1.01110	0	134	-	1.01168
		12	**266**	**1.01086**	**10**	**171**	**0.99461**	**-**	**239**	**1.01344**	**10**	**140**	**0.99529**	**-**
	120	11	297	1.00854	0	170	-	1.00901	278	1.00979	0	189	-	1.01029
		12	**290**	**1.00995**	**4**	**218**	**0.99502**	**1.01046**	**267**	**1.01185**	**4**	**207**	**0.99541**	**1.01235**
		13	285	1.01137	10	233	0.99385	-	258	1.01392	10	185	0.99443	-
	130	12	315	1.00918	0	288	-	1.00959	293	1.01056	0	166	-	1.01109
		13	**309**	**1.01049**	**8**	**304**	**0.99437**	**1.01093**	**284**	**1.01241**	**10**	**205**	**0.99474**	**-**
		14	304	1.01181	10	356	0.99311	-	277	1.01430	10	236	0.99377	-
	140	13	332	1.00974	0	369	-	1.01019	310	1.01121	0	376	-	1.01169
		14	**327**	**1.01096**	**10**	**436**	**0.99380**	**-**	**302**	**1.01289**	**10**	**412**	**0.99399**	**-**
	150	13	356	1.00909	0	479	-	1.00948	336	1.01022	0	363	-	1.01065
		14	**351**	**1.01023**	**1**	**470**	**0.99412**	**1.01061**	327	1.01175	0	343	-	1.01224
		15	346	1.01137	10	500	0.99323	-	**320**	**1.01329**	**10**	**367**	**0.99379**	**-**
45	40	5	173	0.99927	0	44	-	1.00348	272	1.00121	0	54	-	1.00141
		6	**139**	**1.00416**	**7**	**53**	**1.00188**	**1.00667**	**129**	**1.00687**	**10**	**57**	**1.00261**	**-**
		7	122	1.00949	10	95	0.99884	-	90	1.01738	10	73	0.99989	-
	50	6	174	1.00267	0	89	-	1.00528	188	1.00400	0	105	-	1.00452
		7	**152**	**1.00758**	**10**	**135**	**0.99984**	**-**	**121**	**1.01200**	**10**	**137**	**1.00121**	**-**
	60	7	183	1.00608	0	180	-	1.00694	170	1.00728	0	139	-	1.00804
		8	**169**	**1.00887**	**10**	**201**	**0.99827**	**-**	**133**	**1.01422**	**10**	**184**	**1.00026**	**-**
	70	7	213	1.00487	0	217	-	1.00595	213	1.00542	0	241	-	1.00595
		8	**197**	**1.00759**	**3**	**270**	**0.99869**	**1.00820**	**174**	**1.00970**	**7**	**306**	**0.99933**	**1.01053**
		9	186	1.00996	10	329	0.99674	-	150	1.01544	10	263	0.99816	-
	80	8	225	1.00664	0	344	-	1.00717	211	1.00752	0	285	-	1.00815
		9	**212**	**1.00871**	**9**	**404**	**0.99749**	**1.00936**	**185**	**1.01150**	**10**	**381**	**0.99828**	**-**
		10	204	1.01075	10	444	0.99575	-	168	1.01590	10	328	0.99736	-
	90	9	239	1.00774	0	430	-	1.00827	218	1.00927	0	395	-	1.00995
		10	**230**	**1.00955**	**10**	**542**	**0.99641**	**-**	**200**	**1.01259**	**10**	**416**	**0.99740**	**-**
	100	10	255	1.00859	0	583	-	1.00913	231	1.01049	0	570	-	1.01114
		11	**248**	**1.01026**	**10**	**739**	**0.99528**	**-**	**217**	**1.01337**	**10**	**714**	**0.99624**	**-**

Table 7.5: Gaussian secrets

β	n	$\log(q)$	d_{2008}	δ_{2008}	Number of successes	Average time (min)	Average successful δ	Average failed δ	d_{2016}	δ_{2016}	Number of successes	Average time (min)	Average successful δ	Average failed δ
30	40	7	170	1.00677	0	3	-	1.00694	157	1.00799	0	4	-	1.00814
		8	**150**	**1.00998**	**10**	**3**	**0.99758**	**-**	**126**	**1.01413**	**10**	**4**	**0.99918**	**-**
	50	7	213	1.00487	0	5	-	1.00550	207	1.00571	0	11	-	1.00582
		8	**187**	**1.00798**	**4**	**7**	**0.99833**	**1.00813**	171	1.00965	0	7	-	1.00973
		9	171	1.01086	10	8	0.99621	-	**147**	**1.01467**	**10**	**6**	**0.99726**	**-**
	60	8	225	1.00664	0	10	-	1.00671	213	1.00738	0	16	-	1.00749
		9	**205**	**1.00904**	**5**	**11**	**0.99709**	**1.00912**	**186**	**1.01099**	**7**	**16**	**0.99800**	**1.01109**
		10	192	1.01148	10	10	0.99506	-	168	1.01492	10	12	0.99561	-
	70	9	239	1.00775	0	18	-	1.00781	224	1.00882	0	23	-	1.00889
		10	**223**	**1.00983**	**4**	**35**	**0.99609**	**1.00996**	**204**	**1.01185**	**5**	**25**	**0.99659**	**1.01191**
		11	212	1.01200	10	31	0.99415	-	189	1.01516	10	22	0.99487	-
	80	10	255	1.00859	0	46	-	1.00868	238	1.00985	0	32	-	1.00997
		11	**242**	**1.01049**	**9**	**52**	**0.99521**	**1.01060**	**222**	**1.01253**	**10**	**42**	**0.99544**	**-**
		12	232	1.01245	10	56	0.99341	-	209	1.01537	10	43	0.99389	-
	90	11	272	1.00932	0	69	-	1.00943	255	1.01069	0	64	-	1.01073
		12	**261**	**1.01106**	**10**	**87**	**0.99419**	**-**	**241**	**1.01307**	**10**	**75**	**0.99463**	**-**
	100	12	290	1.00995	0	107	-	1.01004	272	1.01138	0	133	-	1.01142
		13	**281**	**1.01155**	**10**	**126**	**0.99363**	**-**	**260**	**1.01352**	**10**	**90**	**0.99387**	**-**
	110	12	319	1.00904	0	138	-	1.00912	303	1.01008	0	116	-	1.01011
		13	**309**	**1.01049**	**1**	**156**	**0.99435**	**1.01053**	289	1.01195	0	136	-	1.01205
		14	300	1.01196	10	172	0.99298	-	**279**	**1.01388**	**10**	**144**	**0.99346**	**-**
	120	13	337	1.00961	0	209	-	1.00965	319	1.01072	0	228	-	1.01077
		14	**327**	**1.01096**	**3**	**235**	**0.99367**	**1.01104**	**308**	**1.01243**	**7**	**212**	**0.99396**	**1.01246**
		15	320	1.01232	10	253	0.99248	-	298	1.01417	10	211	0.99292	-
	130	14	355	1.01011	0	172	-	1.01014	336	1.01126	0	193	-	1.01133
		15	**346**	**1.01137**	**9**	**327**	**0.99318**	**1.01144**	**326**	**1.01283**	**7**	**292**	**0.99352**	**1.01290**
		16	339	1.01264	10	358	0.99195	-	318	1.01443	10	285	0.99215	-
	140	15	373	1.01055	0	423	-	1.01059	354	1.01172	0	390	-	1.01177
		16	**365**	**1.01173**	**9**	**487**	**0.99266**	**1.01181**	**345**	**1.01317**	**10**	**405**	**0.99279**	**-**
		17	359	1.01292	10	499	0.99151	-	337	1.01465	10	429	0.99184	-
	150	15	399	1.00985	0	524	-	1.00991	382	1.01078	0	369	-	1.01082
		16	**391**	**1.01095**	**1**	**516**	**0.99319**	**1.01101**	**372**	**1.01212**	**2**	**601**	**0.99333**	**1.01217**
		17	385	1.01205	10	560	0.99214	-	364	1.01347	10	430	0.99242	-
	160	17	410	1.01130	0	691	-	1.01135	391	1.01247	0	344	-	1.01249
		18	**404**	**1.01234**	**10**	**860**	**0.99177**	**-**	**383**	**1.01373**	**10**	**401**	**0.99195**	**-**
	170	17	436	1.01063	0	1067	-	1.01066	417	1.01160	0	838	-	1.01166
		18	**429**	**1.01161**	**1**	**949**	**0.99232**	**1.01166**	**409**	**1.01277**	**2**	**587**	**0.99220**	**1.01284**
		19	423	1.01260	10	1168	0.99134	-	402	1.01395	10	688	0.99158	-
	180	18	454	1.01096	0	1256	-	1.01102	435	1.01194	0	1285	-	1.01201
		19	**448**	**1.01190**	**2**	**1533**	**0.99184**	**1.01195**	**428**	**1.01305**	**7**	**1188**	**0.99209**	**1.01310**
		20	443	1.01284	10	1600	0.99102	-	422	1.01416	10	694	0.99103	-
	190	19	473	1.01127	0	1642	-	1.01131	454	1.01225	0	1445	-	1.01228
		20	**467**	**1.01216**	**1**	**1871**	**0.99153**	**-**	**447**	**1.01329**	**10**	**1023**	**0.99178**	**-**
		21	462	1.01305	10	1853	0.99057	-	441	1.01434	10	1698	0.99098	-
	200	20	492	1.01155	0	1969	-	1.01158	472	1.01252	0	1757	-	1.01259
		21	**487**	**1.01239**	**10**	**2249**	**0.99123**	**-**	**466**	**1.01351**	**10**	**1124**	**0.99131**	**-**
35	40	6	207	1.00183	0	4	-	1.00403	225	1.00335	0	13	-	1.00341
		7	**170**	**1.00677**	**1**	**4**	**0.99939**	**1.00694**	157	1.00802	0	9	-	1.00814
		8	150	1.00998	10	5	0.99750	-	**121**	**1.01534**	**10**	**3**	**0.99973**	**-**
	50	7	213	1.00487	0	7	-	1.00550	210	1.00556	0	12	-	1.00565
		8	**187**	**1.00798**	**2**	**8**	**0.99874**	**1.00813**	**169**	**1.00984**	**7**	**13**	**0.99870**	**1.00996**
		9	171	1.01086	10	8	0.99614	-	143	1.01560	10	8	0.99759	-
	60	8	225	1.00664	0	13	-	1.00671	214	1.00735	0	22	-	1.00742
		9	**205**	**1.00904**	**6**	**13**	**0.99701**	**1.00912**	**183**	**1.01127**	**6**	**19**	**0.99776**	**1.01146**
		10	192	1.01148	10	19	0.99512	-	164	1.01567	10	10	0.99641	-
	70	9	239	1.00775	0	34	-	1.00781	223	1.00889	0	26	-	1.00897
		10	**223**	**1.00983**	**8**	**33**	**0.99611**	**1.00996**	**201**	**1.01216**	**10**	**39**	**0.99682**	**-**
		11	212	1.0120	10	36	0.99425	-	185	1.01580	10	20	0.99516	-
	80	10	255	1.00859	0	57	-	1.00868	237	1.00998	0	49	-	1.01006
		11	**242**	**1.01049**	**10**	**69**	**0.99516**	**-**	**219**	**1.01285**	**10**	**50**	**0.99573**	**-**
	90	11	272	1.00932	0	84	-	1.00943	253	1.01085	0	76	-	1.01090
		12	**261**	**1.01106**	**10**	**97**	**0.99436**	**-**	**238**	**1.01339**	**10**	**80**	**0.99508**	**-**
	100	11	303	1.00839	0	117	-	1.00843	286	1.00941	0	101	-	1.00946
		12	**290**	**1.00995**	**2**	**133**	**0.99508**	**1.01004**	**269**	**1.01156**	**3**	**112**	**0.99533**	**1.01168**
		13	281	1.01155	10	140	0.99359	-	257	1.01383	10	109	0.99404	-

Table 7.6: Gaussian secrets (continued)

β	n	$\log(q)$	d_{2008}	δ_{2008}	Number of successes	Average time (min)	Average successful δ	Average failed δ	d_{2016}	δ_{2016}	Number of successes	Average time (min)	Average successful δ	Average failed δ
35	110	12	319	1.00904	0	104	-	1.00912	301	1.01018	0	147	-	1.01024
		13	**309**	**1.01049**	**5**	**166**	**0.99425**	**1.01053**	**287**	**1.01215**	**10**	**170**	**0.99458**	**-**
		14	300	1.01196	10	203	0.99302	-	276	1.01417	10	193	0.99346	-
	120	13	337	1.00961	0	235	-	1.00965	317	1.01084	0	259	-	1.01091
		14	**327**	**1.01096**	**10**	**278**	**0.99372**	**-**	**305**	**1.01263**	**8**	**209**	**0.99389**	**1.01270**
		15	320	1.01232	10	321	0.99243	-	295	1.01446	10	139	0.99285	-
	130	13	365	1.00887	0	331	-	1.00890	347	1.00979	0	300	-	1.00985
		14	**355**	**1.01011**	**2**	**341**	**0.99413**	**1.01014**	334	1.01139	0	286	-	1.01146
		15	346	1.01137	10	376	0.99312	-	**324**	**1.01303**	**10**	**245**	**0.99339**	**-**
	140	14	382	1.00939	0	438	-	1.00942	363	1.01038	0	468	-	1.01044
		15	**373**	**1.01055**	**2**	**463**	**0.99366**	**1.01059**	352	1.01186	0	424	-	1.01190
		16	365	1.01173	10	490	0.99274	-	**342**	**1.01337**	**10**	**398**	**0.99292**	**-**
	150	15	399	1.00985	0	526	-	1.00991	380	1.01088	0	756	-	1.01093
		16	**391**	**1.01095**	**3**	**580**	**0.99309**	**1.01101**	**370**	**1.01226**	**1**	**557**	**0.99331**	**1.01231**
		17	385	1.01205	10	698	0.99234	-	361	1.01366	10	487	0.99236	-
40	40	6	207	1.00183	0	9	-	1.00403	233	1.00313	0	20	-	1.00318
		7	**170**	**1.00677**	**3**	**13**	**0.99979**	**1.00694**	155	1.00820	0	12	-	1.00835
		8	150	1.00998	10	12	0.99755	-	**113**	**1.01773**	**10**	**10**	**0.99967**	**-**
	50	7	213	1.00487	0	18	-	1.00550	212	1.00547	0	26	-	1.00555
		8	**187**	**1.00798**	**6**	**19**	**0.99849**	**1.00813**	**166**	**1.01020**	**5**	**35**	**0.99884**	**1.01032**
		9	171	1.01086	10	20	0.99619	-	136	1.01713	10	19	0.99788	-
	60	8	225	1.00664	0	41	-	1.00671	213	1.00740	0	31	-	1.00749
		9	**205**	**1.00904**	**8**	**45**	**0.99720**	**1.00912**	**180**	**1.01172**	**9**	**39**	**0.99748**	**1.01185**
		10	192	1.01148	10	47	0.99502	-	159	1.01679	10	32	0.99676	-
	70	9	239	1.00775	0	65	-	1.00781	221	1.00904	0	73	-	1.00914
		10	**223**	**1.00983**	**10**	**79**	**0.99618**	**-**	**197**	**1.01263**	**10**	**51**	**0.99644**	**-**
	80	9	273	1.00677	0	86	-	1.00682	261	1.00739	0	75	-	1.00747
		10	**255**	**1.00859**	**1**	**99**	**0.99653**	**1.00868**	234	1.01019	0	63	-	1.01032
		11	242	1.01049	10	102	0.99520	-	**215**	**1.01330**	**10**	**68**	**0.99588**	**-**
	90	10	287	1.00764	0	127	-	1.00769	271	1.00857	0	132	-	1.00863
		11	**272**	**1.00932**	**1**	**138**	**0.99573**	**1.00943**	**250**	**1.01110**	**2**	**127**	**0.99623**	**1.01117**
		12	261	1.01106	10	169	0.99440	-	234	1.01382	10	129	0.99515	-
	100	11	303	1.00839	0	173	-	1.00843	284	1.00954	0	203	-	1.00960
		12	**290**	**1.00995**	**6**	**194**	**0.99498**	**1.01004**	**267**	**1.01182**	**5**	**166**	**0.99567**	**1.01186**
		13	281	1.01155	10	209	0.99357	-	253	1.01424	10	149	0.99419	-
	110	12	319	1.00904	0	251	-	1.00912	299	1.01034	0	285	-	1.01038
		13	**309**	**1.01049**	**10**	**312**	**0.99430**	**-**	**284**	**1.01242**	**10**	**255**	**0.99472**	**-**
	120	13	337	1.00961	0	346	-	1.00965	315	1.01102	0	344	-	1.01105
		14	**327**	**1.01096**	**10**	**403**	**0.99367**	**-**	**302**	**1.01289**	**10**	**359**	**0.99393**	**-**
	130	13	365	1.00887	0	409	-	1.00890	345	1.00990	0	345	-	1.00997
		14	**355**	**1.01011**	**1**	**541**	**0.99421**	**1.01014**	332	1.01158	0	433	-	1.01160
		15	346	1.01137	10	552	0.99310	-	**320**	**1.01329**	**10**	**368**	**0.99350**	**-**
	140	14	382	1.00939	0	597	-	1.00942	361	1.01051	0	485	-	1.01056
		15	**373**	**1.01055**	**4**	**606**	**0.99376**	**1.01059**	**349**	**1.01205**	**1**	**574**	**0.99384**	**1.01211**
		16	365	1.01173	10	656	0.99281	-	339	1.01363	10	537	0.99320	-
	150	15	399	1.00985	0	716	-	1.00991	378	1.01102	0	690	-	1.01105
		16	**391**	**1.01095**	**8**	**842**	**0.99320**	**1.01101**	**367**	**1.01246**	**2**	**717**	**0.99356**	**1.01251**
		17	385	1.01205	10	914	0.99233	-	358	1.01391	10	589	0.99239	-
45	40	6	207	1.00183	0	90	-	1.00403	240	1.00294	0	118	-	1.00300
		7	**170**	**1.00677**	**4**	**158**	**1.00007**	**1.00694**	**152**	**1.00856**	**5**	**168**	**0.99977**	**1.00869**
		8	150	1.00998	10	149	0.99754	-	90	1.02778	10	42	1.00463	-
	50	7	213	1.00487	0	175	-	1.00550	213	1.00544	0	121	-	1.00550
		8	**187**	**1.00798**	**7**	**236**	**0.99854**	**1.00813**	**161**	**1.01079**	**10**	**248**	**0.99938**	**-**
		9	171	1.01086	10	300	0.99608	-	126	1.01990	10	107	0.99855	-
	60	8	225	1.00664	0	280	-	1.00671	211	1.00753	0	331	-	1.00763
		9	**205**	**1.00904**	**10**	**334**	**0.99723**	**-**	**175**	**1.01240**	**10**	**308**	**0.99839**	**-**
	70	8	262	1.00569	0	367	-	1.00576	259	1.00585	0	521	-	1.00589
		9	**239**	**1.00775**	**1**	**410**	**0.99782**	**1.00781**	218	1.00929	0	347	-	1.00939
		10	223	1.00983	10	436	0.99620	-	**192**	**1.01327**	**10**	**441**	**0.99748**	**-**
	80	10	255	1.00859	0	542	-	1.00868	231	1.01049	0	615	-	1.01059
		11	**242**	**1.01049**	**10**	**656**	**0.99518**	**-**	**211**	**1.01391**	**10**	**593**	**0.99559**	**-**
	90	10	287	1.00764	0	753	-	1.00769	269	1.00871	0	587	-	1.00876
		11	**272**	**1.00932**	**4**	**804**	**0.99595**	**1.00943**	**246**	**1.01143**	**3**	**762**	**0.99634**	**1.01154**
		12	261	1.01106	10	908	0.99427	-	229	1.01439	10	870	0.99482	-
	100	11	303	1.00839	0	941	-	1.00843	281	1.00973	0	840	-	1.00980
		12	**290**	**1.00995**	**8**	**1080**	**0.99509**	**1.01004**	**263**	**1.01216**	**10**	**963**	**0.99534**	**-**

Bibliography

[1] Robert D. M. Accola. “On defining equations for the Jacobian locus in genus five”. In: *Proc. Amer. Math. Soc.* 89.3 (1983), pp. 445–448.

[2] Malcolm Adams et al. “Invariants of Gauss maps of theta divisors”. In: *Differential geometry: geometry in mathematical physics and related topics (Los Angeles, CA, 1990).* Vol. 54. Proc. Sympos. Pure Math. Amer. Math. Soc., Providence, RI, 1993, pp. 1–8.

[3] Daniele Agostini and Lynn Chua. “Computing Theta Functions with Julia”. In: *arXiv e-prints* (2019). arXiv: `1906.06507`.

[4] Daniele Agostini and Lynn Chua. “On the Schottky problem for genus five Jacobians with a vanishing theta null”. In: *Annali della Scuola Normale Superiore di Pisa, Classe di Scienze* to appear (2020).

[5] Miklós Ajtai. “The shortest vector problem in L2 is NP-hard for randomized reductions”. In: *Proceedings of the thirtieth annual ACM symposium on Theory of computing.* ACM. 1998, pp. 10–19.

[6] Martin Albrecht, Rachel Player, and Sam Scott. “On the concrete hardness of Learning with Errors”. In: *Journal of Mathematical Cryptology* 9.3 (2015), pp. 169–203.

[7] Martin Albrecht et al. *Homomorphic Encryption Security Standard.* Tech. rep. Toronto, Canada: HomomorphicEncryption.org, 2018.

[8] Martin Albrecht et al. “Revisiting the Expected Cost of Solving uSVP and Applications to LWE”. In: *Advances in Cryptology – ASIACRYPT 2017.* Ed. by Tsuyoshi Takagi and Thomas Peyrin. Cham: Springer International Publishing, 2017, pp. 297–322.

[9] Erdem Alkim et al. “Post-quantum Key Exchange—A New Hope”. In: *25th USENIX Security Symposium (USENIX Security 16).* Austin, TX: USENIX Association, 2016, pp. 327–343.

[10] Aldo Andreotti. “On a Theorem of Torelli”. In: *Amer. J. Math.* 80 (1958), p. 801.

[11] Aldo Andreotti and Alan L. Mayer. “On period relations for abelian integrals on algebraic curves”. In: *Annali della Scuola Normale Superiore di Pisa - Classe di Scienze* Ser. 3, 21 (1967), pp. 189–238.

[12] Enrico Arbarello, Maurizio Cornalba, and Phillip A. Griffiths. *Geometry of algebraic curves. Vol. II.* Vol. 268. Grundlehren der Mathematischen Wissenschaften. With a contribution by Joseph D. Harris. Springer, Heidelberg, 2011, pp. xxx+963.

[13] Enrico Arbarello et al. *Geometry of algebraic curves. Vol. I.* Vol. 267. Grundlehren der Mathematischen Wissenschaften. Springer-Verlag, New York, 1985, pp. xvi+386.

[14] Robert Auffarth, Giulio Codogni, and Riccardo Salvati Manni. "The Gauss map and secants of the Kummer variety". In: *Bull. Lond. Math. Soc.* (2019).

[15] Liljana Babinkostova et al. "Elliptic Reciprocity". In: *ArXiv e-prints* (2012). arXiv: `1212.1983`.

[16] Shi Bai and Steven D. Galbraith. "Lattice Decoding Attacks on Binary LWE". In: *Information Security and Privacy.* Cham: Springer International Publishing, 2014, pp. 322–337.

[17] Shi Bai, Shaun Miller, and Weiqiang Wen. "A Refined Analysis of the Cost for Solving LWE via uSVP". In: *Progress in Cryptology – AFRICACRYPT 2019.* Cham: Springer International Publishing, 2019, pp. 181–205.

[18] Paulo SLM Barreto, Ben Lynn, and Michael Scott. "Constructing elliptic curves with prescribed embedding degrees". In: *International Conference on Security in Communication Networks.* Springer. 2002, pp. 257–267.

[19] Paulo SLM Barreto and Michael Naehrig. "Pairing-friendly elliptic curves of prime order". In: *International Workshop on Selected Areas in Cryptography.* Springer. 2005, pp. 319–331.

[20] Arnaud Beauville. "Prym varieties and the Schottky problem". In: *Invent. Math.* 41.2 (1977), pp. 149–196.

[21] Eli Ben-Sasson et al. "Scalable Zero Knowledge via Cycles of Elliptic Curves". In: *Proceedings of the 34th Annual International Cryptology Conference.* CRYPTO '14. 2014, pp. 276–294.

[22] Daniel J. Bernstein and Tanja Lange. "Faster addition and doubling on elliptic curves". In: *Proceedings of the 13th International Conference on the Theory and Application of Cryptology and Information Security.* ASIACRYPT '07. 2007, pp. 29–50.

[23] Daniel J. Bernstein et al. "High-speed High-security Signatures". In: *Proceedings of the 13th International Conference on Cryptographic Hardware and Embedded Systems.* CHES '11. 2011, pp. 124–142.

[24] Daniel J. Bernstein et al. "Twisted Edwards curves". In: *Proceedings of the 1st International Conference on Cryptology in Africa.* AFRICACRYPT' 08. 2008, pp. 389–405.

[25] Jeff Bezanson et al. "Julia: A Fresh Approach to Numerical Computing". In: *SIAM Review* 59.1 (2017), pp. 65–98. eprint: `https://doi.org/10.1137/141000671`.

[26] Christina Birkenhake and Herbert Lange. *Complex Abelian Varieties.* Grundlehren der mathematischen Wissenschaften. Springer-Verlag Berlin Heidelberg, 2004.

[27] Barbara Bolognese, Madeline Brandt, and Lynn Chua. "From curves to tropical Jacobians and back". In: *Combinatorial Algebraic Geometry: Selected Papers From the 2016 Apprenticeship Program.* New York, NY: Springer New York, 2017, pp. 21–45.

[28] Dan Boneh and Matthew K. Franklin. "Identity-Based Encryption from the Weil Pairing". In: *SIAM Journal on Computing* 32.3 (2003), pp. 586–615.

[29] Wieb Bosma, John Cannon, and Catherine Playoust. "The Magma algebra system. I. The user language". In: *J. Symbolic Comput.* 24.3-4 (1997). Computational algebra and number theory (London, 1993), pp. 235–265.

[30] Zvika Brakerski and Vinod Vaikuntanathan. "Efficient Fully Homomorphic Encryption from (Standard) LWE". In: *2011 IEEE 52nd Annual Symposium on Foundations of Computer Science.* 2011, pp. 97–106.

[31] Zvika Brakerski et al. "Classical Hardness of Learning with Errors". In: *Proceedings of the Forty-fifth Annual ACM Symposium on Theory of Computing.* STOC '13. New York, NY, USA: ACM, 2013, pp. 575–584.

[32] Silvia Brannetti, Margarida Melo, and Filippo Viviani. "On the tropical Torelli map". In: *Advances in Mathematics* 226.3 (2011), pp. 2546–2586.

[33] Arthur Breitman. *Scaling Tezos.* 2017. URL: `https://hackernoon.com/scaling-tezo-8de241dd91bd`.

[34] Friederike Brezing and Annegret Weng. "Elliptic curves suitable for pairing based cryptography". In: *Designs, Codes and Cryptography* 37.1 (2005), pp. 133–141.

[35] Nils Bruin, Jeroen Sijsling, and Alexandre Zotine. *Riemann matrices and endomorphism rings of algebraic Riemann surfaces.* 2019. URL: `http://doc.sagemath.org/html/en/reference/curves/sage/schemes/riemann_surfaces/riemann_surface.html`.

[36] Johannes Buchmann et al. "Creating Cryptographic Challenges Using Multi-Party Computation: The LWE Challenge". In: *Proceedings of the 3rd ACM International Workshop on ASIA Public-Key Cryptography.* AsiaPKC '16. Xi'an, China: ACM, 2016, pp. 11–20.

[37] Melody Chan. "Combinatorics of the tropical Torelli map". In: *Algebra & Number Theory* 6.6 (2012), pp. 1133–1169.

[38] Hao Chen et al. "On the concrete security of LWE with small secret". In: *Submitted* (2020).

[39] Yuanmi Chen. "Réduction de réseau et sécurité concrète du chiffrement complètement homomorphe". Thèse de doctorat dirigée par Nguyen, Phong-Quang Informatique Paris 7 2013. PhD thesis. 2013, 1 vol. (133 p.) URL: `http://www.theses.fr/2013PA077242`.

[40] Yuanmi Chen and Phong Q. Nguyen. “BKZ 2.0: Better Lattice Security Estimates”. In: *Advances in Cryptology – ASIACRYPT 2011*. Ed. by Dong Hoon Lee and Xiaoyun Wang. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 1–20. ISBN: 978-3-642-25385-0.

[41] Alessandro Chiesa, Lynn Chua, and Matthew Weidner. “On Cycles of Pairing-Friendly Elliptic Curves”. In: *SIAM Journal on Applied Algebra and Geometry* 3.2 (2019), pp. 175–192.

[42] Christopher Swierczewski et. al. *Abelfunctions: A library for computing with Abelian functions, Riemann surfaces, and algebraic curves*. 2016. URL: `https://www.github.com/abelfunctions/abelfunctions`.

[43] Lynn Chua, Mario Kummer, and Bernd Sturmfels. “Schottky algorithms: Classical meets tropical”. In: *Mathematics of Computation* 88 (2019), pp. 2541–2558.

[44] C. Cocks and R.G.E. Pinch. “Identity-based cryptosystems based on the Weil pairing”. Unpublished manuscript. 2001.

[45] Coda. *Coda Cryptocurrency Protocol*. 2018. URL: `https://codaprotocol.com/`.

[46] Giulio Codogni, Samuel Grushevsky, and Edoardo Sernesi. “The degree of the Gauss map of the theta divisor”. In: *Algebra Number Theory* 11.4 (2017), pp. 983–1001.

[47] Maurizio Cornalba. “Moduli of curves and theta-characteristics”. In: *Lectures on Riemann Surfaces*. World Scientific, 1989, pp. 560–589.

[48] Francesco Dalla Piazza, Alessio Fiorentino, and Riccardo Salvati Manni. “Plane quartics: the universal matrix of bitangents”. In: *Israel J. Math.* 217.1 (2017), pp. 111–138.

[49] Robin De Jong. “Theta functions on the theta divisor”. In: *Rocky Mountain J. Math.* 40.1 (2010), pp. 155–176.

[50] Olivier Debarre. “Le lieu des variétés abéliennes dont le diviseur thêta est singulier a deux composantes”. In: *Ann. Sci. École Norm. Sup. (4)* 25.6 (1992), pp. 687–707.

[51] Bernard Deconinck and Mark van Hoeij. “Computing Riemann matrices of algebraic curves”. In: vol. 152/153. Advances in nonlinear mathematics and science. 2001, pp. 28–46.

[52] Bernard Deconinck et al. “Computing Riemann theta functions”. In: *Mathematics of Computation* 73.247 (2004), pp. 1417–1442.

[53] Max Deuring. “Die Typen der Multiplikatorenringe elliptischer Funktionenkörper”. In: *Abh. Math. Sem. Hansischen Univ.* 14 (1941), pp. 197–272.

[54] Ron Donagi. “Non-Jacobians in the Schottky loci”. In: *Ann. of Math. (2)* 126.1 (1987), pp. 193–217.

[55] Régis Dupont, Andreas Enge, and François Morain. “Building curves with arbitrary small MOV degree over finite prime fields”. In: *Journal of Cryptology* 18.2 (2005), pp. 79–89.

[56] Mathieu Dutour Sikirić. *Polyhedral, a GAP package.* 2013. URL: `http://mathieudutour.altervista.org/Polyhedral/index.html`.

[57] Mathieu Dutour Sikirić et al. "The complete classification of five-dimensional Dirichlet-Voronoi polyhedra of translational lattices". In: *Acta Crystallographica A.* 72(6) (2016).

[58] Harold M. Edwards. "A Normal Form for Elliptic Curves". In: *Bulletin of the American Mathematical Society* 44.3 (2007), pp. 393–422.

[59] Hershel Farkas, Samuel Grushevsky, and Riccardo Salvati Manni. "An explicit solution to the weak Schottky problem". In: *arXiv e-prints* (2017). arXiv: `1710.02938`.

[60] Jörg Frauendiener, Carine Jaber, and Christian Klein. "Efficient computation of multidimensional theta functions". In: *Journal of Geometry and Physics* 141 (2019), pp. 147–158.

[61] David Freeman. "Constructing pairing-friendly elliptic curves with embedding degree 10". In: *International Algorithmic Number Theory Symposium.* Springer. 2006, pp. 452–465.

[62] David Freeman, Michael Scott, and Edlyn Teske. "A taxonomy of pairing-friendly elliptic curves". In: *Journal of Cryptology* 23.2 (2010), pp. 224–280.

[63] Gerhard Frey and Hans-Georg Rück. "A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves". In: *Math. Comp.* 62.206 (1994), pp. 865–874.

[64] Nicolas Gama and Phong Q. Nguyen. "Predicting Lattice Reduction". In: *Advances in Cryptology – EUROCRYPT 2008.* Ed. by Nigel Smart. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 31–51.

[65] Nicolas Gama, Phong Q. Nguyen, and Oded Regev. "Lattice Enumeration Using Extreme Pruning". In: *Advances in Cryptology – EUROCRYPT 2010.* Ed. by Henri Gilbert. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 257–278.

[66] *GAP – Groups, Algorithms, and Programming, Version 4.8.5.* The GAP Group. 2016. URL: `http://www.gap-system.org)`.

[67] Ewgenij Gawrilow and Michael Joswig. "polymake: a framework for analyzing convex polytopes". In: *Polytopes—combinatorics and computation (Oberwolfach, 1997).* Vol. 29. DMV Sem. Birkhäuser, Basel, 2000, pp. 43–73.

[68] Alain Ghouila-Houri. "Caractérisation des matrices totalement unimodulaires". In: *C. R. Acad. Sci. Paris* 254 (1962), pp. 1192–1194.

[69] Daniel Grayson and Michael Stilmann. *Macaulay2, a software system for research in algebraic geometry.* URL: `http://www.math.uiuc.edu/Macaulay2/`.

[70] Samuel Grushevsky. "The Schottky problem". In: *Current developments in algebraic geometry.* Vol. 59. MSRI Publications. Cambridge University Press, 2012.

[71] Samuel Grushevsky and Riccardo Salvati Manni. “Jacobians with a vanishing theta-null in genus 4”. In: *Israel J. Math.* 164.1 (2008), pp. 303–315.

[72] Samuel Grushevsky and Riccardo Salvati Manni. “Singularities of the theta divisor at points of order two”. In: *Int. Math. Res. Not.* 15 (2007).

[73] Samuel Grushevsky and Martin Möller. “Explicit formulas for infinitely many Shimura curves in genus 4”. In: *Asian J. Math.* 22.2 (2018), pp. 381–390.

[74] Jun-ichi Igusa. “A desingularization problem in the theory of Siegel modular functions”. In: *Math. Ann.* 168 (1967), pp. 228–260.

[75] Jun-ichi Igusa. “On the irreducibility of Schottky’s divisor”. In: *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* 28.3 (1981), pp. 531–545.

[76] Nathan Jones. “Elliptic aliquot cycles of fixed length”. In: *Pacific J. Math.* 263.2 (2013), pp. 353–371.

[77] Antoine Joux. “A One Round Protocol for Tripartite Diffie–Hellman”. In: *Journal of Cryptology* 17.4 (2004), pp. 263–276.

[78] Ravi Kannan. “Minkowski’s Convex Body Theorem and Integer Programming”. In: *Mathematics of Operations Research* 12.3 (1987), pp. 415–440.

[79] Koray Karabina and Edlyn Teske. “On Prime-Order Elliptic Curves with Embedding Degrees k=3, 4, and 6”. In: *Algorithmic Number Theory.* Ed. by Alfred J. van der Poorten and Andreas Stein. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 102–117.

[80] George Kempf. “On the geometry of a theorem of Riemann”. In: *Ann. of Math. (2)* 98 (1973), pp. 178–185.

[81] George Kempf. “The equations defining a curve of genus 4”. In: *Proc. Amer. Math. Soc.* 97.2 (1986), pp. 219–225.

[82] Thomas Krämer. “Cubic threefolds, Fano surfaces and the monodromy of the Gauss map”. In: *Manuscripta Mathematica* 149 (2015), pp. 303–314.

[83] Kim Laine and Kristin Lauter. *Key Recovery for LWE in Polynomial Time.* Cryptology ePrint Archive. 2015. URL: `https://eprint.iacr.org/2015/176`.

[84] Serge Lang. *Fundamentals of Diophantine Geometry.* New York, NY: Springer New York, 1983.

[85] Arjen Klaas Lenstra, Hendrik Willem Lenstra, and László Lovász. “Factoring polynomials with rational coefficients”. In: *Mathematische Annalen* 261.4 (1982), pp. 515–534.

[86] Diane Maclagan and Bernd Sturmfels. *Introduction to tropical geometry.* Vol. 161. Graduate Studies in Mathematics. American Mathematical Society, Providence, RI, 2015, pp. xii+363.

[87] A. J. Menezes, T. Okamoto, and S. A. Vanstone. “Reducing elliptic curve logarithms to logarithms in a finite field”. In: *IEEE Transactions on Information Theory* 39.5 (1993), pp. 1639–1646.

[88] Daniele Micciancio and Chris Peikert. “Hardness of SIS and LWE with Small Parameters”. In: *Advances in Cryptology – CRYPTO 2013*. Ed. by Ran Canetti and Juan A. Garay. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 21–39.

[89] Preda Mihăilescu. “Cyclotomy of rings & primality testing”. PhD thesis. ETH Zürich, Zürich, 1997.

[90] Preda Mihăilescu. “Dual Elliptic Primes and Applications to Cyclotomy Primality Proving”. In: *ArXiv e-prints* (2007). arXiv: `0709.4113`.

[91] Grigory Mikhalkin and Ilia Zharkov. “Tropical curves, their Jacobians and theta functions”. In: *Curves and abelian varieties.* Vol. 465. Contemp. Math. Amer. Math. Soc., Providence, RI, 2008, pp. 203–230.

[92] Atsuko Miyaji, Masaki Nakabayashi, and Shunzou Takano. “New explicit conditions of elliptic curve traces for FR-reduction”. In: *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences* 84.5 (2001), pp. 1234–1243.

[93] David Mumford. “On the Kodaira dimension of the Siegel modular variety”. In: *Lecture Notes in Mathematics*. Springer Berlin Heidelberg, 1983, pp. 348–375.

[94] David Mumford. *Tata lectures on theta. II.* Modern Birkhäuser Classics. Birkhäuser Boston, Inc., Boston, MA, 2007.

[95] John Christian Ottem et al. “Quartic spectrahedra”. In: *Math. Program.* 151.2, Ser. B (2015), pp. 585–612.

[96] James Parks. “Amicable pairs and aliquot cycles on average”. In: *Int. J. Number Theory* 11.6 (2015), pp. 1751–1790.

[97] James Parks. “An asymptotic for the average number of amicable pairs for elliptic curves”. In: *Mathematical Proceedings of the Cambridge Philosophical Society* (2017), pp. 1–27.

[98] Wilhelm Plesken and Bernd Souvignier. *isom and autom.* 1995. URL: `http://www.math.uni-rostock.de/~waldmann/ISOM_and_AUTO.zip`.

[99] Oded Regev. “On Lattices, Learning with Errors, Random Linear Codes, and Cryptography”. In: *J. ACM* 56.6 (2009), 34:1–34:40.

[100] Oded Regev. “On lattices, learning with errors, random linear codes, and cryptography”. In: *Proceedings of the thirty-seventh annual ACM symposium on Theory of computing - STOC ’05*. ACM Press, 2005.

[101] Qingchun Ren et al. “The universal Kummer threefold”. In: *Exp. Math.* 22.3 (2013), pp. 327–362.

[102] Herman Rohrbach. “The Geometry of the Gauss Map and Moduli of Abelian Varieties”. MA thesis. Universiteit Leiden, 2014.

[103] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 8.6)*. 2019. URL: `https://www.sagemath.org`.

[104] Takakazu Satoh and Kiyomichi Araki. “Fermat Quotients and the Polynomial Time Discrete Log Algorithm for Anomalous Elliptic Curves”. In: *Commentarii mathematici Universitatis Sancti Pauli* 47.1 (1998), pp. 81–92.

[105] Claus P. Schnorr. “Lattice Reduction by Random Sampling and Birthday Methods”. In: *STACS 2003*. Ed. by Helmut Alt and Michel Habib. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 145–156.

[106] Claus-Peter Schnorr and Martin Euchner. “Lattice basis reduction: Improved practical algorithms and solving subset sum problems”. In: *Mathematical Programming* 66.1-3 (1994), pp. 181–199.

[107] Friedrich Schottky. “Zur Theorie der Abelschen Functionen von vier Variabeln”. In: *J. Reine Angew. Math.* 102 (1888), pp. 304–352.

[108] I. A. Semaev. “Evaluation of Discrete Logarithms in a Group of P-torsion Points of an Elliptic Curve in Characteristic P”. In: *Math. Comput.* 67.221 (1998), pp. 353–356.

[109] Carl Ludwig Siegel. *Topics in complex function theory. Vol. III.* Wiley Classics Library. John Wiley & Sons, Inc., New York, 1989, pp. x+244.

[110] Joseph H Silverman. *The arithmetic of elliptic curves.* Vol. 106. Springer Science & Business Media, 2009.

[111] Joseph H Silverman and Katherine E Stange. “Amicable pairs and aliquot cycles for elliptic curves”. In: *Experimental Mathematics* 20.3 (2011), pp. 329–357.

[112] N. P. Smart. “The Discrete Logarithm Problem on Elliptic Curves of Trace One”. In: *Journal of Cryptology* 12.3 (1999), pp. 193–196.

[113] Andrew V. Sutherland. “Accelerating the CM method”. In: *LMS J. Comput. Math.* 15 (2012), pp. 172–204.

[114] Christopher Swierczewski and Bernard Deconinck. “Computing Riemann theta functions in Sage with applications”. In: *Mathematics and Computers in Simulation* 127 (2016). Special Issue: Nonlinear Waves: Computation and Theory-IX, pp. 263–272.

[115] Montserrat Teixidor i Bigas. “The divisor of curves with a vanishing theta-null”. In: *Compositio Math.* 66 (1988), pp. 15–22.

[116] The FPLLL development team. “fplll, a lattice reduction library”. 2016. URL: `https://github.com/fplll/fplll`.

[117] W. T. Tutte. “An algorithm for determining whether a given binary matroid is graphic”. In: *Proc. Amer. Math. Soc.* 11 (1960), pp. 905–917.

[118] Frank Vallentin. “Sphere Covering, Lattices, and Tilings (in Low Dimensions)”. PhD thesis. TU München, 2003.

[119] Pauli Virtanen et al. “SciPy 1.0: Fundamental Algorithms for Scientific Computing in Python”. In: *Nature Methods* 17 (2020), pp. 261–272.

[120] Georges Voronoi. “Nouvelles applications des paramètres continus à la théorie des formes quadratiques, Deuxième mémoire, Recherches sur les parallélloèdres primitifs.” In: *Journal für die reine und angewandte Mathematik* 134 (1908), pp. 198–287. URL: `http://eudml.org/doc/149291`.

[121] Lawrence C Washington. *Introduction to cyclotomic fields*. Vol. 83. Springer Science & Business Media, 1997.

[122] Wen Zhang, Sanzheng Qiao, and Yimin Wei. “HKZ and Minkowski Reduction Algorithms for Lattice-Reduction-Aided MIMO Detection”. In: *IEEE Transactions on Signal Processing* 60.11 (2012), pp. 5963–5976.