Computational Aspects of Jacobians of Hyperelliptic Curves

THÈSE N^{O} 7114 (2016)

PRÉSENTÉE LE 27 OCTOBRE 2016

À LA FACULTÉ INFORMATIQUE ET COMMUNICATIONS
LABORATOIRE DE CRYPTOLOGIE ALGORITHMIQUE
PROGRAMME DOCTORAL EN INFORMATIQUE ET COMMUNICATIONS

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

POUR L'OBTENTION DU GRADE DE DOCTEUR ÈS SCIENCES

PAR

Alina DUDEANU

acceptée sur proposition du jury:

Prof. O. N. A. Svensson, président du jury
Prof. A. Lenstra, Prof. D. P. Jetchev, directeurs de thèse
Dr D. Robert, rapporteur
Dr P. Gaudry, rapporteur
Prof. D. Testerman, rapporteuse

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Suisse
2016

It does not matter how slowly you go
as long as you do not stop.
— Confucius

To my dear family and friends. . .

Acknowledgements

First and foremost, I would like to thank my principal supervisor Prof. Arjen K. Lenstra for accepting me first as an intern in his Laboratory for Cryptologic Algorithms (LACAL) and afterwards, as a PhD student. By far, he is one of the most supportive persons I have ever encountered and it has been a great pleasure to be part of his group. Furthermore, I would also like to thank my second supervisor Prof. Dimitar Jetchev for continuous guidance and constructive advice in the realm of mathematics. I have worked under his guidance on the main projects of this thesis and I am really grateful for the opportunity to do so. I would also like to thank both my supervisors for their valuable and timely input on this document and other research related documents I have worked on. I am also grateful for the opportunity to attend two big conferences in cryptography, EuroCrypt 2012 and Crypto 2014, and two summer schools in 2012, CryptoBG and the Oberwolfach Seminar on Algorithms for Complex Multiplication over Finite Fields. I am also grateful for the opportunity to give a talk in 2014 at the conference Theoretical and Practical Aspects of the DLP, in Ascona and in 2015, at the seminar Special LACAL@RISC Seminar on Cryptologic Algorithms, at CWI, in Amsterdam.

A special thanks goes to Dr. Damien Robert with whom Dimitar and I have collaborated on the main topic of this thesis, namely computing cyclic isogenies in genus 2, and with whom we have had frequent and valuable discussions via Skype. I am also grateful for visiting his INRIA office in Bordeaux in May 2014 to work on our project. I would also like to thank Damien together with Dr. Pierrick Gaudry for being the external referees at my public PhD defense and for their valuable comments regarding this document. Moreover, I would like to thank Prof. Donna Testerman for being the internal referee and Prof. Ola Svensson for being the president of the jury at my private defense.

Furthermore, I would also like to thank Dr. Kristin Lauter for accepting me as a summer intern in her Cryptography group at Microsoft Research Redmond (MSR) during the summer of 2014. I would also like to thank Kristin and Prof. Bianca Viray for supervising my work on computing denominators of Igusa class polynomials that was completed during my stay in Redmond. I am also grateful for the opportunity of working with Dimitar and former PhD student at LACAL, Dr. Joppe Bos, on the Pollard rho project.

A special thanks goes to my colleagues from the math department, Dr. Hunter Brooks and PhD student Marius Vuille. With both of them I have had numerous theoretical and practical

conversations that proved to be really useful in understanding certain mathematical concepts. I am also grateful that, together with Dimitar, they have organized several valuable seminar talks in mathematics. Another special thanks goes to my former officemate of 4 years and a half, Dr. Andrea Miele, with whom I have had valuable conversations about research and life in general.

I would also like to thank all the researchers from LACAl with whom I have interacted during my entire stay here : Dr. Anja Becker, Dr. Nicolas Gama, Dr. Robert Granger, Dr. Marcelo Kaihara, Dr. Thorsten Kleinjung, Dr. Martijn Stam and Prof. Jens Zumbrägel. I would also like to thank all the current or former PhD-students : Dr. Maxime Augier, Dr. Joppe Bos, Kostic Dusan, Dr. Shahram Khazaei, Dr. Andrea Miele, Dr. Onur Özen, Dr. Juraj Sarinay and Benjamin Wesolowski. I am grateful for the various maths discussions with Thorsten and Benjamin and for attending the various research talks given at LACAL or as part of the crypto seminars organized by Anja. In addition to the valuable discussions on multiple research topics, I am grateful for all the fun activities that I took part in : watching great movies during our lunch breaks, tasting delicious homemade cakes during our birthday parties and afternoon breaks, enjoying our lab dinners, summer barbecues and even our long ago hikes. I would also like to thank the secretary of our laboratory, Monique Amhof, for her help with any administrative or personal issues.

In the end, I would like to thank my parents and brother for their love, continuous support and unshakeable belief in me. I would also like to thank my dear friend Marina Boia whom I consider as part of my family. I am grateful for the time spent together during our PhD studies, for her being the best roommate ever, a true friend and a fun travel companion. I would also like to thank Florin Dinu for being supportive and patient, especially for being so understanding during the months dedicated to writing my thesis and preparing the defense presentations. I am also grateful for the opportunity of becoming good friends with Adrian Popescu, Andrew Becker, Daniel Lupei, Dimitri Melissovas, Immanuel Trummer, Irina Prostakova, Onur Yuruten, Regis Blanc, Sergii Vozniuk, Sergiu Gaman, Valentina Sintsova. I am grateful for our conversations, our trips, swimming outings, dinners and all the other fun activities that we have enjoyed together during the years spent in Lausanne. I am looking forward to continuing our friendship even after some of us are leaving Lausanne. I am also grateful for going on hiking trips in Switzerland and Italy with Alexandre Duc and Petr Susil and visiting Croatia with Goran Radanovic as a guide. I would also like to thank my dear friends from Romania with whom I have managed to keep in touch, Andreea-Elena Ţibuleac, Camelia Smeria, Corina Chipirişteanu, Cristina Szabo, Daniela Băboi, Laura Trotuş, Monica Roman, Monica Strugaru, Paul Diac, Vlad Manea.

Abstract

Nowadays, one area of research in cryptanalysis is solving the Discrete Logarithm Problem (DLP) in finite groups whose group representation is not yet exploited. For such groups, the best one can do is using a generic method to attack the DLP, the fastest of which remains the Pollard rho algorithm with r-adding walks. For the first time, we rigorously analyze the Pollard rho method with r-adding walks and prove a complexity bound that differs from the birthday bound observed in practice by a relatively small factor.

There exist a multitude of open questions in genus 2 cryptography. In this case, the DLP is defined in large prime order subgroups of rational points that are situated on the Jacobian of a genus 2 curve defined over a large characteristic finite field. We focus on one main topic, namely we present a new efficient algorithm for computing cyclic isogenies between Jacobians. Comparing to previous work that computes non cyclic isogenies in genus 2, we need to restrict to certain cases of polarized abelian varieties with specific complex multiplication and real multiplication. The algorithm has multiple applications related to the structure of the isogeny graph in genus 2, including random self-reducibility of DLP. It helps support the widespread intuition of choosing *any* curve in a class of curves that satisfy certain public and well studied security parameters.

Another topic of interest is generating hyperelliptic curves for cryptographic applications via the CM method that is based on the numerical estimation of the rational Igusa class polynomials. A recent development relates the denominators of the Igusa class polynomials to counting ideal classes in non maximal real quadratic orders whose norm is not prime to the conductor. Besides counting, our new algorithm provides precise representations of such ideal classes for all real quadratic fields and is part of an implementation in Magma of the recent theoretic work in the literature on the topic of denominators.

Key words : the discrete logarithm problem, Pollard-rho, cyclic isogenies in genus 2, polarized abelian varieties, theta structures, CM theory, Igusa class polynomials, ideal classes in real quadratic orders.

Résumé

De nos jour, la résolution du problème du logarithme discret (PLD) dans des groupes finis où la représentation des éléments n'a pas encore été exploitée est un important domaine de recherche en cryptanalyse. Seules les méthodes génériques sont applicables à ces groupes, dont la plus rapide est l'algorithme rho de Pollard avec r-adding walks. Pour la premieère fois, nous analysons l'algorithme rho de Pollard avec r-adding walks de manière rigoureuse, et prouvons une complexité différant par un facteur relativement petit de la compléxité observée en pratique.

Il y a une multitude de questions ouvertes dans la cryptographie en genre 2. Dans ce cas-ci, le PLD est défini sur de grands sous-groupes d'ordre premiers de points rationnels sur des Jacobiennes de courbes de genre 2, définies sur des corps finis de grande caractéristique. Nous nous concentrons sur un sujet particulier, introduisant un nouvel algorithme efficace pour le calcul d'isogénies cycliques entre Jacobiennes. Par rapport aux travaux précédants sur le calcul d'isogénies non-cycliques en genre 2, nous devons nous restreindre à des variétés abéliennes principalement polarisées dont la multiplication complexe et réelle ont certaines propriétés. Cet algorithme a de multiples applications liées à la structure du graphe d'isogénies en genre 2, notamment concernant l'auto-réductibilité aléatoire du DLP. Cela contribue à soutenir l'intuition selon laquelle, du point de vue des paramètres de sécurité, le choix d'une Jacobienne particuleère importe peu dès lors que la classe d'isogénie est fixée.

Un autre sujet d'intérêt est la génération de courbes hyperelliptiques pour des applications cryptographiques via la méthode CM, qui est basée sur l'estimation numérique des polynômes rationnels d'Igusa. Un développement récent a lié les dénominateurs des polynômes d'Igusa au nombre de classes d'idéaux d'un ordre non-maximal dans un corps quadratiques réel, dont la norme n'est pas première avec l'indice de l'ordre. En plus de résoudre ce comptage, notre nouvel algorithme fournit des représentations précises de ces classes d'idéaux pour tous les corps quadratiques réels, et fait partie d'une implémentation en Magma du rćent travail théorique dans la litérature sur le sujet des dénominateurs.

Mots clefs : le problème du logarithme discret, Pollard-rho, isogénies cycliques en genre 2, variétés abéliennes polarisées, thêta structures, théorie de Multiplication Complexe, polynômes d'Igusa, classes d'idéaux d'un ordre non-maximal dans un corps quadratiques réel.

Table des matières

1 Introduction

The World Wide Web technology grants us a multitude of fascinating opportunities and one of them is access to an extensive amount of information. The data is so considerable in size, diversity and scope that users are mostly concerned with high speed data processing and communication, easy and pleasant access. Nevertheless, during the past few years, users are more and more made aware of other important aspects, mainly the need of secure private data. Users realize more and more that they are vulnerable to diverse exploits by unknown or known parties and hence, they start to request better protection and presentation of the security risks they might be subjected to. In the WWW, the classical notions of trust and personal privacy are obsolete. Instead, we require secure channels or secure communication protocols, trusted certificate authorities, long-term secure encryption to name a few.

To design reliable methods of data protection is very complex as it is dependent on a multitude of factors, related or not to the application itself. Most encryption schemes rely on some algorithm or construction that, under certain assumptions, is most probably not leaking significant data to some unauthorised party in a certain amount of time. In this context, we say that the algorithm is (sufficiently) secure against known attacks. Naturally, a security claim of this form relies heavily on the current computer architecture and its capacity for doing arithmetic operations.

Nowadays, a distinct class of algorithms are used for establishing a common key between two distinct parties. The key is next used to encrypt data transmitted on a non-trusted channel. One of the currently most deployed methods is due to Diffie and Hellman and is based on the security assumption that with the current architecture, solving the Discrete Logarithm Problem (DLP) in certain types of large finite cyclic groups requires too many resources. For the precise definition of the DLP and useful security requirements of the groups we refer to the second chapter of the thesis. In current protocols, there exists a tendency to replace the classical multiplicative groups of large characteristic finite fields with groups $\mathbf{G}$ for which currently known DLP attacks are unable to exploit specific properties of the way the elements of $\mathbf{G}$ are represented. Such groups and attacks are commonly called *generic* (see first paragraph of Section 2.2).

One of the generic attacks most used in practice is the Pollard-rho method with several distinct adding walks. The algorithm was proven to be faster in practice than the classical Pollard-rho [77, 9] whose rigorous complexity analysis was given by [38, 40]. Chapter 2 gives a rigorous analysis of the algorithm in the case of an r-adding walk defined in the context of Section 2.2.2. The assumptions of the second model are used to estimate the probability of a collision between two random walks on a certain graph. In collaboration with Joppe Bos and Dimitar Jetchev, we proved a theorem that gives an estimate on the number of steps until a (highly) probable collision between two independent Pollard-rho walks. The result presented in this chapter differs by a factor of $\sqrt{\log |\mathbf{G}|}$ from the birthday bound observed in practice, namely $\Theta(\sqrt{|\mathbf{G}|})$.

If we assume a secure environment on the current computer architecture, the hardness of the DLP in generic groups guarantees a sufficiently long life for keys established with methods like Diffie-Hellman. For cryptographic applications, an alternative to the classical multiplicative group for DLP is a large prime order group of rational points on an elliptic (genus 1) curve or on the Jacobian of a genus 2 hyperelliptic curve. If the parameters of the (hyper)elliptic curve cryptographic system are carefully chosen, the best known attack is generic. We could conclude that both curves currently offer similar levels of security. On the other hand, in the higher genus case there exist a multitude of open questions that still need to be solved. Following our work with Dimitar Jetchev and Damien Robert, the main question that we answer in this thesis is whether or not a method exists of computing cyclic isogenies between Jacobians of dimension 2 defined over a finite field. The answer is indeed positive in the context of 4.1 and the main result of chapter 4 gives such an efficient algorithm (polynomial in $\log q$) when given an isogeny kernel of order polynomial in $\log q$. To understand the theory on which the current algorithm relies, in chapter 3 we briefly review a number of known concepts with a focus on the results of Mumford[60] and Lubicz-Robert [66, 48]. More precisely, for the purpose of later chapters, we focus on the concepts of principally polarized abelian varieties with Complex Multiplication (CM) by an order in a quartic field, theta structures and isogenies between polarized abelian varieties.

Similar to the genus 1 case, there are numerous applications to cyclic isogenies. First, we mention proving the random self-reducibility of the discrete logarithm problem [36] and if possible, computing an isogeny between two random Jacobians in the same isogeny graph [20]. In the case of elliptic curves, an $\mathbf{F}_q$-isogeny graph contains all the curves over $\mathbf{F}_q$ that have the same characteristic polynomial χ_π of the Frobenius endomorphism [76]. Let $\pi \in K$ correspond to the Frobenius endomorphism. The levels of the graph are in bijection with the orders $\mathcal{O}$, such that $\mathbf{Z}[\pi] \subseteq \mathcal{O} \subseteq \mathcal{O}_K$, in the imaginary quadratic field $K = \mathbf{Q}(\pi)$ and each vertex is identified with an ideal class of some quadratic order. Each vertex is in 1-to-1 correspondence with an $\mathbf{F}_q$-isomorphism class of elliptic curves over $\mathbf{F}_q$ and each such curve has CM by $\mathcal{O}_K$. Under the GRH assumption, the work of [36] proves random self-reducibility of DLP for elliptic curves with CM by $\mathcal{O}_K$. More precisely, if there exists a deterministic algorithm that solves the DLP on a fraction of $1/\mathrm{pol}(\#\operatorname{Pic}(\mathcal{O}_K))$ isomorphism classes of elliptic curves with CM by $\mathcal{O}_K$, then there exists a randomized algorithm that solves the DLP with high probability for any $\mathbf{F}_q$-isomorphism class of curves with CM by $\mathcal{O}_K$.

In the case of genus 2 curves, the levels of the graph are indexed by orders in a quartic field instead of an imaginary quadratic field. Each vertex is identified with an ideal class in some order $\mathcal{O}$, where $\mathbf{Z}[\pi, \pi^\dagger] \subseteq \mathcal{O} \subseteq \mathcal{O}_K$ and $\pi^\dagger$ is the Rosatti involution of π. The number of vertices is equal to the class number of $\mathcal{O}$. We say that if a Jacobian A has $\mathrm{End}_{\mathbf{F}_q}(A) \simeq_{\mathbf{F}_q} \mathcal{O}$, then it has CM by $\mathcal{O}$. An isogeny of prime degree corresponds to an edge between abelian surfaces with CM by orders $\mathcal{O}$ and $\mathcal{O}'$ respectively, satisfying either $\mathcal{O} = \mathcal{O}'$ (horizontal isogenies) or $\mathcal{O} \subset \mathcal{O}'$ or $\mathcal{O}' \subset \mathcal{O}$ (vertical isogenies). Our algorithm of computing cyclic isogenies enables us to traverse the $\mathbf{F}_q$-isogeny graph when the restrictions in 4.1 hold. For instance, one such assumption is that both abelian varieties have real multiplication by the maximal order $\mathcal{O}_0$ of the quadratic field K_0 inside K. In particular, if we want to transfer the discrete logarithm problem between the source surface and the target variety of a prime degree isogeny, the discriminant of K_0 must be sufficiently small (polynomial in $\log q$). Given our algorithm for computing cyclic isogenies and assuming GRH, the random self-reducibility of DLP in genus 2 [37] proves that with high probability, any two Jacobians with CM by the maximal order $\mathcal{O}_K$ of certain quartic CM-fields K have comparable security level. We conclude that the security parameters of a cryptographic scheme based on genus 2 hyperelliptic curves depends on the choice of the Frobenius polynomial. The number of rational points on the Jacobian is equal to the value of the Frobenius polynomial evaluated at 1.

Similarly to the case of elliptic curves, we expect that the isogeny computation algorithm has other applications related to the structure of the isogeny graph in genus 2. In genus 1, the well known Schoof–Elkies–Atkin algorithm for point counting depends significantly on efficient computation of cyclic isogenies of small degree. In the case of genus 2, the best point counting algorithm of [23] for Jacobians requires instead fast real multiplication. If we also consider a possible extension of the cyclic isogeny algorithm to genus 3, an application is the transfer of the DLP from a given hyperelliptic curve to some non-hyperelliptic curve. The non-hyperelliptic curves are suspected to be less secure as a solution can be found currently in significant less time [14].

For cryptographic purposes, the number of rational points is chosen to be equal or to differ from a large prime number Q by really small factors. Starting from Q or from a suitable Frobenius polynomial, an algorithm of generating curves over a large characteristic field $\mathbf{F}_q$ is the CM method [80]. If we assume that the class number of the real quadratic field inside K is 1 and that, as a Galois extension, K is cyclic over $\mathbf{Q}$ (or in other words, all abelian varieties with real multiplication by $\mathcal{O}_0$ are principally polarizable and simple), one type of CM method requires a numerical estimation of three rational polynomials called Igusa polynomials. A triple (i_1, i_2, i_3) that contains a root of each Igusa polynomial is next tested whether it determines or not a genus 2 curve over $\mathbf{F}_q$ whose Jacobian has the right number of points.

A rich area of research is dedicated to generating the Igusa class polynomials when given the quartic field K [74]. Similarly to the case of elliptic curves, there are three main methods of computing the Igusa class polynomials of K, the p-adic method, the Chinese Remainder Theorem (CRT) method and the complex approximation method. To compute the Igusa class polynomials given the estimates of its complex roots as in [74, §II.10], it is necessary to give close bounds or precise values of the prime powers in the denominators of the polynomials [24, 46, 45]. Recent work related the prime powers in the denominators to counting certain ideals in non-maximal orders in real quadratic fields [44]. The main result of chapter 5 is done in colaboration with Kristin Lauter and Binca Viray. It proves that the ideals are of a certain form and so, there exists a precise number of such ideals. In addition, we also propose an implementation in Magma (to be made public) that computes the ideals of this form. The implementation is used as part of an algorithm implementation that follows [44] and outputs the precise ℓ-valuation of the intersection number for most primes ℓ or a tight upper bound in the other cases.

The present thesis focuses on the mathematical aspect of security systems of interest, aiming to improve the understanding of their theoretic properties. The findings presented contribute to the confidence we may have in the mathematical soundness of actual cryptographic systems that have been proposed and that may soon become mainstream.

2 Complexity Analysis of the Additive Pollard's Rho

2.1 Introduction

The results presented in this chapter were done in collaboration with Joppe Bos and Dimitar Jetchev and published in [7].

Let $\mathbf{G}$ be a finite cyclic group of prime order and let $g \in \mathbf{G}$ be a generator. Given an element $h \in \mathbf{G}$, the *discrete logarithm problem* (DLP) is the problem of computing an integer y such that $h = g^y$. This problem is *believed* to be hard for certain groups of points on elliptic curves over a finite field but can be solved in subexponential time for multiplicative groups of finite fields [1] and for Jacobians of hyperelliptic curves of high genus [2, 3, 18, 21, 31, 15]. For this reason, the *elliptic curve discrete logarithm problem* (ECDLP) is used as the theoretical foundation of many standardized protocols used in elliptic curve cryptography [42, 54].

The parallelized [78] Pollard rho algorithm [64] is one of the most commonly used methods for solving the discrete logarithm problem when $\mathbf{G}$ is a generic finite cyclic group. The basic idea is to define a *walk* over the elements of the group $\mathbf{G}$ using an iteration function. One might solve the DLP when a group element is encountered twice (such an event is commonly referred to as a *collision*). If one assumes that the elements from the walk generated by this iteration function are independent and uniformly random among all elements of $\mathbf{G}$, the birthday paradox implies that one can obtain a collision with probability greater than 50% after $\mathcal{O}(\sqrt{|\mathbf{G}|})$ steps and with high probability after $\mathcal{O}(\sqrt{|\mathbf{G}| \log |\mathbf{G}|})$ steps [30, 19]. Here, *with high probability* means that the probability of success is $1 - \mathcal{O}(|\mathbf{G}|^{-c})$ for some $c > 0$ that does not depend on $|\mathbf{G}|$.

Obviously, the assumption that the points generated by the Pollard rho iteration function are independent and uniformly at random among all elements of $\mathbf{G}$ is incorrect (see Section 2.2 for more details). This has motivated a line of research to *rigorously* prove the desired bound of $\mathcal{O}(\sqrt{|\mathbf{G}|})$ matching the lower bound for solving discrete logarithms for generic algorithms in prime order groups that was given by Shoup [72] (in the black-box model). This is an active area demonstrated by the fact that the run time of another generic method to solve the DLP, the Pollard kangaroo method [64, 65], has been rigorously proven correct [58]. The rigorous proof for the Pollard rho method was established using Markov chains by Kim, Montenegro, Peres and Tetali in 2008 [38, 40] improving on previous attempts [52, 39].

Unfortunately, the proof presented in [38, 40] works only for the original iteration function used by Pollard in [64]. In practice, however, the so-called additive walks are preferred and hence, our proof is useful for studying the complexity of deployed algorithms. The additive walks as studied by Teske [77] are used to solve instances of the DLP (see e.g., the methods described in [29, 11, 8] for solving the discrete logarithm problem for elliptic curves). A property from the original Pollard rho iteration function that is not present in these additive walks is crucial for establishing rapid mixing results for random walks in the proof by Kim et al.

As far as we know, this work is the first attempt to rigorously prove the run time of the additive Pollard rho method. It is well-known from experimental data [77, 9] and heuristic arguments [4, Appendix B] that by increasing the number of components of the partition used for the additive walk, the performance of the iteration function better resembles the behavior of a truly random walk. We use a model introduced by Greenhalgh [26] and extended by Hildebrand [33, Thm.2] where the number of components used to partition the iteration function depends logarithmically on the cardinality of the group $\mathbf{G}$. This is in agreement with the intuition that one should use more components when larger instances of the DLP are being solved. Using this idea together with results about estimating mixing times for random walks on additive groups due to Dou and Hildebrand [32, 16], we prove a collision bound of $\mathcal{O}(\sqrt{|\mathbf{G}| \log |\mathbf{G}|})$ with probability greater than 50% and a collision bound of $\mathcal{O}(\sqrt{|\mathbf{G}|} \log |\mathbf{G}|)$ with high probability (see Corollary 2.3.2). Hence, we are short by a factor of $\sqrt{\log |\mathbf{G}|}$ from the birthday bound for both the case of 50% probability of success and the case of high probability of success.

This chapter is organized as follows: Section 2.2 states the preliminaries related to Pollard rho and motivates our work. In Section 2.3, we explain why the recent methods of Kim et al. [38, 40] are not applicable in any obvious way to the setting of the additive Pollard rho algorithm. In Section 2.4, we recall some basics on random walks on groups, convolutions of functions from Fourier analysis and their links to the distributions of end-points of random walks. Section 2.5 is devoted to the proof of our main theorem.

2.2 Preliminaries and Motivation

2.2.1 The Classical Pollard Rho Method

Throughout, we use multiplicative notation for the group $\mathbf{G}$ of prime order N. The Pollard rho algorithm, originally proposed as an integer factorization method [63], was later modified to obtain one of the most commonly used methods for solving the *discrete logarithm problem* when $\mathbf{G}$ is a generic finite cyclic group [64]. In this context, *generic* means that the application of the algorithm is independent of the representation of the group elements, i.e., the algorithm works for any representation as long as the group operation and the operation of testing equality of two group elements are both efficient.

The original Pollard rho method works as follows: partition the group $\mathbf{G}$ into three sets S_1, S_2 and S_3 of roughly the same size, pick a random element $v_0 \in [0, |\mathbf{G}|-1]$, compute $x_0 = g^{v_0} \in \mathbf{G}$ and for $i \geq 0$ let $x_{i+1} = f(x_i)$ where $f \colon \mathbf{G} \to \mathbf{G}$ is defined as follows:

$$f(x) = \begin{cases} gx & \text{if } x \in S_1, \\ hx & \text{if } x \in S_2, \\ x^2 & \text{if } x \in S_3. \end{cases}$$

The sequence $\{x_i\}_{i\geq 0}$ represents a walk on $\mathbf{G}$ that will eventually enter a cycle, i.e., there will be integers $m > n$ such that $x_m = x_n$ (we say that we have obtained a collision). Since each x_n is of the form $g^{u_n}h^{v_n}$ for some known $u_n, v_n \in \mathbf{Z}$, we obtain $u_m + yv_m \equiv u_n + yv_n \bmod N$, i.e., unless $v_m \equiv v_n \bmod N$, the solution of the discrete logarithm problem is $y = \dfrac{u_n - u_m}{v_m - v_n} \bmod N$. Using standard cycle-detection algorithms, such as Floyd's cycle finding method [41, Ex. 3.1.6], the above method requires to store a constant number of group elements. If one makes the heuristic assumption that the subsequent elements of the Pollard rho walk are independent and uniformly random, one would get (by using the birthday bound) that it takes $\mathcal{O}(\sqrt{|\mathbf{G}|})$ steps in order to obtain a collision with probability greater than 50%.

2.2.2 Complexity Analysis

Regardless of the simplicity of the above method, a mathematically rigorous run time analysis is a rather subtle question of probability theory and statistics. There are two separate stages for analyzing the complexity of solving the discrete logarithm problem via Pollard rho: 1) one needs upper bounds for the number of steps required to obtain a collision in the Pollard rho walk; 2) one needs to estimate the probability of the collision being degenerate. In this chapter, we only restrict to 1) and only note that 2) has been carried out rigorously for the classical version of the algorithm in [53].

Regarding 1), we start with the following heuristic argument: if one makes the false assumption that the elements $x_0, x_1, \ldots$ (up to the first step when a collision is obtained) are independent and uniformly random among all elements of $\mathbf{G}$, the birthday paradox would imply that one can reach a collision with probability greater than 50% after $\mathcal{O}(\sqrt{|\mathbf{G}|})$ steps and with high probability after $\mathcal{O}(\sqrt{|\mathbf{G}| \log |\mathbf{G}|})$ steps [30, 19]. The elements $x_0, x_1, \ldots$ are, however, far from being independent and uniformly random as they are constructed using the random initial point, the iteration function f and the partitioning $\mathbf{G} = S_1 \sqcup S_2 \sqcup S_3$. The obvious goal is to rigorously prove the birthday bound $\mathcal{O}(\sqrt{|\mathbf{G}|})$ that is observed in practice.

The function f in the original Pollard rho algorithm is fixed. As far as choosing the partition $\mathbf{G} = S_1 \sqcup S_2 \sqcup S_3$ is concerned, we can view it as being given by a function $\ell \colon \mathbf{G} \to \{1, 2, 3\}$.

The number of steps it takes to obtain a collision depends on the choice of the function ℓ. It is clear that for certain (degenerate) choices, this number can be quite large (e.g., if $S_1 = \mathbf{G}$ and $S_2 = S_3 = \emptyset$ then it can take as many as $|\mathbf{G}|$ steps to obtain a collision). What one could hope for is that for a random choice of ℓ (selected among some prescribed distribution on the set of all such functions), the collision time will be what we expect (namely, $\mathcal{O}(\sqrt{|\mathbf{G}|})$). If we consider the steps of the Pollard rho walk as random variables $X_0, X_1, \ldots$, the collision time T will then be a stopping time random variable where the randomness is determined by the choice of ℓ as well as by the random choice of the initial element. One could then try to show that with high probability, $T = \mathcal{O}(\sqrt{|\mathbf{G}|})$. We refer to this probabilistic model as **Model 1**. It is clear that the values of $X_1, \ldots, X_n, \ldots$ are completely determined by the choices of X_0 and ℓ. Unfortunately, it is not known how to analyze the statistical behavior of Model 1. A common approach to remedy this problem is to use pseudo-random walks in order to approximate (statistically) the random variables X_i with other random variables that are easier to work with. The idea is that X_{n+1} can be modeled as being computed from X_n by using (with probability 1/3) a random transition out of the three different transition steps. This gives us the model of a random walk on the so-called Pollard rho graph (a 4-regular graph whose vertices are the elements of $\mathbf{G}$ and whose edges are determined by the transition steps). Of course, once we obtain a collision, the walk should no longer be random, but deterministic. We refer to this approximation model as **Model 2**. In this case (for the classical Pollard rho), one can show that with probability more than 50% (or, more generally, with any probability that is independent of $|\mathbf{G}|$), a collision occurs after $\mathcal{O}(\sqrt{|\mathbf{G}|})$ steps. In fact, this was not known until recently: the desired bound of $\mathcal{O}(\sqrt{|\mathbf{G}|})$ was rigorously established using Markov chains by Kim, Montenegro, Peres and Tetali in 2008 [38, 40] improving on [52, 39]. The argument relies on establishing rapid mixing results for random walks in the Pollard rho graph where the squaring step plays a crucial role (see Section 2.3.1 for more details). Yet, currently nothing is known about how well Model 2 approximates Model 1 or vice versa.

2.2.3 Additive Pollard Rho Method

When trying to solve an elliptic curve discrete logarithm problem in practice, the squaring step is often avoided because it is relatively inefficient. Instead, a small integer r is chosen and an r-tuple $(s_1, \ldots, s_r)$ of group elements (transition steps) is precomputed. Given a new partition function $\ell \colon \mathbf{G} \to \{1, 2, \ldots, r\}$, one uses the transition function $f(x) = x + s_{\ell(x)}$ instead of the function defined in the original Pollard rho method. This gives rise to a variation of Pollard rho that uses no squaring steps. These walks are known as r-adding walks [77].

The theoretical question studied in this chapter is relevant as it is the first attempt to provide a rigorous analysis of the variation of Pollard rho that is most commonly used nowadays. In practice, when solving the discrete logarithm problem, one uses a parallel version of Pollard rho [78]. This leads to an m-fold speedup when the workload is shared among m computational units. The main cost of the Pollard rho method is computing the iteration function f. Computing a single step in the Pollard rho walk (a single iteration of f), is equivalent to computing the group operation in $\mathbf{G}$. In the setting of elliptic curves where we use the additive notation for the group operation, this operation is either a point doubling or a point addition.

Montgomery's *simultaneous inversion* method is often used to speed up Pollard rho [59]. When processing m independent walks in the parallel version of the algorithm, the simultaneous inversion method allows one to substitute m inversions by $3m-3$ multiplications and a single inversion. When used in combination with affine Weierstrass coordinates, this results in an average cost (ignoring modular additions and subtractions) of s squarings, $2+\dfrac{3m-3}{m}$ multiplications and $\dfrac{1}{m}$ inversions to implement the group operation for a single walk where $s=1$ and $s=2$ for elliptic curve addition and point doubling, respectively. This makes affine Weierstrass coordinates the preferred point representation for this type of application and shows that from a performance perspective, point doublings are to be avoided.

2.3 Runtime Analysis for r-adding Walks

Analyzing Model 1 is out of reach even in the setting of the classical Pollard rho method. We thus restrict ourselves to Model 2 in the setting of the Pollard rho method using r-adding walks.

2.3.1 Classical Pollard Rho and Block Walks

The method of Kim, Montenegro, Peres and Tetali [38, 40] applies to the classical version of Pollard rho that uses three transition steps, one of which is the squaring step and the other two are multiplications by g and h, respectively. Under Model 2, this is achieved by choosing transition steps uniformly at random among the three until a collision has been obtained. Under this model, it is shown that a collision is obtained in $\mathcal{O}(\sqrt{|\mathbf{G}|})$ steps. The key observation is the fact that one can split the pseudo-random walk into blocks using the squaring steps of the walk as a separating move. More precisely, if one represents the walk by the random variables $X_i = g^{Y_i}$ for unique Y_i-s in $[0, |\mathbf{G}|-1]$ then one defines a new sequence of random variables $\{T_i\}$ as follows: let $T_0 = 1$ and let T_1 be the first step when the walk makes a squaring transition. More generally, let T_i be the first step after T_{i-1} when the walk makes a squaring transition. Let $b_i = Y_{T_i-1} - Y_{T_{i-1}}$ be the contribution from the ith block (this is the part of the original walk covered by addition steps only). The block walk is then defined as the random process $Z_s = Y_{T_s} = 2^s Y_{T_0} + 2\sum_{i=1}^{s} 2^{s-i} b_i$. One can estimate the probability $B^s(u,v)$ of reaching a vertex v starting from a vertex u via a pseudo-random walk consisting of exactly s blocks (as opposed to a fixed number of steps). More precisely, assuming that $Z_0 = u$, the probability that $Z_s = v$ is $B^s(u,v)$. Obtaining good upper and lower bounds for these probability is possible for the following two reasons: if S is the set of blocks for which $b_i = 0$ or 1, i.e., the blocks of zero steps (two consecutive squarings), and the blocks of one multiplication-by-g step (a squaring followed by multiplication by g followed by another squaring) then one can separate the total contribution from these special blocks and conditions on the total contribution of the remaining blocks. Calculating this conditional probability amounts to calculating the probability of a given integer w being represented as $w = \sum_{i=1}^{s} 2^{s-i} b_i$ where $b_i = 0$ or 1. Using the uniqueness of the binary representation of w, one can determine uniquely the contribution of each block from the set S and thus, establish strong upper bounds on this conditional probability. This allows to deduce (via Plancherel's formula from Fourier analysis and the fact that the contributions b_i of the blocks are independent when considered as random variables) that $B^s(u,v)$ is close to uniform for s that is polylogarithmic in $\log|\mathbf{G}|$ which shows rapid mixing for the block walk. In this argument, the squaring step plays a key role.

It is difficult to generalize the block-walk method of [38, 40] in the additive Pollard rho setting since we have no natural choice for the separating move (as is the squaring step in the classical Pollard rho). Even if one declares one of the existing steps as separating, one still has no analogue of the uniqueness of the binary expansion. One can work harder and estimate the number of representations of w as a combination of the remaining (non-separating) steps, but eventually, we were unable to obtain an asymptotically useful bound. From that point of view, the problem of analyzing Pollard rho equipped with r-adding walks looks harder than analyzing the original Pollard rho using a mixed walk. Before stating the main result, we make two separate comments that will motivate the precise formulation chosen for the complexity analysis.

2.3.2 Randomization over the Addition Steps

Suppose that one is interested in analyzing the case of Pollard rho for additive walks. One then loses the important property that the squaring step contributes to the rapid mixing properties of the Pollard rho walk. When no squaring is used, there exist special cases in which it might take as many as $|\mathbf{G}|$ steps for the walk to even reach a certain element of the group.

To make this precise, note that each choice of the r-tuple $(s_1, \ldots, s_r)$ of transition elements gives rise to a stopping time random variable $T_{s_1,\ldots,s_r}$, namely, the first time when a collision is obtained in the walk. More precisely, let

$$T_{s_1,\ldots,s_r} = \min\left\{j > 0 \colon \exists i < j \text{ such that } X_i = X_j\right\},$$

where $(s_1, \ldots, s_r)$ are the transition steps in the Pollard rho walk.

Here, the distribution of $T_{s_1,\ldots,s_r}$ depends on the source of randomness for the Pollard rho walk. For Model 1, this source is the choice of a random partition of $\mathbf{G}$ into r disjoint sets whereas for Model 2, it is the random choice of a transition element at each step in the walk. In either case, we are interested in showing that $T_{s_1,\ldots,s_r}$ is bounded by some appropriate upper bound with either probability at least 50% (or any fixed probability, independent of $|\mathbf{G}|$) or with high probability (i.e., probability $1 - \mathcal{O}(|\mathbf{G}|^{-c})$ for some $c > 0$) over the desired source of randomness. For instance, one might want to show that $T_{s_1,\ldots,s_r}$ is less than a constant times $\sqrt{|\mathbf{G}|}$ with probability more than 50% for an r-tuple $(s_1, \ldots, s_r)$ of transition steps. Yet, in the r-adding walk case, it is unreasonable to expect such a result to hold for a fixed r-tuple $(s_1, \dots, s_r)$ as there might be very degenerate choices that do not even allow one to reach every element of the group $\mathbf{G}$ in $\mathcal{O}(\sqrt{|\mathbf{G}|})$ steps. For instance, consider $\mathbf{G} = (\mathbf{Z}/N\mathbf{Z}, +)$ for some integer $N > 0$ and suppose that $r = \mathcal{O}(\log N)$. Consider the transition elements $s_i = i \bmod N$ for $i = 1, \dots, r$. It is clear that if the walk starts at the zero element, it cannot reach the element $N - 1 \bmod N$ in time less than $N/\log N$. This degeneracy leads to a poor mixing time for the Pollard rho walk for this particular choice of steps. One way to remedy this issue is to establish the expected upper bound on the stopping time $T_{s_1,\dots,s_r}$ with high probability over the random choice of the transition elements $(s_1, \dots, s_r)$ as well as over the source of randomness of Model 2.

2.3.3 Dependency on r

One expects that by increasing the size of the set of precomputed points that can be added to the current point in the iteration function results in a pseudo-random walk behaving more like a truly random walk. This was experimentally shown to be true by Teske [77] and is made more precise by Bernstein et al. who showed, using a heuristic argument [4, Appendix B] refining the analysis from [10], that the expected number of steps to reach a collision when using an r-adding walk is $\sqrt{\dfrac{\pi|\mathbf{G}|}{2\left(1 - \sum_{j=1}^{r} p_j^2\right)}}$ where typically $p_j \approx \dfrac{1}{r}$ (see also [5]). Hence, the use of an r-adding walk results in a bound that is larger than the birthday bound $\sqrt{\dfrac{\pi|\mathbf{G}|}{2}}$ by a factor of $\sqrt{\dfrac{r}{r-1}}$, so the larger r is, the closer the expected bound is to the birthday bound. This argument is extended in [9] when using mixed walks (walks that have both multiplication and squaring steps). The expected number of steps for reaching a collision is then $\sqrt{\dfrac{\pi|\mathbf{G}|}{2(1 - p_D^2 - \sum_{j=1}^{r} p_j^2)}}$ where $p_D = 1 - \sum\limits_{i=1}^{r} p_i$ is the probability of choosing a squaring step. It follows from this result that for instance, the original mixed walk used by Pollard is expected to differ from the birthday bound by a factor of $\sqrt{3/2} \approx 1.22$.

A major question is then how r should depend on $|\mathbf{G}|$. Assuming that r does not depend on $|\mathbf{G}|$, we note that an argument of Greenhalgh [26] as extended by Hildebrand [33, Thm.2] (see also Theorem 2.4.4) establishes lower bounds on the mixing time that are exponential (in $\log|\mathbf{G}|$) as opposed to mixing times that are polynomial (in $\log|\mathbf{G}|$) in the case when r depends logarithmically on $|\mathbf{G}|$ (see Theorem 2.4.2). One would then expect that in the case when the mixing time is poor, the number of steps to achieve a collision must be far from the birthday bound. We thus allow r to depend logarithmically on $|\mathbf{G}|$.

2.3.4 Main Theorem

Similarly to the case of the classical Pollard rho algorithm with three transitions, proving anything under Model 1 seems hopeless. Our main theorem shows that such a result for r-adding walks can however be shown under Model 2 with an asymptotic upper bound $\sqrt{|\mathbf{G}| \log |\mathbf{G}|}$ on the number of steps (with probability greater than 50%).

Theorem 2.3.1. *Let $a > 1$, $\delta > 0$ and $\gamma > 0$ be real numbers. There exists $n_0 \geq 0$ with the following property: if $\mathbf{G}$ is a finite cyclic group of prime order $|\mathbf{G}| \geq n_0$ and $\kappa > 1$ is a real number then*

$$\Pr_{\substack{s_1,\ldots,s_r \\ \textit{random walk}}} \left[T_{s_1,\ldots,s_r} \leq \sqrt{\frac{(2+\delta)\kappa}{e} |\mathbf{G}| \log |\mathbf{G}|} \right] \geq 1 - e^{-\kappa} - \frac{1}{|\mathbf{G}|^{\gamma}},$$

where $r = \lfloor (\log |\mathbf{G}|)^a \rfloor$ and e is the Euler's number $2.7828\ldots$.. Here, the probability is taken over a uniformly random choice of an r-tuple $(s_1, \ldots, s_r)$ of distinct elements of $\mathbf{G}$ and over the randomness of Model 2.

The implications of this theorem are stated in the following corollary.

Corollary 2.3.2. *Let $a > 1$ be a real number. If $\mathbf{G}$ is a finite group that is cyclic of prime order and if $r = \lfloor (\log |\mathbf{G}|)^a \rfloor$ then solving the discrete logarithm problem with the Pollard rho method using an r-adding walk requires*

- *(i) $\mathcal{O}(\sqrt{|\mathbf{G}| \log |\mathbf{G}|})$ steps with probability ≥ 0.5 as $|\mathbf{G}| \to \infty$,*
- *(ii) $\mathcal{O}(\sqrt{|\mathbf{G}|} \log |\mathbf{G}|)$ steps with high probability, i.e., if $\gamma > 0$ is any fixed real number (independent of $|\mathbf{G}|$) then the probability of not finding a collision in $\mathcal{O}(\sqrt{|\mathbf{G}|} \log |\mathbf{G}|)$ steps is bounded by $\mathcal{O}(|\mathbf{G}|^{-\gamma})$ as $|\mathbf{G}| \to \infty$,*

where the probability is over the choice of uniformly random r-tuple $(s_1, \ldots, s_r)$ of distinct elements of $|\mathbf{G}|$ and the randomness in Model 2.

Proof. This follows immediately from Theorem 2.3.1 when we fix a constant $\gamma > 0$ and consider $\kappa = \log \frac{2|\mathbf{G}|^{\gamma}}{|\mathbf{G}|^{\gamma} - 1}$ for the first part and $\kappa = \gamma \log |\mathbf{G}|$ for the second part. □

To prove the theorem, we first need mixing time estimates for random walks on the group $\mathbf{G}$. Such estimates over a random choice of r independent adding steps were established by Dou and Hildebrand [32, 16]. The idea then is the following: given the mixing time τ (i.e., the number of steps needed to make the end point of the walk look uniformly random), we make t_0 initial steps and then τ additional steps. Since τ is a mixing time, the probability of the end point of the walk being any of the t_0 initial points is $\frac{t_0}{|\mathbf{G}|}$, i.e., the probability of failing to produce a collision at this step should be bounded by $1 - \frac{t_0}{|\mathbf{G}|}$. If no collision has occurred, we perform another τ steps and calculate the probability of failure. We continue until the probability of failure becomes less than $e^{-\kappa}$. Suppose we have done s such iterations (performing τ steps s times after the original t_0 steps). We then need to minimize the total number $t_0 + \tau s$ of steps subject to the constraint that the failure probability is smaller than $e^{-\kappa}$. By solving this optimization problem, we see that it takes $\mathcal{O}(\sqrt{|\mathbf{G}| \log |\mathbf{G}|})$ steps to produce a collision with probability at least $1 - e^{-\kappa}$.

2.4 Random Walks on Groups and Mixing Times

Let $\mathbf{G}$ be a finite abelian group, let P be a probability distribution on $\mathbf{G}$ and let U be the uniform distribution on $\mathbf{G}$. Following [32], we define the statistical distance between the probability distribution P and the uniform distribution U as

$$\|P - U\| := \frac{1}{2} \sum_{s \in \mathbf{G}} \left| P(s) - \frac{1}{|\mathbf{G}|} \right|.$$

Given two real-valued functions $f\colon \mathbf{G} \to \mathbf{R}$ and $g\colon \mathbf{G} \to \mathbf{R}$, we define their convolution as

$$(f \star g)(x) := \sum_{y \in \mathbf{G}} f(xy^{-1}) g(y).$$

As the convolution is associative, the m-fold convolution $f \star \cdots \star f$ is well-defined and we denote it by $f^{\star m}$. Let r be a positive integer (that may or may not depend on $|\mathbf{G}|$) and let $s_1, \ldots, s_r \in \mathbf{G}$ be a sequence of r distinct elements of $\mathbf{G}$ (we refer to these elements as the transition steps). Let $p_1, \ldots, p_r$ be a set of non-negative real numbers such that $\sum_{i=1}^{r} p_i = 1$ (we refer to these numbers as transition probabilities). Let $P_{s_1,\ldots,s_r}$ be the distribution defined by:

$$P_{s_1,\ldots,s_r}(s) := \begin{cases} p_i & \text{if } s = s_i \text{ for some } i = 1, \ldots, r, \\ 0 & \text{otherwise.} \end{cases}$$

In the case of the r-adding walk version of Pollard rho under Model 2, we take $p_i = 1/r$ for every $i = 1, \ldots, r$. Note that $P^{\star m}_{s_1,\ldots,s_r}$ is the distribution of the end point of an m-step random walk starting from the identity element of the group $\mathbf{G}$ (this follows, e.g., by induction on m).

Definition 2.4.1. Given $\epsilon > 0$ and a sequence $s_1, \ldots, s_r$ of transition steps, we define the ϵ-mixing time $\tau_{s_1,\ldots,s_r}(\epsilon)$ with respect to that sequence to be the smallest integer m such that $\|P^{\star m}_{s_1,\ldots,s_r} - U\| < \epsilon$.

Remark 1. Using the fact that $s_1, \ldots, s_r$ generate $\mathbf{G}$ (since $\mathbf{G}$ is of prime order), using spectral analysis of the adjacency matrices of the Cayley graph constructed from $\{s_1, \ldots, s_r\}$, one can show that the mixing time $\tau_{s_1,\ldots,s_r}(\epsilon)$ is well-defined.

Remark 2. We cannot find a reasonable bound for $\tau_{s_1,\ldots,s_r}(\epsilon)$ for every r-tuple $(s_1, \ldots, s_r)$ of transition steps. Yet, for a uniformly random r-tuple among all $\frac{|\mathbf{G}|!}{(|\mathbf{G}| - r)!}$ r-tuples of distinct elements of $\mathbf{G}$, one could expect a reasonable upper bound. This can be formalized using Markov's inequality as well as bounds on the expectation of the statistical difference between the distribution of the end-point of the mth step of the random walk and the uniform distribution (due to Hildebrand). This is indeed the approach that we take.

The next theorem shows that if we allow polylogarithmic dependence of r on $|\mathbf{G}|$ then one does indeed get a polynomial (in $\log|\mathbf{G}|$) mixing time.

Theorem 2.4.2. *[16, Thm. 1] Let $r = \lfloor (\log|\mathbf{G}|)^a \rfloor$ for some constant $a > 1$ and let $\epsilon' > 0$ be given. Suppose that $m > \dfrac{a}{a-1}\dfrac{\log|\mathbf{G}|}{\log r}(1+\epsilon')$. Then*

$$\mathcal{E}_{s_1,\ldots,s_r}[\|P^{*m}_{s_1,\ldots,s_r} - U\|] \to 0 \text{ as } |\mathbf{G}| \to \infty,$$

where the probability is taken over a uniformly random r-tuple $(s_1, \ldots, s_r)$ of distinct elements of $\mathbf{G}$.

Remark 3. For our particular application, the version stated above is not sufficient as it does not quantify the rate of convergence of the expectation as $|\mathbf{G}| \to \infty$. Yet, we should point out that such a quantification is implicit in the proof by Dou and Hildebrand. We state and prove an effective version in the next section and apply this version to obtain upper bounds on the mixing time $\tau_{s_1,\ldots,s_r}(\epsilon)$ that holds with high probability over the choice of the r-tuple $(s_1, \ldots, s_r)$.

Remark 4. We note that Hildebrand's bound is optimal in the following sense: it is shown in [32, Thm.3] that if $r = \lfloor (\log|\mathbf{G}|)^a \rfloor$ for some constant $a < 1$ then for any fixed positive real number b, the distance $\|P^{*m}_{s_1,\ldots,s_r} - U\| \to 1$ as $|\mathbf{G}| \to \infty$ for $m = \lfloor (\log|\mathbf{G}|)^b \rfloor$ and any choice $s_1, \ldots, s_r \in \mathbf{G}$ of transition steps.

Finally, we note that if r is independent of $|\mathbf{G}|$ then the mixing time becomes exponential as shown by the following two theorems establishing upper and lower bounds, respectively.

Theorem 2.4.3. *[32, Thm.1] Suppose that $r \geq 2$ is a fixed positive integer and let $p_1, \ldots, p_r$ be fixed transition probabilities as above. Given $\epsilon > 0$, there exists a constant γ that depends on r, ϵ and the p_i's, but not on $|\mathbf{G}|$ such that*

$$\mathcal{E}_{s_1,\ldots,s_r}[\|P^{*m}_{s_1,\ldots,s_r} - U\|] < \epsilon$$

for $m = \lfloor \gamma|\mathbf{G}|^{\frac{2}{r-1}} \rfloor$ where the expectation is taken over a uniformly random r-tuple $(s_1, \ldots, s_r)$ of distinct elements of $\mathbf{G}$.

Theorem 2.4.4. *[33, Thm.2] Let r be constant (independent of $|\mathbf{G}|$) and let $p_i = 1/r$ for $i = 1, \ldots, r$. Let $\delta < \dfrac{1}{2}$ be fixed. There exists a value $\gamma > 0$ (independent of $|\mathbf{G}|$) such that if $m < \gamma|\mathbf{G}|^{\frac{2}{r-1}}$ then $\|P^{*m}_{s_1,\ldots,s_r} - U\| > \delta$ for any r-tuple $(s_1, \ldots, s_r)$ of distinct elements of $\mathbf{G}$.*

2.4.1 Upper Bounds on Mixing Times

The mixing time $\tau_{s_1,\ldots,s_r}(\epsilon)$ can get as large as $|\mathbf{G}|$ for certain degenerate r-tuples $(s_1,\ldots,s_r)$ of transition steps. We thus need a way to show that with high probability over a randomly chosen r-tuple $(s_1,\ldots,s_r)$ of distinct elements of $\mathbf{G}$, the mixing time can be bounded by a sufficiently strong upper bound. The following definition is helpful in order to make this rigorous:

Definition 2.4.5. Let $\epsilon > 0$ be a real number and let m be a positive integer. We say that an r-tuple $(s_1,\ldots,s_r)$ of distinct elements of $\mathbf{G}$ is (ϵ, m)**-faulty** if $\|P^{\star m}_{s_1,\ldots,s_r} - U\| > \epsilon$ or equivalently, if $\tau_{s_1,\ldots,s_r}(\epsilon) > m$.

Using the work of Dou and Hildebrand [16] and Markov's inequality, one can prove the following:

Lemma 2.4.6. *Let $a > 1$ be any real number and let ϵ' be a real number that satisfies $0 < \epsilon' < \frac{(a-1)}{e}\log\log|\mathbf{G}| - 1$. Let $r = \lfloor(\log|\mathbf{G}|)^a\rfloor$ and let $m = \left\lceil \frac{\log|\mathbf{G}|}{(a-1)\log\log|\mathbf{G}|}(1+\epsilon')\right\rceil$. There exists $n'_0 > 0$ such that if $|\mathbf{G}| \geq n'_0$ then for any $\epsilon > 0$, we have*

$$\Pr_{s_1,\ldots,s_r}[(s_1,\ldots,s_r) \textit{ is } (\epsilon,m)\textit{-faulty}] = \Pr_{s_1,\ldots,s_r}[\|P^{\star m}_{s_1,\ldots,s_r} - U\| > \epsilon] < \frac{3}{4\epsilon^2|\mathbf{G}|^{\epsilon'}},$$

where the probability is taken over a uniformly random r-tuple $(s_1,\ldots,s_r)$ of distinct elements of $\mathbf{G}$.

Proof. We follow the proof of [16, Theorem 1]. Throughout, we omit the explicit reference to the floor and ceiling notation, this does not affect any of the conclusions. It is shown in [16, p. 996] that

$$\mathcal{E}_{s_1,\ldots,s_r}[\|P^{\star m}_{s_1,\ldots,s_r} - U\|^2] \leq \frac{3}{4}\frac{|\mathbf{G}|(em)^m}{r^m}, \tag{2.1}$$

whenever $|\mathbf{G}|$ is sufficiently large, i.e., whenever $|\mathbf{G}| \geq n'_0$ for some $n'_0 > 0$. Letting $d = \frac{a}{a-1}\frac{1+\epsilon'}{\log r} = \frac{1+\epsilon'}{(a-1)\log\log|\mathbf{G}|}$, note that $(em)^m = |\mathbf{G}|^{d(\log d+1)}$ and $r^m = e^{m(a-1)\log\log|\mathbf{G}|}$. The right side of the inequality (2.1) becomes:

$$\frac{3|\mathbf{G}|(em)^m}{4r^m} = \frac{3e^{\log|\mathbf{G}|}|\mathbf{G}|^{d(\log d+1)}}{4e^{m(a-1)\log\log|\mathbf{G}|}} = \frac{3}{4}|\mathbf{G}|^{-\epsilon'+d(\log d+1)}.$$

If $\epsilon' < \frac{(a-1)\log\log|\mathbf{G}|}{e} - 1$ then $\log d < -1$, hence, $d(\log d+1) < 0$ and inequality (2.1) then implies

$$\mathcal{E}_{s_1,\ldots,s_r}[\|P^{\star m}_{s_1,\ldots,s_r} - U\|^2] \leq \frac{3}{4}\frac{1}{|\mathbf{G}|^{\epsilon'-d(\log d+1)}} < \frac{3}{4|\mathbf{G}|^{\epsilon'}}. \tag{2.2}$$

Using Markov's inequality, we obtain

$$\Pr_{s_1,\ldots,s_r}[\|P^{\star m}_{s_1,\ldots,s_r} - U\|^2 > \epsilon^2] < \frac{3}{4\epsilon^2|\mathbf{G}|^{\epsilon'}}.$$

Since the statistical distance is non-negative, the above inequality is equivalent to

$$\Pr_{s_1,\dots,s_r}[\|P^{\star m}_{s_1,\dots,s_r} - U\| > \epsilon] < \frac{3}{4\epsilon^2 |\mathbf{G}|^{\epsilon'}}. \tag{2.3}$$

□

2.5 Application to Pollard Rho – Proof of Theorem 2.3.1

We prove Theorem 2.3.1 in two steps: 1) we establish collision bounds in terms of mixing times; 2) we combine the previous bounds via a simple result from probability theory and carefully optimize for the parameters involved.

2.5.1 Collision Bounds and Mixing Times

Our proof is based on the following argument: let $\epsilon > 0$ and the r-tuple of transition steps $(s_1, \dots, s_r)$ be fixed. For notational convenience, we substitute $\tau = \tau_{s_1,\dots,s_r}(\epsilon)$. Given $t \geq 0$, we consider the probability $p(\epsilon, t, t_0)$ that no collision has occurred after the first $t_0 + (t+1)\tau$ steps of the walk. For instance, in case $t = 0$, we make $t_0 + \tau$ steps of the walk and compare the resulting end-point with the first t_0 elements of the walk. We can look at the probability $p(\epsilon, 0, t_0)$ and by definition of the mixing time τ,

$$p(\epsilon, 0, t_0) \leq 1 - \frac{t_0(1 - 2\epsilon|\mathbf{G}|)}{|\mathbf{G}|}.$$

More generally, the probability that the $(t_0 + (t+1)\tau)$th element of the walk does not collide with any of the first $t_0 + t\tau$ elements is at most

$$1 - \frac{(t_0 + t\tau)(1 - 2\epsilon|\mathbf{G}|)}{|\mathbf{G}|}.$$

Using $1 - x \leq e^{-x}$ for $x < 1$, we obtain

$$\begin{aligned} p(\epsilon, t, t_0) &\leq \left(1 - \frac{(t_0 + t\tau)(1 - 2\epsilon|\mathbf{G}|)}{|\mathbf{G}|}\right) p(\epsilon, t-1, t_0) \\ &\leq \exp\left(-\frac{(t_0 + t\tau)(1 - 2\epsilon|\mathbf{G}|)}{|\mathbf{G}|}\right) p(\epsilon, t-1, t_0). \end{aligned}$$

By induction on t, we prove the following lemma:

Lemma 2.5.1. *Let $\epsilon > 0$ be a real number and let $(s_1, \dots, s_r)$ be a fixed r-tuple of distinct elements of $\mathbf{G}$. Let $\tau = \tau_{s_1,\dots,s_r}(\epsilon)$ be the mixing time introduced in Definition 2.4.1. For any* *positive integers $t \geq 0$ and t_0 we have*

$$p(\epsilon, t, t_0) \leq \exp\left(-\frac{(1-2\epsilon|\mathbf{G}|)(t+1)(2t_0+t\tau)}{2|\mathbf{G}|}\right) =: B(\epsilon, t, t_0).$$

The above lemma bounds the probability that a collision is obtained after $t_0+(t+1)\tau$ steps. The next step is to optimize the integer parameters t_0 and t. Thus, the probability of **obtaining a collision** after at most $t(\epsilon, t, t_0) := t_0 + (t+1)\tau(\epsilon)$ Pollard rho steps is lower bounded by

$$\Pr_{\text{random walk}}[T_{s_1,\dots,s_r} \leq t(\epsilon, t, t_0)] \geq 1 - B(\epsilon, t, t_0).$$

For any $\epsilon < \dfrac{1}{2|\mathbf{G}|}$ and any t_0 (keeping in mind that $\kappa > 1$ by hypothesis), we first determine the minimal value of t for which the probability of failure (not obtaining a collision after $t(\epsilon, t, t_0)$ steps) is at most $e^{-\kappa}$. In other words,

$$B(\epsilon, t, t_0) = \exp\left(-\frac{(1-2\epsilon|\mathbf{G}|)(t+1)(2t_0+t\tau)}{2|\mathbf{G}|}\right) \leq e^{-\kappa} \iff$$
$$\frac{\tau}{2}t^2 + \left(\frac{\tau}{2}+t_0\right)t + t_0 - \frac{\kappa|\mathbf{G}|}{1-2\epsilon|\mathbf{G}|} \geq 0.$$

Here, we have used the hypothesis $\epsilon < \frac{1}{2|\mathbf{G}|}$ which implies that the discriminant of the above quadratic polynomial in t is positive, hence, by solving the quadratic inequality, we obtain:

$$t \geq \frac{-\left(\frac{\tau}{2}+t_0\right) + \sqrt{\frac{2\kappa|\mathbf{G}|}{1-2\epsilon|\mathbf{G}|}\tau + \left(\frac{\tau}{2}-t_0\right)^2}}{\tau} =: t'.$$

This means that $t_{\min} = \lceil t' \rceil$ is the minimal possible value for t that yields a probability of failure smaller than $e^{-\kappa}$ given $\epsilon, (s_1, \dots, s_r)$ and t_0. Hence, the number of Pollard rho steps necessary for producing a collision can be bounded by

$$t(\epsilon, t_{\min}, t_0) \leq \sqrt{\frac{2\kappa|\mathbf{G}|}{1-2\epsilon|\mathbf{G}|}\tau + \left(\frac{\tau}{2}-t_0\right)^2} + \frac{\tau}{2}.$$

The value of t_0 that minimizes the above bound is $t_0 = \left\lfloor \dfrac{\tau}{2} \right\rfloor$. Hence,

$$\begin{aligned}\min_{t,t_0} t(\epsilon, t, t_0) &\leq \sqrt{\frac{2\kappa|\mathbf{G}|}{1-2\epsilon|\mathbf{G}|}\tau + \frac{1}{4}} + \frac{\tau}{2} \\ &=: \mathbf{t}_{s_1,\dots,s_r}(\epsilon).\end{aligned}$$

Here, we intentionally write $s_1, \dots, s_r$ in the subscript to remind the reader of the dependency on the transition steps. Finally,

$$\Pr_{\text{random walk}}[T_{s_1,\ldots,s_r} \le \mathsf{t}_{s_1,\ldots,s_r}(\epsilon)] \ge 1 - e^{-\kappa}. \tag{2.4}$$

2.5.2 Completing the Proof

Recall that we need to prove the existence of $n_0 \ge 0$ for which the statement of Theorem 2.3.1 holds. As we proceed with the proof, we will show what inequalities the value n_0 needs to satisfy. First, suppose that n_0 satisfies

$$\frac{a-1}{e} \log\log n_0 - 1 > 0. \tag{2.5}$$

Second, suppose that $n_0 \ge n_0'$ where n_0' is the bound from Lemma 2.4.6 and suppose that $|\mathbf{G}| \ge n_0$. Let ϵ' be any real number that satisfies $0 < \epsilon' < \frac{a-1}{e}\log\log n_0 - 1$ (the existence of such ϵ' is guaranteed by the above inequality) and let $m = \left\lfloor \frac{\log|\mathbf{G}|}{(a-1)\log\log|\mathbf{G}|}(1+\epsilon') \right\rfloor$. Let $\epsilon > 0$ be a real number that satisfies $\epsilon < \frac{1}{2|\mathbf{G}|}$. Lemma 2.4.6 yields a bound on the probability of drawing an (ϵ, m)-faulty choice of $(s_1, \ldots, s_r)$ out of all r-tuples of distinct elements in $\mathbf{G}$. To complete the proof of Theorem 2.3.1, we need to combine (2.4) and (2.2) to get the desired result. We do this via standard union bounds from probability theory by using that if A, B_1 and B_2 are three events such that $A \Rightarrow \neg B_1 \vee \neg B_2$ then

$$\Pr[A] \le \Pr[\neg B_1] + \Pr[\neg B_2]. \tag{2.6}$$

We would like to apply (2.6) to A being the event

$$\text{Event } A\colon T_{s_1,\ldots,s_r} > c\sqrt{\kappa|\mathbf{G}|\log|\mathbf{G}|}$$

for some constant $c > 0$ that we specify below. Moreover, let B_1 be the event

$$\text{Event } B_1\colon T_{s_1,\ldots,s_r} \le \mathsf{t}_{s_1,\ldots,s_r}(\epsilon),$$

and let B_2 be the event

$$\text{Event } B_2\colon \tau_{s_1,\ldots,s_r}(\epsilon) \le m,$$

where m is the value from Lemma 2.4.6. In order to apply (2.6), we only need to choose the parameters ϵ and ϵ' in such a way that $A \Rightarrow \neg B_1 \vee \neg B_2$.

Assuming that the events B_1 and B_2 both hold, we obtain

$$T_{s_1,\ldots,s_r} \le \sqrt{\frac{2\kappa|\mathbf{G}|}{1-2\epsilon|\mathbf{G}|}m + \frac{1}{4}} + \frac{m}{2}.$$

Since $\epsilon' < \frac{(a-1)}{e} \log\log|\mathbf{G}| - 1$ then $m < \frac{\log|\mathbf{G}|}{e} + 1$. Substituting this in the above inequality, we obtain

$$\begin{aligned} T_{s_1,\ldots,s_r} &\leq \sqrt{\frac{2\kappa|\mathbf{G}|}{e(1-2\epsilon|\mathbf{G}|)}(\log|\mathbf{G}|+e)+\frac{1}{4}} + \frac{\log|\mathbf{G}|+e}{2e} \\ &\overset{(*)}{\leq} \sqrt{\frac{2\kappa|\mathbf{G}|}{e(1-2\epsilon|\mathbf{G}|)}(\log|\mathbf{G}|+3)}. \end{aligned}$$

Here, the inequality $(*)$ holds since we add an extra condition on n_0 that is deduced below. First let us notice that $\sqrt{a}+b = \sqrt{a+b^2+2b\sqrt{a}}$, for all positive real numbers a, b. Applying this for $a = \dfrac{2\kappa|\mathbf{G}|}{e(1-2\epsilon|\mathbf{G}|)}(\log|\mathbf{G}|+e)+\dfrac{1}{4}$ and $b = \dfrac{\log|\mathbf{G}|+e}{2e}$, we observe that in order for $(*)$ to hold, we need to prove that

$$\frac{1}{4} + \left(\frac{\log|\mathbf{G}|+e}{2e}\right)^2 + \frac{\log|\mathbf{G}|+e}{e}\sqrt{\frac{2\kappa|\mathbf{G}|}{e(1-2\epsilon|\mathbf{G}|)}(\log|\mathbf{G}|+e)+\frac{1}{4}} < \frac{2\kappa|\mathbf{G}|(3-e)}{e(1-2\epsilon|\mathbf{G}|)}.$$

Equivalently, we need to show that

$$\begin{aligned} \frac{e(1-2\epsilon|\mathbf{G}|)}{8\kappa|\mathbf{G}|} &+ \frac{(\log|\mathbf{G}|+e)^2(1-2\epsilon|\mathbf{G}|)}{8e\kappa|\mathbf{G}|} + \\ &+ \frac{(\log|\mathbf{G}|+e)^{3/2}\sqrt{e(1-2\epsilon|\mathbf{G}|)}}{e\sqrt{2\kappa|\mathbf{G}|}}\sqrt{1+\frac{e(1-2\epsilon|\mathbf{G}|)}{8\kappa|\mathbf{G}|(\log|\mathbf{G}|+e)}} < \\ &< 3-e \end{aligned}$$

and as $1-2\epsilon|\mathbf{G}| < 1$ and $\kappa > \log 2$, it suffices to show that one can choose n_0 such that for any $\mathbf{G}$ with $|\mathbf{G}| \geq n_0$,

$$\frac{e}{8|\mathbf{G}|\log 2} + \frac{(\log|\mathbf{G}|+e)^2}{8e\log 2\cdot|\mathbf{G}|} + \frac{(\log|\mathbf{G}|+e)^{3/2}}{\sqrt{2e\log 2\cdot|\mathbf{G}|}}\sqrt{1+\frac{e}{8|\mathbf{G}|\log 2(\log|\mathbf{G}|+e)}} < 3-e. \tag{2.7}$$

Now, if our n_0 is chosen such that each term

$$\frac{e}{8n_0\log 2} < \frac{3-e}{3},$$

$$\frac{(\log n_0+e)^2}{8e\log 2\cdot n_0} < \frac{3-e}{3}$$

and

$$\frac{(\log n_0+e)^{3/2}}{\sqrt{2e\log 2\cdot n_0}}\sqrt{1+\frac{e}{8n_0\log 2(\log n_0+e)}} < \frac{3-e}{3},$$

then inequality (2.7) holds for any $\mathbf{G}$ with $|\mathbf{G}| \geq n_0$.

The largest term in (2.7) is upper bounded by $\dfrac{(\log n_0+e)^{3/2}}{\sqrt{n_0}}$. If we impose the extra condition that this bound is also less than $\dfrac{3-e}{3}$ (i.e., the extra condition that n_0 should satisfy $9(\log n_0+e)^3 < (3-e)^2 n_0$), all of the above inequalities will hold whenever $|\mathbf{G}| \geq n_0$.

We now specify the constant c: it should be chosen such that the above upper bound can be further bounded by $c\sqrt{\kappa|\mathbf{G}|\log|\mathbf{G}|}$. It is clear that $c = 2/e$ is too small. Yet, we observe that for any positive real number $\delta > 0$ (independent of $|\mathbf{G}|$), one can use $c = \sqrt{\frac{(2+\delta)}{e}}$ and as long as $\epsilon < \left(1 - \frac{2}{2+\delta}\right)\frac{1}{2|\mathbf{G}|}$, i.e.,

$$T_{s_1,\ldots,s_r} \le \sqrt{\frac{(2+\delta)}{e}\kappa|\mathbf{G}|\log|\mathbf{G}|}. \tag{2.8}$$

Next, for the specified $\gamma > 0$, we would like to choose ϵ such that the upper bound on $\Pr(\neg B_2)$ established in Lemma 2.4.6 is upper bounded by $|\mathbf{G}|^{-\gamma}$, e.g., that $\frac{3}{4\epsilon^2|\mathbf{G}|^{\epsilon'}} < \frac{1}{|\mathbf{G}|^{\gamma}}$ which is achieved as long as $\epsilon > \sqrt{\frac{3}{4}}|\mathbf{G}|^{\frac{\gamma-\epsilon'}{2}}$.

To summarize, if we want to choose ϵ so that we guarantee simultaneously the following two conditions:

1. (i) $B_1 \wedge B_2 \Rightarrow \neg A$,
2. (ii) $\Pr(\neg B_2) < |\mathbf{G}|^{-\gamma}$,

then we need the lower bound on ϵ (namely, $\sqrt{\frac{3}{4}}|\mathbf{G}|^{\frac{\gamma-\epsilon'}{2}}$) to not exceed the upper bound (namely, $\left(1 - \frac{2}{2+\delta}\right)\frac{1}{2|\mathbf{G}|}$). This is achieved as long as $\epsilon' > \gamma + 2$. Since the only constraint on ϵ' is $\epsilon' < \frac{(a-1)}{e}\log\log|\mathbf{G}| - 1$, if we choose n_0 sufficiently large so that

$$\frac{(a-1)}{e}\log\log n_0 - 1 > \gamma + 2, \tag{2.9}$$

$$9(\log n_0 + e)^3 < (3-e)^2 n_0, \tag{2.10}$$

and

$$n_0 \ge n_0' \qquad \text{where } n_0' \text{ is the bound from Lemma 2.4.6}, \tag{2.11}$$

then for any $\mathbf{G}$ for which $|\mathbf{G}| \ge n_0$, the two conditions (i) and (ii) will hold. Thus, the only conditions that we need for n_0 are the inequalities (2.9),(2.10) and (2.11).

Finally, if the events B_1 and B_2 both occur then

$$T_{s_1,\ldots,s_r} < \sqrt{\frac{2+\delta}{e}\kappa|\mathbf{G}|\log|\mathbf{G}|},$$

so the event A, i.e., $T_{s_1,\ldots,s_r} > \sqrt{\frac{2+\delta}{e}\kappa|\mathbf{G}|\log|\mathbf{G}|}$, is impossible. The union bound then implies

$$\Pr_{\substack{s_1,\ldots,s_r\\ \text{random walk}}}\left[T_{s_1,\ldots,s_r} > \sqrt{\frac{2+\delta}{e}\kappa|\mathbf{G}|\log|\mathbf{G}|}\right] < e^{-\kappa} + \frac{1}{|\mathbf{G}|^{\gamma}},$$

i.e.,

$$\Pr_{\substack{s_1,\ldots,s_r\\ \text{random walk}}}\left[T_{s_1,\ldots,s_r} \le \sqrt{\frac{2+\delta}{e}\kappa|\mathbf{G}|\log|\mathbf{G}|}\right] \ge 1 - e^{-\kappa} - \frac{1}{|\mathbf{G}|^{\gamma}},$$

which concludes the proof of Theorem 2.3.1.

2.6 Conclusions

In the past few years, there has been a lot of attempts dedicated to rigorously proving the asymptotic run time of generic algorithms to solve the discrete logarithm problem based on the Pollard's rho method [52, 39, 38, 58, 40]. With respect to Model 2, we rigorously prove collision bounds for general cyclic groups $\mathbf{G}$ of prime order for the most common variation of Pollard rho (currently used to solve the discrete logarithm problem on a generic elliptic curve), namely the Pollard rho method using additive walks. Using mixing time estimates from Dou and Hildebrand [32, 16], we are able to prove a collision bound of $\mathcal{O}(\sqrt{|\mathbf{G}| \log |\mathbf{G}|})$ with probability greater than 50%. We hope that, just as in the case of the original Pollard rho setting, this is only the first step in rigorously proving the asymptotic bound for the additive Pollard rho algorithm.

3 Analytic and Algebraic Theory of Polarized Abelian Varieties

This chapter is meant to provide the theoretic background for Chapter 4 regarding explicit computations of cyclic isogenies between Jacobians of genus 2 hyperelliptic curves. In Section 3.1.1 we focus on the theory of g-dimensional complex abelian varieties whose group of complex points has the structure of a complex torus admitting a non-degenerate Riemann form. Moreover, the condition for the torus to admit an embedding into a suitable projective space is given in a few equivalent ways. For the purpose of fixing a certain embedding of a complex torus into a suitable projective space in Section 3.1.2.1, we give a short exposition of the Riemann theta functions in Section 3.1.2. It is followed by an useful application in Section 3.1.3 that links the projective coordinates of an arbitrary point on two isomorphic principally polarized complex tori. The last part 3.1.4 of this section is dedicated to a brief overview of the Taniyama–Shimura theory of complex abelian varieties with complex multiplication as it is useful for presenting the results of Chapter 4. In Section 3.2, we switch to abelian varieties defined over an arbitrary field k and present the theory behind theta structures and isogenies of polarized abelian varieties with compatible theta structures. The aim is to give an algebraic description of the theory over the complex field presented in the previous section.

3.1 Abelian Varieties over the Complex Field

3.1.1 Preliminaries

Let V denote a complex vector space of dimension g. The group of complex points of an abelian variety X of dimension g over the complex field is isomorphic to a complex torus $T := V/\Lambda$ for some $\mathbf{Z}$-lattice $\Lambda \subset V$ of maximal rank $2g$. The torus T is a connected and compact complex manifold. The torus together with an analytic isomorphism $\theta_X : X \to T$ is called an analytic system of coordinates for the abelian variety X [71, p.21]. The dual $\mathbf{R}$ vector space of V is the set of $\mathbf{R}$-linear homomorphisms $V^\vee := \mathrm{Hom}_{\mathbf{R}}(V, \mathbf{R})$ [57, p.1] and we define the dual lattice of Λ in $V^\vee$ as $\Lambda^\vee := \{\varphi \in V^\vee | \varphi(\lambda) \in \mathbf{Z},\ \forall \lambda \in \Lambda\}$. The *dual torus* is by definition $T^\vee = V^\vee/\Lambda^\vee$.

The converse of this statement is not true as not all complex tori correspond to abelian varieties. In order for a complex torus V/Λ to be identified with the group of complex points of an abelian variety, the torus must admit a non-degenerate Riemann form $E\colon V \times V \to \mathbf{R}$ [67, p.85].

By definition, a Riemann form E is an $\mathbf{R}$-bilinear form $E\colon V \times V \to \mathbf{R}$ satisfying

— $E(u,u)=0$ for all $u \in V$ (alternating),
— $E(\Lambda,\Lambda) \subseteq \mathbf{Z}$,
— $E(iv,iw)=E(v,w)$ for all complex vectors v,w and i the complex root $\sqrt{-1}$.
Following the definition of a symplectic form on any vector space (namely it is an $\mathbf{R}$-bilinear, alternating, non-degenerate form), a non-degenerate Riemann form E is also a symplectic form on V, and so, the vector space V is symplectic. We call a non-degenerate Riemann form $E\colon V \times V \to \mathbf{R}$ with respect to Λ a **polarization on** V/Λ.

Next, we give an explicit formula for the Riemann form in terms of a basis of the lattice (and of the complex space V). If $\{v_1, \dots v_{2g} \in V\}$ is a basis for the lattice, we represent E as a matrix $J \in M_{2g\times 2g}(\mathbf{Z})$ whose element on row s and column t is $j_{s,t}=E(v_s,v_t)$. The matrix J is a representation matrix of E and is skew-symmetric ($-J^t=J$) and invertible.[1]

For the rest of this section, we fix once and for all a complex basis of V. We also use the standard basis of $\mathbf{R}^{2g}$ and the standard representation of $\mathbf{C}$ as an $\mathbf{R}$ vector space of dimension 2. Hence, we identify V with an $\mathbf{R}$-vector space V of dimension $2g$. Then, the value of the Riemann form at any pair of points $x,y \in V$ is given by $E(x,y)=a^t \cdot J \cdot b$, where a,b are unique in $\mathbf{R}^{2g}$ such that $x=\sum_i^{2g} a_i v_i$ and $y=\sum_i^{2g} b_i v_i$.

Moreover, according to [6, p.46], there exists a $\mathbf{Z}$-basis $\mathcal{B}=\{v_1,\dots,v_g,w_1,\dots,w_g\}$ of Λ for which the matrix representation of E is $J_D := \begin{pmatrix} O_g & D \\ -D & O_g \end{pmatrix}$, with $D=\mathrm{diag}(d_1,\dots,d_g)$ where d_i are strictly positive integers satisfying $d_i|d_{i+1}$ for all $i \in \{1,\dots,g-1\}$, and O_g is the zero matrix in $M_g(\mathbf{Z})$. By definition *the type of* E (or of the polarization) is $\delta := (d_1,\dots,d_g)$, or equivalently, the diagonal matrix D.

Such a basis $\mathcal{B}$ is called a *symplectic basis* of Λ with respect to E. This definition is a generalization of the classical definition of symplectic bases for E, i.e., $\mathcal{B}$ is symplectic if it satisfies $E(v_i,v_j)=0=E(w_i,w_j)$ and $E(v_i,w_j)=\delta_{i,j}$ for all $i,j=1,\dots,g$.[2] Moreover, in our case we also obtain that $\langle v_1,\dots,v_g\rangle \oplus \langle w_{g+1},\dots,w_{2g}\rangle$ is a decomposition of Λ in 2 isotropic spaces for the choice of E. It automatically induces a decomposition of the symplectic space V in two isotropic spaces.

We define the *period matrix* of Λ as $P=(P_1\ P_2)$, where $P_1=(v_1\dots v_g)$ and $P_2=(w_1\dots w_g)$ are two complex square matrices of dimension $g\times g$. According to [43, p.134], if the Riemann form E is of type $(1,\dots,1)$, then the matrix P_2 is invertible and moreover, the matrix $\Omega := P_1P_2^{-1}$ is in the Siegel upper half space

$$\mathcal{H}_g = \{X+iY=\Omega \in M_g(\mathbf{C}) \,|\, \Omega=\Omega^t \text{ and } Y \text{ positive definite}\}.$$

In this case, we also say that the complex torus admits a *principal polarization.* Thus, the existence of a principal polarization on T induces a decomposition of the lattice Λ as $\Omega\mathbf{Z}^2+\mathbf{Z}^2$. Conversely, given $\Omega \in \mathcal{H}_2$ such that $\Lambda=\Omega\mathbf{Z}^2+\mathbf{Z}^2$, a non-degenerate Riemann form of type $(1,\dots,1)$ on Λ is given by $E(x_1\Omega+y_1, x_2\Omega+y_2)=x_1^ty_2-y_1^tx_2$. This result is very important as the existence of a principal polarization on V/Λ that gives rise to $\Omega \in \mathcal{H}_g$ allows us to define later on analytic theta functions and to embed T into a suitable projective space. The existence of such an embedding is guaranteed by the Lefschetz's theorem (see Section 3.1.2).

We can extend the above result to complex tori with Riemann forms of general type D, namely given $(V/\Lambda,E)$ and a symplectic basis $\mathcal{B}$ for E, there exists a matrix $\Omega \in \mathcal{H}_g$ such that $\Lambda=\Omega\mathbf{Z}^g+D\mathbf{Z}^g$ [6, §8.1].

[1] J^t denotes the transpose of J

[2] $\delta_{i,j}=1$ if $i=j$, and $\delta_{i,j}=0$ otherwise.

We write the corresponding period matrix as $P_D = (\Omega\, D)$. Since a common aspect for all complex tori with polarizations of arbitrary type is the existence of a matrix in $\mathcal{H}_g$, it is natural to present morphisms between two complex tori (that may not or not preserve the type of the polarization) in relation with their period matrices. We start with isomorphisms that preserve the polarization type as it is particularly useful later on when defining embeddings of isomorphic tori into some projective space via analytic Riemann theta functions (see Section 3.1.3). First, for any symplectic matrix $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{Sp}_{2g}(\mathbf{Q})$, with $\gamma\Lambda \subseteq \Lambda$, the map $\Omega \mapsto \gamma \cdot \Omega = (a\Omega + b)(c\Omega + d)^{-1}$ defines an action of $\mathbf{Sp}_{2g}(\mathbf{Q})$ on the Siegel upper half space $\mathcal{H}_g$. We denote by $P'_D = (\gamma \cdot \Omega\, D)$ the period matrix of the torus T'. The change of basis induces an isomorphism from $T = V/\Omega\mathbf{Z}^g + D\mathbf{Z}^g$ onto $V/\gamma \cdot \Omega\mathbf{Z}^g + D\mathbf{Z}^g$ [6, p.212]. According to [6, Prop. 8.1.3], the elements $\{\gamma \in \mathbf{Sp}_{2g}(\mathbf{Q}) |\ \gamma\Lambda \subseteq \Lambda\}$ are in bijection with the set of isomorphic complex tori with polarizations of the same type D, namely $\{V/\Omega\mathbf{Z}^2 + D\mathbf{Z}^2 |\ \Omega \in \mathcal{H}_2\}$.

We also mention other maps between complex tori, starting with general homomorphisms, and their analytic and rational representation, and ending with the isogeny definition. A map $\phi\colon V/\Lambda \to V/\Lambda' =: T'$, where Λ' is a $\mathbf{Z}$-lattice of rank $2g$, is called a *homomorphism* of complex tori if it is a holomorphic map that preserves the group structures. According to [6, p.10], it admits an analytic representation via a map $\rho_a\colon \mathrm{Hom}(T, T') \to \mathrm{End}_{\mathbf{C}}(V)$ that associates a unique $\mathbf{C}$-linear map $\Phi\colon V \to V$ with $\Phi(\Lambda) \subset \Lambda'$ to the homomorphism ϕ. The rational representation of ϕ is the restriction Φ_Λ of Φ to the lattice Λ via the injective homomorphism $\rho_r\colon \mathrm{Hom}(T, T') \to \mathrm{Hom}_{\mathbf{Z}}(\Lambda, \Lambda')$. The map Φ is given by a g-by-g complex matrix M_a and the matrix representation of $\rho_r(\phi)$ is a $2g$-by-$2g$ integer matrix M_r, satisfying $M_a P_D = P'_D M_r$.

Definition 3.1.1. An isogeny of complex tori $\varphi\colon T \to T'$ is a surjective homomorphism of finite kernel.

Next, for the purpose of finding analogue concepts in the case of abelian varieties over an arbitrary field, we give alternative descriptions of polarizations on T (and consequently on the abelian variety X) that are not in terms of bilinear forms, or period matrices. First, we introduce a connection between a Riemann form E on the torus T and a class of line bundles $\mathcal{L}$ on T. We make the observation that from now on we do not impose (unless made precise) that the Riemann form is non-degenerate, or in other words, that it is a polarization. Another good consequence of introducing line bundles is a new description of the dual torus $T^\vee$ that was defined at the beginning of this section.

As in [6, p.24], the group $H^1(T, \mathcal{O}_X^*)$ is identified with the group of *holomorphic line bundles* on T.[3] We define the *Néron-Severi group* as the image of the homomorphism $c_1\colon H^1(T, \mathcal{O}_T^*) \to H^2(T, \mathbf{Z})$. Consider a holomorphic line bundle $\mathcal{L}$ and let $c_1(\mathcal{L}) \in H^2(T, \mathbf{Z})$ be the first Chern class of $\mathcal{L}$. According to [6, Cor. 1.3.2] the first Chern class of $\mathcal{L}$ is identified with an alternating $\mathbf{Z}$-valued form E on the lattice Λ. The next goal is to prove that E can be extended to a Riemann form on V/Λ.

First, according to [6, Append. B], the line bundle $\mathcal{L}$ is canonically identified with a non vanishing holomorphic function $f\colon \Lambda \times V \to \mathbf{C}^*$ satisfying $f(\lambda + \mu, v) = f(\lambda, \mu + v) \cdot f(\mu, v)$ for all parameters $\lambda, \mu \in \Lambda$ and $v \in V$. The function f is called the canonical factor of automorphy for $\mathcal{L}$. Next, the factor of automorphy f allows us to map $c_1(\mathcal{L})$ to an alternating form $E\colon \Lambda \times \Lambda \to \mathbf{Z}$ of equation given in [6, Thm. 2.1.2]. The form E is indeed a Riemann form [6, Prop. 2.1.6], and moreover the existence of a Riemann form on T is equivalent to the existence of a holomorphic line bundle on T for which $c_1(\mathcal{L})$ is

[3] The group operation on $H^1(T, \mathcal{O}_X^*)$ is classically denoted by $\otimes$, but we omit it in general in the exponent, i.e., $\mathcal{L}^n = \underbrace{\mathcal{L} \otimes \ldots \otimes \mathcal{L}}_{n}$.

identified with E.

Next, we make more precise the connection between a polarization on T and a specific holomorphic line bundle (out of all line bundles that have the same Chern class). First we define a form on $V \times V$ that can also be identified with $c_1(\mathcal{L})$. Given a Riemann form $E\colon V \times V \to \mathbf{R}$ on the torus T, we define the Hermitian form $H\colon V \times V \to \mathbf{C}$ as $H(u,v) = E(iu,v) + iE(u,v)$. Indeed, it is easy to see that H is $\mathbf{C}$-linear in the first parameter and satisfies $H(u,v) = \overline{H(v,u)}$. Moreover, the set of Hermitian forms on V, with imaginary part $\mathrm{Im}(H(\Lambda,\Lambda)) \subseteq \mathbf{Z}$, is in bijection with the set of Riemann forms on T [6, Lem 2.1.7]. Hence, there exists a line bundle $\mathcal{L}$ whose first Chern class is identified with H (or equivalently with E).

We also link a holomorphic line bundle $\mathcal{L}$ of first Chern class H to a semicharacter for H. By definition, a semicharacter for H is a map $\chi\colon \Lambda \to \mathbf{C}_1$, where $\mathbf{C}_1 := \{z \in \mathbf{C} : \ |z| = 1\}$, such that for all $\lambda,\, \mu \in \Lambda,\ \chi(\lambda+\mu) = \chi(\lambda)\chi(\mu)e(\frac{1}{2}\mathrm{Im}H(\lambda,\mu))$ (where we use the classical notation of $e(x) := e^{2\pi i x}$ where i is the square root of -1 and π the constant number $3.14159\ldots$). Given a pair (H,χ), one can deduce a corresponding factor of automorphy [6, p.30] that leads to a line bundle $\mathcal{L}(H,\chi) \simeq V \times \mathbf{C}/\Lambda$ via the method in [6, Append. B]. The Appel–Humbert Theorem [6, Thm. 2.2.3] proves that any holomorphic line bundle $\mathcal{L}$ whose first Chern class corresponds to H is isomorphic to $\mathcal{L}(H,\chi)$, for a unique semicharacter χ. We define the *Picard group* $\mathrm{Pic}(T)$ as the group of isomorphism classes of holomorphic line bundles on T and $\mathrm{Pic}^0(T)$ as the group of isomorphism classes of line bundles of Chern class 0 (representatives of the form $\mathcal{L}(0,\chi)$, with $\chi \in \mathrm{Hom}(\Lambda, \mathbf{C}_1)$).

The group $\mathrm{Pic}^0(T)$ is identified with the dual torus $T^\vee$ [6, Prop. 2.4.1]. For any line bundle $\mathcal{L}$ on T and any $x \in T$, the line bundle $t_x^*\mathcal{L} \otimes \mathcal{L}^{-1}$, where t_x represents translation by x, is of first Chern class 0. Hence, for any line bundle $\mathcal{L}$ and $x \in T$, we define a map $\varphi_{\mathcal{L}}\colon T \to T^\vee$, of this form $x \to t_x^*\mathcal{L} \otimes \mathcal{L}^{-1}$. This map is proven to be a homomorphism [6, p.36] that depends only on $c_1(\mathcal{L})$ [6, Cor. 2.4.6]. The kernel of $\varphi_{\mathcal{L}}$ is denoted by $K(\mathcal{L})$ and in the case of $c_1(\mathcal{L}) = E$ being non-degenerate, the kernel is finite and so $\varphi_{\mathcal{L}}$ is an isogeny of degree equal to $\det(E)$. If the isogeny has degree 1 then we are in the case of a principal polarization that we denote by $\mathcal{L}_0$.

Remark 5. Hence, we identify a polarization on T with a non-degenerate Riemann form E or a positive definite Hermitian form H or a holomorphic line bundle of non-degenerate first Chern class $c_1(\mathcal{L})$.

We review quickly some well known definitions of line bundles. A *positive definite line bundle* $\mathcal{L}$ is by definition a line bundle whose first Chern class is given by a positive definite Hermitian form H (or alternatively by a non-degenerate Riemann form). Equivalently, in this case the line bundle is said to be ample [6, Th. 4.5.1]. We can also verify that $\mathcal{L}$ being an *ample line bundle* implies that the surjective map $\varphi_{\mathcal{L}}\colon T \to T^*$ of kernel $K(\mathcal{L})$ is indeed an isogeny.

We say that two line bundles $\mathcal{L}_1$ and $\mathcal{L}_2$ on T are *algebraically equivalent* if and only if they have the same Chern class. Since $\mathrm{Pic}(T)/\mathrm{Pic}^0(T)$ is the group of isomorphism classes of holomorphic line bundles modulo algebraic equivalence, there exists a line bundle $\mathcal{L}^0 \in \mathrm{Pic}^0(T)$ such that $\mathcal{L}_2 = \mathcal{L}_1 \otimes \mathcal{L}^0$. If $\mathcal{L}_1$ is ample, there exists some $x \in K(\mathcal{L}_1)$ such that $\mathcal{L}_2 = t_x^*\mathcal{L}_1$ [6, Cor. 2.5.4] and so the line bundle $\mathcal{L}^0$ from above can be written as $t_x^*\mathcal{L}_1 \otimes \mathcal{L}_1^{-1}$. We say that two line bundles $\mathcal{L}_1$ and $\mathcal{L}_2$ are *linearly equivalent* if they are isomorphic, or in other words if they are represented by linearly equivalent divisors. One can extend the notion of algebraic equivalence by saying that $\mathcal{L}_1$ and $\mathcal{L}_2$ are equivalent up to an automorphism whenever there exists an automorphism ξ of T such that $\mathcal{L}_2$ is algebraically equivalent to $\xi^*\mathcal{L}_1$.

3.1.2 Riemann Theta Functions

In this section we define Riemann theta functions with respect to a period matrix of the form $P = (\Omega\, I_g)$, with $\Omega \in \mathcal{H}_g$. As before, the corresponding complex torus is $T = \mathbf{C}^g/\Omega\mathbf{Z}^2 + \mathbf{Z}^2$.

Consider the positive definite Hermitian form $H\colon V \times V \to \mathbf{C}$ that is corresponding to $\Omega \in \mathcal{H}_g$ and let $E = \mathrm{Im}(H)$. Let $V = V_1 \oplus V_2$ be the decomposition of V given by the decomposition of $\Lambda = \Lambda_1 \oplus \Lambda_2$ (due to the period matrix P). Consider the line bundle $\mathcal{L}_0 = L(H, \chi_0)$ of first Chern class H and semicharacter $\chi_0\colon \Lambda \to \mathbf{C}^\times$ given by $\chi_0(v) = e(\frac{1}{2}E(v_1, v_2))$, where $v = v_1 + v_2$ with $v_1 \in \Lambda_1, v_2 \in \Lambda_2$. When restricted to $v \in \Lambda_1$ or $v \in \Lambda_2$, we have $E(v_1, v_2) = 0$ and so, the semicharacters $\chi_0|_{\Lambda_1}, \chi_0|_{\Lambda_2}$ are trivial.

Moreover, the line bundle $\mathcal{L}_0 = \mathcal{L}(H, \chi_0)$ is well defined among all holomorphic line bundles of the same first Chern class H (or equivalently in the same algebraic equivalence class) and $\mathcal{L}_0$ is the only line bundle of first Chern class H whose semicharacter is trivial when restricted onto Λ_1 and Λ_2 respectively. Next, we see that we can link the canonical factors of automorphy of $\mathcal{L}_0$ (see [6, p.50] for the definition) to the so-called Riemann theta function corresponding to Ω.

Definition 3.1.2. Given $\Omega \in \mathcal{H}_g$, the Riemann theta function $\theta\colon V \to \mathbf{C}$ associated to Ω is

$$\theta(z, \Omega) := \sum_{x \in \mathbf{Z}^g} e\left(\frac{1}{2}x^t\Omega x + x^t z\right). \tag{3.1}$$

The Riemann theta function of characteristic $(a, b) \in \mathbf{R}^g \times \mathbf{R}^g$ associated to Ω is by definition $\theta\begin{bmatrix} a \\ b \end{bmatrix} : V \to \mathbf{C}$, with

$$\theta\begin{bmatrix} a \\ b \end{bmatrix}(z, \Omega) := \sum_{x \in \mathbf{Z}^g} e\left[\frac{1}{2}(a + x)^t\Omega(a + x) + (a + x)^t(z + b)\right]. \tag{3.2}$$

Let $c = \Omega a + b \in V$, with $a, b \in \mathbf{R}^g$. Then the canonical semicharacter for the line bundle $t_c^*\mathcal{L}_0$ is of the form $\chi_c\colon \Lambda \to C^\times$ where $\chi_c = \chi_0 \cdot e(E(c, \cdot))$ [6, Lem 2.3.2] and furthermore, according to [6, Rem. 8.5.3], the canonical factor of automorphy corresponding to $t_c^*\mathcal{L}_0$ is $g_c\colon \Lambda \times V \to \mathbf{C}^*$ of the form

$$g_c(\Omega\alpha + \beta, z) = e(a^t\beta + b^t\alpha - \frac{1}{2} \cdot \alpha^t\Omega\alpha - z^t\alpha), \text{ where } \alpha, \beta \in \mathbf{Z}^2 \text{ and } z \in V.$$

In case $c = 0$ and the corresponding line bundle is $\mathcal{L}_0$, the canonical factor of automorphy g for the Riemann theta function is $g_0(\Omega\alpha + \beta, z) = e(-\frac{1}{2}\alpha^t\Omega\alpha - z^t\alpha)$, where $\alpha, \beta \in \mathbf{Z}^2$ and $z \in V$.

According to [6, §8.5], the space of Riemann theta functions with characteristics $a, b \in \mathbf{R}^g$ is identified with the space of holomorphic functions $\Theta\colon V \to \mathbf{C}$ that satisfy $\Theta(\lambda + z) = g_{a\Omega+b}(\lambda, z)\Theta(z)$ for all $\lambda \in \Omega\mathbf{Z}^2 + \mathbf{Z}^2$ and $z \in V$. Following [66, p.23], the space of Riemann theta functions with characteristics a, b is identified with the space of global sections of $\Gamma(T, t_c^*\mathcal{L}_0))$.

Given a line bundle $\mathcal{L}$, there exists $c = \Omega a + b \in V$, with $a, b \in \mathbf{R}^g$ (unique up to translation by $\lambda \in \Lambda$) such that $t_c^*\mathcal{L}_0 \simeq \mathcal{L}$ [6, Lem.3.1.2]. The uniqueness up to translation is in other words: for all $a, b \in \mathbf{R}^g$, if and only if $c', c'' \in \mathbf{Z}^g$ then

$$\theta\begin{bmatrix} a + c' \\ b + c'' \end{bmatrix}(z, \Omega) = \theta\begin{bmatrix} a \\ b \end{bmatrix}(z, \Omega), \text{ for all } z \in V \tag{3.3}$$

Definition 3.1.3. Consider the lattice decomposition $\Lambda = \Omega\mathbf{Z}^2 + D\mathbf{Z}^2$, with $D = \mathrm{diag}(d_1, \ldots, d_g)$ for some positive integers $d_1|d_2|\ldots|d_g$. A Riemann theta function with characteristics $a \in D^{-1}\mathbf{Z}^g$ and $b \in \mathbf{Z}^g$ is called a Riemann theta function of type D.

If $d_1 = \ldots = d_g = n$, for some integer $n \geq 2$, a Riemann theta function with characteristics $a \in 1/n\mathbf{Z}^g$ and $b \in \mathbf{Z}^g$ is called a *Riemann theta function of level* n.

3.1.2.1 Embeddings of T into a Projective Space

The Riemann theta functions of level $n \geq 2$ prove to be particularly useful when embedding the torus into a certain complex projective space. As in [66, 13], for a positive integer $n \geq 2$, we define the group $\mathbf{Z}(n) := (\mathbf{Z}/n\mathbf{Z})^g$ whose elements are written as column vectors with elements in $\mathbf{Z}/n\mathbf{Z}$. When using $\mathbf{Z}(n)$ in the definitions of theta functions below, we see an element $a \in \mathbf{Z}(n)$ as $a \in \mathbf{Z}^g$. Given $a \in \mathbf{Z}(n)$ (or $a \in \mathbf{Z}^g$) and a positive integer m, by abuse of notation we denote by a/m the rational vector $(a_1/m, \ldots, a_g/m)^t$.

First, let $\mathcal{L} = \mathcal{L}_0^n = \mathcal{L}(nH, \chi_0^n)$ for some integer $n \geq 2$. Then, the kernel $K(\mathcal{L})$ consists of the n-torsion points $\Omega a/n + b/n$, where $a, b \in \mathbf{Z}^g$, [6, Lem. 2.4.7]. Furthermore, there exists an n-torsion point c, such that $t_c^*\mathcal{L}_0 \simeq \mathcal{L}$. Again, following [6, §8.5] and [66, p.23], the space of global sections $\Gamma(T, \mathcal{L})$ is identified with the space of Riemann theta functions of level n. Given the property (3.3), in order to generate the space of Riemann theta functions of level n, it is enough to consider the case of $a \in \mathbf{Z}(n)$ and $b = 0$.

Similarly to the work of [22, 66, 12, 48], we prefer to work with a second basis for the space of global sections $\Gamma(T, \mathcal{L})$ that corresponds to $a = 0$ and $b \in \mathbf{Z}(n)$. The basis consists of the following functions $\theta_b \colon V \to \mathbf{C}$ with:

$$\theta_b(z) = \theta \begin{bmatrix} 0 \\ b/n \end{bmatrix} \left(z, \frac{\Omega}{n}\right), \ b \in \mathbf{Z}(n). \tag{3.4}$$

For the change of basis we refer to [12, Eq. (3.6-7)].

Consider the projective space $\mathbf{P}(\Gamma(T, \mathcal{L}))$ of dimension $n^g - 1$ over $\mathbf{C}$. A theorem of Lefschetz [6, Thm. 4.5.1] states that for $n \geq 3$, the map $(\theta_i)_{i \in \mathbf{Z}(n)} : T \to \mathbf{P}(\Gamma(T, \mathcal{L}))$ is an embedding. For $n = 2$, the level 2 theta functions determine instead an embedding of the Kummer surface $S = T/\{\pm 1\}$ into $\mathbf{P}^{2^g - 1}(\mathbf{C})$ [6, Thm. 4.8.1].

We define the *projective theta null point of level* n as $(\theta_i(0))_{i \in \mathbf{Z}(n)} \in \mathbf{P}(\Gamma(T, \mathcal{L}))$. We also call the embedding of 0 into $\mathbf{P}(\Gamma(T, \mathcal{L}))$ as *theta constants of level* n. By definition, for $z \in V$ the values $(\theta_b(z))_{b \in \mathbf{Z}(n)}$ are called *projective theta coordinates of level* n for the point z.

In the case of $n = k^2$, another basis of $\Gamma(T, \mathcal{L})$ is the so-called basis of level (k, k), given by the so-called Riemann theta functions of level (k, k). The projective theta coordinates of level $(2, 2)$ for $z \in T$ are:

$$\theta \begin{bmatrix} a/k \\ b/k \end{bmatrix} (kz, \Omega), \ a, b \in \mathbf{Z}(k). \tag{3.5}$$

For all $a, b \in \mathbf{Z}(k)$ and $v \in \mathbf{Z}(k)$, the following relation holds (for all $z \in T$):

$$\theta \begin{bmatrix} a/k \\ b/k + v/k \end{bmatrix} (z, \Omega) = e(a^t \cdot v) \cdot \theta \begin{bmatrix} a/k \\ b/k \end{bmatrix} (z, \Omega). \tag{3.6}$$

The level (k, k) basis is particularly interesting in the case of $n = 4$ and $k = 2$ as this is the case of the smallest even level for which there exists an embedding of T into a projective space. Later on, we will require n to be even for the purpose of defining operations on points in projective theta coordinates. Going back and forth between theta coordinates of level 4 and level $(2, 2)$ for a point $z \in T$ is given below as in [12, p.38]. For every $z \in V$, for every $b \in \mathbf{Z}(4)$, we have

$$\theta_b \left(z, \frac{\Omega}{4} \right) = \sum_{\alpha \in \mathbf{Z}(2)} \theta \begin{bmatrix} \alpha/2 \\ b/2 \end{bmatrix} (2z, \Omega) \, . \tag{3.7}$$

Remark 6. In order for the value $\theta \begin{bmatrix} \alpha/2 \\ b/2 \end{bmatrix} (2z, \Omega)$ to be computed by evaluating a theta function of level $(2, 2)$ at z, we first write uniquely $b = 2v + b'$, where b' has components in $\{0, 1\}$ (so $v, b' \in \mathbf{Z}(2)$), and by (3.6), we obtain:

$$\theta \begin{bmatrix} \alpha/2 \\ b/2 \end{bmatrix} (2z, \Omega) = e(2a^t \cdot v) \cdot \theta \begin{bmatrix} \alpha/2 \\ b'/2 \end{bmatrix} (2z, \Omega) = \theta \begin{bmatrix} \alpha/2 \\ b'/2 \end{bmatrix} (2z, \Omega) \, .$$

For any point $z \in T$, to change the level from $(2, 2)$ to 4, we use that for all $a, b \in \mathbf{Z}(2)$ we have:

$$\theta \begin{bmatrix} a/2 \\ b/2 \end{bmatrix} (2z, \Omega) = \frac{1}{2^g} \sum_{\beta \in \mathbf{Z}(2)} (-1)^{a^t \beta} \theta \begin{bmatrix} 0 \\ b/4 + \beta/2 \end{bmatrix} \left(z, \frac{\Omega}{4} \right) . \tag{3.8}$$

Following [12, Prop. 3.1.11], given a theta null point of level n, we can obtain the corresponding projective theta coordinates of level n (also called canonical) for the n-torsion points $\Omega\alpha/n + \beta/n$, with $\alpha, \beta \in \mathbf{Z}(n)$ as:

$$\theta_b \left(\Omega\alpha/n + \beta/n, \Omega \right) = e(-\alpha^t b/n) \cdot \theta_{b+\beta} \left(0, \Omega \right) , \tag{3.9}$$

for all $b \in \mathbf{Z}(n)$.

Furthermore, given a theta null point of level $(2, 2)$, we can obtain projective theta coordinates of level $(2, 2)$ for the 4-torsion points $\Omega\alpha/4 + \beta/4$, with $\alpha, \beta \in \mathbf{Z}(4)$, as:

$$\theta \begin{bmatrix} a/2 \\ b/2 \end{bmatrix} (2(\Omega\alpha + \beta), \Omega) = e(-\alpha^t b/4) \cdot \theta \begin{bmatrix} (a + 2\alpha)/2 \\ (b + 2\beta)/2 \end{bmatrix} (0, \Omega) \, , \tag{3.10}$$

for all $a, b \in \mathbf{Z}(2)$.

Consider the classical projective map $p_T \colon \mathbf{A}(\Gamma(T, \mathcal{L})) \setminus \{0\} \to \mathbf{P}(\Gamma(T, \mathcal{L}))$ and define the affine cone of T as $\widetilde{T} := p^{-1}(T)$. An affine lift of $z \in T$ is simply an element in the preimage $p_T^{-1}(x)$ and is denoted by $\widetilde{0}$.

3.1.3 Symplectic Isomorphisms and Theta Functions

Recall that in Section 3.1.1 we introduced symplectic isomorphisms of complex tori of the form $V/\Omega\mathbf{Z}^g + \mathbf{Z}^g \to V/\Omega'\mathbf{Z}^g + \mathbf{Z}^g$, where $\Omega, \Omega' \in \mathcal{H}_g$. Here we show that we can compute the theta functions of level $n \geq 2$ corresponding to Ω' (for the isomorphic torus T') from the theta functions of level n corresponding to Ω (for the torus T). That allows us to switch between different projective embeddings of the same isomorphism class of complex tori. This formula has an analogue in the case of abelian varieties over an arbitrary field, and in particular in the case of Jacobians of hyperelliptic curves (see section 4.7).

The elements $\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ of $\mathbf{Sp}_{2g}(\mathbf{Z})$ act as an isomorphism on the Siegel upper half space $\mathcal{H}_g$ given by $\Omega \to \gamma \cdot \Omega = (A\Omega + B)(C\Omega + D)^{-1}$. It induces an isomorphism of corresponding tori, i.e., $\gamma \colon T = V/\Omega\mathbf{Z}^g + \mathbf{Z}^g \to T' = V/\gamma \cdot \Omega\mathbf{Z}^g + \mathbf{Z}^g$ of the form $z = \Omega z_1 + z_2 \to \gamma \cdot z = ((C\Omega + D)^t)^{-1} z$, for any $z \in T$.

Given the Riemann theta functions of level $n \geq 2$ associated to Ω and the corresponding projective theta coordinates of any $z \in T$ (as defined in Section 3.1.2), we expect to be able to obtain Riemann theta functions of level n associated to $\gamma \cdot \Omega$ together with the corresponding projective theta coordinates of $\gamma \cdot z$. Indeed, such relation exists and it is proven by Igusa [34, §5, Thm.2] for general $\gamma \in \mathbf{Sp}_{2g}(\mathbf{Z})$. We review the equation proven by Igusa.

Let $\mathbf{a} = (a_1, \ldots, a_g)$ and $\mathbf{b} = (b_1, \ldots, b_g)$ be two vectors in $\mathbf{R}^g$. For any $\gamma \in \mathbf{Sp}_{2g}(\mathbf{Z})$ and for any $(z, \Omega) \in \mathbf{C}^g \times \mathcal{H}_g$ the following relation holds:

$$\theta \begin{bmatrix} \mathbf{a}' \\ \mathbf{b}' \end{bmatrix} (\gamma \cdot z, \gamma \cdot \Omega) = \xi_\gamma \cdot \xi_{z,\gamma} \cdot \xi_{\mathbf{a},\mathbf{b}} \cdot \sqrt{\det(C\Omega + D)} \cdot \theta \begin{bmatrix} \mathbf{a} \\ \mathbf{b} \end{bmatrix} (z, \Omega), \tag{3.11}$$

where:

- ξ_γ is an 8th root of unity,
- $\xi_{z,\gamma} = e(\frac{1}{2} z^t (C\Omega + D)^{-1} C z)$,
- $\xi_{\mathbf{a},\mathbf{b}} = e(-\frac{1}{2} \cdot (\mathbf{a}^t AB^t \mathbf{a} + \mathbf{b}^t CD^t \mathbf{b}) - (A^t \mathbf{a} + C^t \mathbf{b} + \mathbf{e}')^t \mathbf{e}'' - \mathbf{a}^t BC^t \mathbf{b})$,
- $\begin{pmatrix} \mathbf{a}' \\ \mathbf{b}' \end{pmatrix} := (\gamma^t)^{-1} \cdot \begin{pmatrix} \mathbf{a} - \mathbf{e}' \\ \mathbf{b} - \mathbf{e}'' \end{pmatrix}$, where $\mathbf{e}' = \dfrac{1}{2} \operatorname{diag}\left(A^t C\right)$ and $\mathbf{e}'' = \dfrac{1}{2}\left(D^t B\right)$.

Mumford proved the same formula for a congruence subgroup of $\mathbf{Sp}_{2g}(\mathbf{Z})$, i.e., the subgroup $\Gamma_2 = \left\{\gamma \in \mathbf{Sp}_{2g}(\mathbf{Z}) \colon \gamma \equiv I_{2g} \bmod 2\right\}$. We introduce two types of congruence subgroups of $\mathbf{Sp}_{2g}(\mathbf{Z})$ whose action on the theta functions is useful further on. Following Igusa and Mumford, for any positive integer n, we denote by:

$$\Gamma'_n := \left\{\gamma \in \mathbf{Sp}_{2g}(\mathbf{Z}) \colon \gamma \equiv \pm I_{2g} \bmod n\right\},$$

and

$$\Gamma'_{n,2n} := \left\{\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma_n \colon \operatorname{diag}(A^t C) \equiv \operatorname{diag}(B^t D) \equiv 0 \bmod 2n\right\}.$$

It follows from [12, Lem. 6.2.1] that for all $a, b \in \mathbf{Z}(n)$ and for all $\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma'_n$, we have:

$$\frac{\theta \begin{bmatrix} a \\ b \end{bmatrix} (0, \gamma \cdot \Omega)}{\theta \begin{bmatrix} 0 \\ 0 \end{bmatrix} (0, \gamma \cdot \Omega)} = \frac{\theta \begin{bmatrix} a \\ b \end{bmatrix} (0, \Omega)}{\theta \begin{bmatrix} 0 \\ 0 \end{bmatrix} (0, \Omega)} \cdot e\left(\frac{1}{2n^2} a^t D^t B a - \frac{1}{2n^2} b^t A^t C b - \frac{1}{n^2} a^t (A - I_n) b\right). \tag{3.12}$$

It follows that Γ'_n is exactly the group fixing the $2n$-th powers of the theta constants of level (n, n) (modulo a constant), $\Gamma'_{n,2n}$ is the group fixing the n-th powers and $\Gamma'_{n^2,2n^2}$ is the group that fixes the theta constants of level (n, n).

3.1.4 Complex Abelian Surfaces of Dimension 2 with CM

In this section we focus on dimension 2 as the CM theory below is particularly useful in the case of hyperelliptic curves of genus 2 that are the main scope of this thesis. We refer to Shimura [70, Ch. II] for a detailed exposition of the notions below.

A quartic CM field K is a totally imaginary quadratic extension of a real quadratic field K_0. The field K has four complex embeddings $\{\varphi_1, \ldots, \varphi_4\}$. A complex abelian variety X has CM by K if there exists an isomorphism ι between K and the endomorphism algebra of X.

Similarly to Section 3.1.1, the isomorphism ι fixes an analytic representation of an endomorphism of X via $\rho_a \colon \operatorname{End}(X) \to \operatorname{End}_{\mathbf{C}}(V)$ and similarly, a rational representation via $\rho_r \colon \operatorname{End}(X) \to \operatorname{End}_{\mathbf{Z}}(\Lambda)$. By taking the tensor product of the rational representation together with $\mathbf{C}$, we have that $\rho_r \otimes \mathbf{C} \simeq \rho_a \oplus \overline{\rho}_a$ and at the same time, $\rho_r \otimes \mathbf{C} \simeq \oplus_{i=1}^4 \varphi_i$. It follows that $\rho_a = \varphi_1 \oplus \varphi_2$ where φ_1 and φ_2 are two distinct, non-conjugate complex embeddings of K.

Let Φ denote the pair $\{\varphi_1, \varphi_2\}$. We define (K, Φ) as the CM-type of the abelian variety (X, ι). If two complex abelian varieties X, Y have the same CM-type then they are isogenous [70, p.41]. If all complex abelian varieties with CM by (K, Φ) are simple, then their CM-type is called primitive. Moreover, the field K is primitive if there exists an element ξ in K where $K = K_0(\xi)$ such that the imaginary parts of $\varphi_1(\xi), \varphi_2(\xi)$ are positive and $-\xi^2$ is a totally positive element of K_0 [70, p.61].

Let the integer ring of K_0 be $\mathcal{O}_0$. If K_0 has class number 1 then the ring of integers $\mathcal{O}_K$ is an $\mathcal{O}_0$-module of rank 2 of the form $\mathcal{O}_0 + \tau\mathcal{O}_0$, for some $\tau \in K$. Let $\pi \in K$ be a root of the minimal polynomial of $K/\mathbf{Q}$. The endomorphism ring of an ordinary, absolutely simple abelian variety over $\mathbf{C}$ of CM-type (K, Φ) is isomorphic to an order $\mathcal{O}$ of K, such that $\mathbf{Z}[\pi, \overline{\pi}] \subseteq \mathcal{O} \subseteq \mathcal{O}_K$ [79].

In the case of $\mathcal{O} = \mathcal{O}_K$, Taniyama–Shimura [71, 70] proved the following. The isomorphism classes of simple abelian varieties with endomorphism ring $\mathcal{O}_K$ are in bijection with the ideal classes in the Picard group $\operatorname{Pic}(\mathcal{O}_K)$ [71, p.60]. For an ideal class $[\mathfrak{a}] \in \operatorname{Pic}(\mathcal{O}_K)$, we associate a complex torus $V/\Phi(\mathfrak{a})$ where the map $\Phi \colon K \to V$ is defined as $x \mapsto (\varphi_1(x), \varphi_2(x))$ [70, §6]. The dual abelian variety of $V/\Phi(\mathfrak{a})$ is by definition the abelian variety $V/\Phi(\mathfrak{a}^*)$, where $\mathfrak{a}^* = \{\beta \in K | \operatorname{Tr}_{K/\mathbf{Q}}(\beta\mathfrak{a}) \subset \mathbf{Z}\}$. Moreover, we have that $\mathfrak{a}^* = (\overline{\mathfrak{a}}\mathfrak{D}_K)^{-1}$, where $\mathfrak{D}_K \subset \mathcal{O}_K$ is the different ideal [70, p.103].

According to [71, §14.3], a polarization $\mathcal{L}$ on $V/\Phi(\mathfrak{a})$ induces an isogeny $\varphi_{\mathcal{L}} \colon V/\Phi(\mathfrak{a}) \to V/\Phi(\mathfrak{a}^*)$ that is given by $x \mapsto \rho_a(\xi)x$ for some element ξ in $(\mathfrak{a}\overline{\mathfrak{a}}\mathfrak{D}_K)^{-1}$. Moreover the polarization comes from the symplectic form $E(x, y) = \mathrm{Tr}_{K/Q}(\xi\overline{x}y)$. It follows that the abelian variety $V/\Phi(\mathfrak{a})$ is polarizable if and only if there exists $\xi \in K$ with imaginary parts $\mathrm{Im}(\varphi_i(\xi)) > 0$ for $i = 1, 2$. In addition, the polarization is principal if and only if $\varphi_{\mathcal{L}}(\Phi(\mathfrak{a})) = \Phi(\mathfrak{a}^*)$. The latter holds if and only if $\xi\mathfrak{a} = \mathfrak{a}^*$. Conversely, any principal polarization on $V/\Phi(\mathfrak{a})$ is of this form. If $\xi \in K$ yields a principal polarization on $V/\Phi(\mathfrak{a})$, then the other polarizations are of the form $\beta\xi$ for $\beta \in \mathrm{End}(V/\Phi(\mathfrak{a}))^{++}$, i.e., β belongs to the set of totally positive real endomorphisms of $(V/\Phi(\mathfrak{a})$. Indeed if β is totally positive and $\xi\mathfrak{a} = \mathfrak{a}^*$, we get that $\xi\beta \subset \mathfrak{a}^*$, and $\mathrm{Im}(\varphi(\beta\xi)) > 0$. Conversely it is easy to check that if there is a polarization corresponding to the element ξ', then $\beta = \xi'/\xi$ is a totally positive real endomorphism [71, §14.1].

3.1.4.1 Isogenies between Complex Abelian Varieties with CM

We distinguish two main classes of isogenies of abelian varieties with the same CM-type (K, Φ), where K is a quartic CM field.

Definition 3.1.4. A horizontal isogeny $\varphi\colon X \to Y$ is an isogeny between abelian varieties X, Y with the same endomorphism ring $\mathcal{O}$.

Let the group of points $X(\mathbf{C})$ be isomorphic to a complex torus $T = V/\Phi(\mathfrak{a})$, for some ideal $\mathfrak{a} \subset \mathcal{O}_K$, and let $Y(\mathbf{C})$ be isomorphic to a complex torus $T' = V/\Phi(\mathfrak{b})$, for some invertible ideal $\mathfrak{b} \subset \mathcal{O}_K$.

According to [70, §7, Prop.15], if $\mathfrak{c} := \mathfrak{a}\mathfrak{b}^{-1} \subset \mathcal{O}_K$, there exists $\gamma \in \mathfrak{c}^{-1}$ such that the isogeny φ is a $\gamma\mathfrak{c}$-multiplication represented by a diagonal matrix with $\Phi(\gamma)$ on the diagonal. The degree of the isogeny is equal to the norm of the ideal $N_{K/\mathbf{Q}}(\mathfrak{c})$. The dual ideal of $\mathfrak{b}$ is

$$\mathfrak{b}^* = (\mathfrak{a}\mathfrak{c}^{-1})^* = \mathfrak{D}_K^{-1}(\overline{\mathfrak{a}\mathfrak{c}^{-1}})^{-1} = \underbrace{(\mathfrak{D}_K\overline{\mathfrak{a}})^{-1}}_{=\mathfrak{a}^*}\overline{\mathfrak{c}} = \mathfrak{a}^*\overline{\mathfrak{c}}.$$

If $\xi \in K$ corresponds to a polarization on T, then the existence of a principal polarization on T' is equivalent to the existence of $\xi' \in K$ with $\Phi(\xi') \in (i\mathbf{R}_{>0})^2$ such that $\xi'\mathfrak{b} = \mathfrak{a}^*\overline{\mathfrak{c}}$. The latter is equivalent to $\mathfrak{c}\overline{\mathfrak{c}} = (\xi'\xi^{-1})$, i.e., $\mathfrak{c}\overline{\mathfrak{c}}$ is a principal ideal generated by a totally positive element.

Definition 3.1.5. A vertical isogeny is an isogeny between two abelian varieties X and Y with CM-type (K, Φ) such that the endomorphism rings are not isomorphic, i.e., $\mathrm{End}(X) \not\simeq \mathrm{End}(Y)$.

The case of vertical isogenies is a little bit more subtle as we see below. Naturally, the corresponding orders in K, namely $\mathcal{O}_X$ and $\mathcal{O}_Y$ respectively, are not equal. The goal of this paragraph is to deduce the CM description $V/\Phi(\mathfrak{b})$ of Y in terms of the CM description $V/\Phi(\mathfrak{a})$ of X. Without loss of generality, we take the case of a descending isogeny, i.e., $\mathcal{O}_Y \subset \mathcal{O}_X$. Otherwise, in the case of an ascending isogeny, we consider the dual isogeny of the same degree from Y to X. In [25], the authors proved that for any quadratic extension K over a principal ideal domain K_0, any order $\mathcal{O}$ of K that is an $\mathcal{O}_0$ module of rank 2 is of the form $\mathcal{O}_0 + m\tau\mathcal{O}_0$ for some $m \in \mathcal{O}_0^*$ (unique up to multiplication by a unit) and $\tau \in K$ such that $\mathcal{O}_K = \mathcal{O}_0 + \tau\mathcal{O}_0$. The conductor of $\mathcal{O}$ is the principal ideal mO_K. In our case, let $\mathcal{O}_X$ be of conductor $m_a\mathcal{O}_K$ and let $\mathcal{O}_Y$ be of conductor $m_b\mathcal{O}_K$. Then, the vertical isogeny $\varphi\colon X \to Y$ corresponds to the element $m_b/m_a \in \mathcal{O}_0^*$ of norm equal to the degree of the isogeny. For the particular case of a cyclic isogeny of degree ℓ the isogeny corresponds to an element $\beta \in K_0$ of norm ℓ and the ideal $\mathfrak{b} = \mathcal{O}_0 + \beta\mathfrak{m}_a\tau\mathcal{O}_0$. A similar result is given in [35, Prop.5].

3.2 Abelian Varieties over an Arbitrary Field

In this section we consider the case of simple, polarizable abelian varieties of dimension g (regularly denoted by A or B) that are defined over an arbitrary field k. Let $\overline{k}$ denote the algebraic closure of k.

3.2.1 Preliminaries

We introduce some concepts regarding polarized abelian varieties over k, that are analogous to the concepts related to complex tori introduced in Section 3.1. The theory over $\mathbf{C}$ gives us a good intuition of what to expect in the case over k. Moreover, we refer to the end of Section 3.1.1 for definitions related to line bundles on an abelian variety.

An abelian variety A over k of dimension g is a complete connected group variety [55, §1.1]. Let $\mathrm{Pic}(A)$ be the group of isomorphism classes of invertible line bundles. Similarly to the case of complex varieties, we identify the dual abelian variety of A with the group $\mathrm{Pic}^0(A)$ [61, p.77], i.e. the subgroup of isomorphism classes of line bundles $[\mathcal{L}] \in \mathrm{Pic}(A)$, such that for all $x \in A(k)$ there exists an isomorphism $\phi_x \colon \mathcal{L} \to t_x^*\mathcal{L}$.[4] Then, two line bundles $\mathcal{L}$ and $\mathcal{L}'$ on A are *algebraically equivalent* if $\mathcal{L} \otimes \mathcal{L}'^{-1} \in \mathrm{Pic}^0(A)$.

A *polarization* on A is *an ample line bundle*. For any polarization $\mathcal{L}$, there exists an isogeny $\varphi_{\mathcal{L}} \colon A(k) \to \mathrm{Pic}^0(A)$ that sends x to the line bundle $t_x^*\mathcal{L} \otimes \mathcal{L}^{-1}$ on A. The kernel of $\varphi_{\mathcal{L}}$ is denoted by $K(\mathcal{L})$, i.e., the set of closed points x in $A(k)$ such that there exists an isomorphism $\phi_x \colon \mathcal{L} \to t_x^*\mathcal{L}$. The degree of the polarization $\mathcal{L}$ is by definition the degree of the isogeny $\varphi_{\mathcal{L}}$. As in the case of complex abelian varieties, a polarization $\mathcal{L}_0$ of degree 1 is called principal. From now on, we only consider ample line bundles (polarizations) $\mathcal{L}$ on A with $\varphi_{\mathcal{L}}$ separable. Then, there exists an integer $n > 0$ such that there exists a canonical embedding of $(A, \mathcal{L}^n)$ into a projective space of dimension over $\overline{k}$ equal to $n^g - 1$. In this case, the line bundle $\mathcal{L}^n$ is *very ample*.

An invertible line bundle $\mathcal{L}$ on A is called *symmetric* if there exists an isomorphism $\psi \colon \mathcal{L} \to [-1]^*\mathcal{L}$. The Néron-Severi group $\mathrm{NS}(A)$ is identified with the group of isomorphism classes of symmetric line bundles on A up to algebraic equivalence. Given $x \in K(\mathcal{L})$, then ψ induces an isomorphism $\psi(x) \colon \mathcal{L}(x) \to [-1]^*\mathcal{L}(x) = \mathcal{L}(-x)$. The isomorphism ψ is *normalized* if its restriction $\psi(0) \colon \mathcal{L}(0) \to \mathcal{L}(0)$ is the identity. In this case, if we take any 2-torsion element $x \in A[2]$ $(x = -x)$ of $K(\mathcal{L})$, then the map $\psi(x) \circ \psi(-x)$ is the identity. Therefore, $\psi(x)$ acts as multiplication by ± 1. The line bundle $\mathcal{L}$ is called *totally symmetric* if $\psi(x)$ is the identity for all $x \in A[2]$.

Next, given an integer $r > 1$, we define a polarization on the r-fold product of an abelian variety A that is determined by $\mathcal{L}$ on A of type δ.

Definition 3.2.1. Given the polarized abelian variety $(A, \mathcal{L})$, consider the line bundle on A^r of the form

$$\mathcal{L}^{\star r} = p_1^*\mathcal{L} \otimes \cdots \otimes p_r^*\mathcal{L},$$

where $p_i \colon A^r \to A$ is the projection to the ith factor.

A polarization (or ample line bundle) $\mathcal{L}'$ on the r-fold product A^r is called an r-fold product polarization if $\mathcal{L}'$ is isomorphic to $p_1^*\mathcal{L} \otimes \cdots \otimes p_r^*\mathcal{L}$ for some polarization $\mathcal{L}$ on A.

[4] t_x represents translation by x.

3.2.2 The Mumford Theta Group and Theta Structures

Similarly to the case of complex abelian varieties we find means of embedding the variety into some suitable projective space over $\overline{k}$. The final goal is to define maps on the projective space that correspond to the operations on the abelian variety itself. To obtain that, we first want an alternative to the concept of theta functions of level n. Moreover, given a polarization $\mathcal{L}$ on the abelian variety A, we define the embedding map into the projective space in terms of a particular class representative for $[\mathcal{L}] \in \mathrm{Pic}(\mathcal{L})$.

We proceed by introducing some very useful definitions that will allow us to define the apparatus for constructing the embedding map later on. The theory below is due to Mumford and we refer to [60] for a more detailed exposition.

Let $(A, \mathcal{L})$ be a polarized abelian variety of dimension g. The *Mumford theta group* associated to the line bundle $\mathcal{L}$ is the group $\mathcal{G}(\mathcal{L})$ of pairs (x, ϕ_x), where $x \in K(\mathcal{L})$ and $\phi_x \colon \mathcal{L} \to t_x^*\mathcal{L}$ is an isomorphism. The group law is given by:

$$(x, \phi_x) \cdot (y, \phi_y) = (x + y, t_x^*\phi_y \circ \phi_x),$$

for any pairs (x, ϕ_x), $(y, \phi_y) \in \mathcal{G}(\mathcal{L})$. There exists an exact sequence

$$0 \to \overline{k}^\times \to \mathcal{G}(\mathcal{L}) \to K(\mathcal{L}) \to 0,$$

with the natural projection of $\mathcal{G}(\mathcal{L})$ onto $K(\mathcal{L})$ being the surjective map of kernel the automorphisms of $\mathcal{L}(0)$, i.e., multiplications by elements of $\overline{k}^\times$.

An ample line bundle $\mathcal{L}$ on A induces a non-degenerate commutator pairing $e_{\mathcal{L}} \colon K(\mathcal{L}) \times K(\mathcal{L}) \to \overline{k}^\times$, i.e., $e_{\mathcal{L}}$ is a skew-symmetric bilinear form, defined as follows

$$e_{\mathcal{L}}(x, y) = (x, \phi_x) \cdot (y, \phi_y) \cdot (x, \phi_x)^{-1}.(y, \phi_y)^{-1},$$

where $(x, \phi_x), (y, \phi_y) \in \mathcal{G}(\mathcal{L})$ are arbitrary lifts of x and y respectively. One can prove easily that the commutator pairing is well defined.

With respect to $e_{\mathcal{L}}$, there exists a symplectic decomposition of $K(\mathcal{L}) = K_1(\mathcal{L}) \oplus K_2(\mathcal{L})$ into maximal isotropic subspaces. Following the theorem of elementary divisors for the abelian group $K_1(\mathcal{L})$, there exist elementary divisors $d_1 \mid d_2 \mid \cdots \mid d_g$ of $K_1(\mathcal{L})$, i.e., $K_1(\mathcal{L})$ is isomorphic to $\mathbf{Z}(\delta)$, for $\mathbf{Z}(\delta) = \bigoplus_{i=1}^r \mathbf{Z}/d_i\mathbf{Z}$. In this case, the ample line bundle $\mathcal{L}$ is said to be of type $\delta = (d_1, \dots, d_g)$. Moreover, $K_2(\mathcal{L})$ is isomorphic to the dual group $\widehat{\mathbf{Z}}(\delta)$, namely the group of homomorphisms in $\mathrm{Hom}(\mathbf{Z}(\delta), \overline{k}^\times)$. Let $K(\delta) := \mathbf{Z}(\delta) \oplus \widehat{\mathbf{Z}}(\delta)$, then one can define the standard pairing $e_\delta \colon K(\delta) \times K(\delta) \to \overline{k}_p^\times$ given by:

$$e_\delta((x_1, y_1), (x_2, y_2)) = \frac{y_2(x_1)}{y_1(x_2)},$$

for $x_1, x_2 \in \mathbf{Z}(\delta)$ and $y_1, y_2 \in \widehat{\mathbf{Z}}(\delta)$. Let $H(\delta)$ denote the Heisenberg group of δ, namely the group of elements in $\overline{k}^\times \times \mathbf{Z}(\delta) \times \widehat{\mathbf{Z}}(\delta)$ with group law:

$$(\alpha_1, x_1, y_1) \cdot (\alpha_2, x_2, y_2) = (\alpha_1\alpha_2 y_2(x_1), x_1 + x_2, y_1 + y_2).$$

There is a canonical map $s_\delta \colon K(\delta) \to H(\delta)$ given by $(x, y) \mapsto (1, x, y)$.

Definition 3.2.2. A theta structure $\Theta_{\mathcal{L}}$ of type δ on the polarized abelian variety $(A, \mathcal{L})$ is by definition an isomorphism

$$\Theta_{\mathcal{L}}\colon H(\delta) \to \mathcal{G}(\mathcal{L})$$

that is the identity on $\overline{k}^{\times}$.

There is an induced symplectic isomorphism $\overline{\Theta}_{\mathcal{L}}\colon K(\delta) \to K(\mathcal{L})$ such that the following diagram is commutative:

$$\begin{tikzcd}
0 \arrow[r] & \overline{k}^{\times} \arrow[r] \arrow[d, "="'] & H(\delta) \arrow[r] \arrow[d, "\Theta_{\mathcal{L}}"'] & K(\delta) \arrow[r] \arrow[d, "\overline{\Theta}_{\mathcal{L}}"'] & 0 \\
0 \arrow[r] & \overline{k}^{\times} \arrow[r] & \mathcal{G}(\mathcal{L}) \arrow[r] & K(\mathcal{L}) \arrow[r] & 0
\end{tikzcd}$$

Now, we define a theta structure on $(A^r, \mathcal{L}^{\star r})$ given the theta structure $\Theta_{\mathcal{L}}$ of type $\delta = (d_1, \ldots, d_g)$. First we notice that the type of $\mathcal{L}^{\star r}$ is of the form

$$\delta^{\star r} = \left(\underbrace{d_1, \ldots, d_1}_{r}, \underbrace{d_2, \ldots, d_2}_{r}, \ldots, \underbrace{d_g, \ldots, d_g}_{r} \right) \in \mathbf{Z}(\delta)^r.$$

Definition 3.2.3. By definition, the r-fold product theta structure $\Theta_{\mathcal{L}^{\star r}}\colon H(\delta^{\star r}) \to \mathcal{G}(\mathcal{L}^{\star r})$ is the theta structure of type $\delta^{\star r}$ that maps

$$(x_1, \ldots, x_r, y_1, \ldots, y_r, \alpha) \in H(\delta^{\star r}) \to (z_1, \ldots, z_r, \phi_z) \in \mathcal{G}(\mathcal{L}^{\star r})$$

where on each factor $i = 1, \ldots, r$, we have $\Theta_{\mathcal{L}}(x_i, y_i, \alpha) = (z_i, \phi_i)$, where $z = (z_1, \ldots, z_r) \in (K(\mathcal{L}))^r$ and $\phi_i\colon \mathcal{L} \xrightarrow{\sim} z_i^* \mathcal{L}$ induce an isomorphism $\phi\colon \mathcal{L}^{\star r} \to t_z^* \mathcal{L}^{\star r}$.

Now, we present several useful properties of theta structures. Given the theta structure $\Theta_{\mathcal{L}}$, there exists a map $s_{K(\mathcal{L})}$ of $K(\mathcal{L})$ into $\mathcal{G}(\mathcal{L})$ corresponding to the canonical map $s_\delta\colon K(\delta) \to H(\delta)$ that was introduced before. When restricted to the two isotropic subgroups, the maps $s_{K_1(\mathcal{L})}\colon K_1(\mathcal{L}) \to \mathcal{G}(\mathcal{L})$ and $s_{K_2(\mathcal{L})}\colon K_2(\mathcal{L}) \to \mathcal{G}(\mathcal{L})$ are group sections.

Following [66, Prop.3.3.3], given a symplectic isomorphism $\overline{\Theta}_{\mathcal{L}}\colon K(\delta) \to K(\mathcal{L})$ together with two group sections $s_{K_1(\mathcal{L})}$, $s_{K_2(\mathcal{L})}$ as above, there exists a unique theta structure $\Theta_{\mathcal{L}}$ above $\overline{\Theta}_{\mathcal{L}}$ inducing the two sections $s_{K_1(\mathcal{L})}$ and $s_{K_2(\mathcal{L})}$. In particular, given any symplectic isomorphism $\overline{\Theta}_{\mathcal{L}}\colon K(\delta) \to K(\mathcal{L})$, there is a theta structure $\Theta_{\mathcal{L}}$ above that isomorphism.

We fix a theta structure above $\overline{\Theta}_{\mathcal{L}}$ for the case of a totally symmetric line bundle $\mathcal{L}$ as follows. First, we consider an isomorphism $\psi\colon \mathcal{L} \xrightarrow{\sim} [-1]^* \mathcal{L}$ that is normalized at 0. Next, we define an automorphism of the theta group that allows the introduction of a symmetric theta structure. Let $\gamma_{-1}\colon \mathcal{G}(\mathcal{L}) \to \mathcal{G}(\mathcal{L})$ be given by:

$$\gamma_{-1}(x, \phi_x) = \left(-x, (t_{-x}^* \psi)^{-1} \circ ([-1]^* \phi_x) \circ \psi\right).$$

Immediately, the following diagram commutes

$$\begin{tikzcd}
0 \arrow[r] & \overline{k}^{\times} \arrow[r] \arrow[d, "="'] & \mathcal{G}(\text{Ł}) \arrow[r] \arrow[d, "\gamma_{-1}"'] & K(\mathcal{L}) \arrow[r] \arrow[d, "-1"'] & 0 \\
0 \arrow[r] & \overline{k}^{\times} \arrow[r] & \mathcal{G}(\mathcal{L}) \arrow[r] & K(\mathcal{L}) \arrow[r] & 0
\end{tikzcd}$$

and $\gamma_{-1} \circ \gamma_{-1}$ is the identity. As a consequence, given $x \in K(\mathcal{L})$, there exist two elements $(x, \phi_x), (x, \phi_x)^{-1}$ in $\mathcal{G}(\mathcal{L})$ above x with $\gamma_{-1}((x, \phi_x)) = (x, \phi_x)^{-1}$.

There exists a similar automorphism $\gamma_{-1}\colon H(\delta) \to H(\delta)$ of the Heisenberg group given by $\gamma_{-1}(\alpha, x, y) = (\alpha, -x, -y)$. A theta structure $\Theta_{\mathcal{L}}$ on the polarized abelian variety $(A, \mathcal{L})$ is called *symmetric* if it satisfies $\gamma_{-1} \circ \Theta_{\mathcal{L}} = \Theta_{\mathcal{L}} \circ \gamma_{-1}$.

3.2.2.1 Theta Coordinates

Having introduced theta structures in the previous section, we are able to adapt the theory from Section 3.1.2.1 to the case of principally polarized abelian varieties defined over an arbitrary field k. More precisely, we consider a principally polarized abelian variety $(A, \mathcal{L}_0)$ over k together with a totally symmetric line bundle $\mathcal{L} \simeq \mathcal{L}_0^{\otimes n}$, where $n \geq 2$ is even. Let the type of $\mathcal{L}$ be $\delta = (n, \ldots, n) \in \mathbf{Z}^g$. If $\varphi_{\mathcal{L}}$ is of degree $n \geq 3$, then $\mathcal{L}$ is very ample and so, there exists an embedding of A into the projective space $\mathbf{P}(\Gamma(A, \mathcal{L}))$ (embedding unique up to multiplication by an element in $\mathbf{PGL}(\Gamma(A, \mathcal{L}))$. In order to fix a projective embedding, we need to define the analogue to the Riemann theta functions of level n, namely we need to fix a basis for the space of global sections $\Gamma(A, \mathcal{L})$.

For that we consider a symmetric theta structure $\Theta_{\mathcal{L}}\colon H(\delta) \to \mathcal{G}(\mathcal{L})$. Let $K(\delta)$ be decomposed as $K_1(\delta) \oplus K_2(\delta)$ with respect to the standard commutator pairing e_δ and let $V(\delta)$ be the space of functions $\{f\colon K_1(\delta) \to k\}$. According to [66, p.50], the theta structure $\Theta_{\mathcal{L}}$ induces an isomorphism $\rho\colon V(\delta) \to \Gamma(A, \mathcal{L})$. The isomorphism ρ is unique up to multiplication by a constant and identifies the irreducible action of the Heisenberg group $H(\delta)$ on $V(\delta)$ with the action of the theta group $\mathcal{G}(\mathcal{L})$ on $\Gamma(A, \mathcal{L})$. The action of $(x, \phi_x) \in \mathcal{G}(\mathcal{L})$ on $s \in \Gamma(A, \mathcal{L})$ is given by

$$(x, \phi_x) \cdot s = t_{-x}^* \phi_x(s)$$

Consider the canonical basis $\{\gamma_i | i \in \mathbf{Z}(\delta)\}$ of $V(\delta)$, where $\gamma_i\colon \mathbf{Z}(\delta) \to \{0, 1\}$ is the Kronecker function, i.e. $\gamma_i(j) = 1$ if and only if $i = j$. By definition, the image

$$(\theta_i^{\Theta_{\mathcal{L}}})_{i \in \mathbf{Z}(\delta)} := (\rho(\gamma_i))_{i \in \mathbf{Z}(\delta)}$$

is the canonical basis of $\Gamma(A, \mathcal{L})$. The basis elements are uniquely determined up to multiplication by a constant in k^* [66, p.50].

Remark 7. From now on, the index i of the theta coordinates of a point belongs either to $K_1(\mathcal{L})$, or to $K_1(\delta) = \mathbf{Z}(\delta)$.

Hence, we are able to give the following definition:

Definition 3.2.4. Let $(A, \mathcal{L}_0)$ be a principally polarized abelian variety. Consider a polarization $\mathcal{L}$ of type

$\delta = (d_1, \dots, d_g)$ with $2|d_1$. Given a theta structure $\Theta_{\mathcal{L}}$ on $(A, \mathcal{L})$ and an isomorphism $\rho\colon V(\delta) \to \Gamma(A, \mathcal{L})$, the projective theta coordinates of a point $x \in A$ are the image $(\theta_i^{\Theta_{\mathcal{L}}}(x))_{i \in K_1(\mathcal{L})} \in \mathbf{P}(\Gamma(A, \mathcal{L}))$ with respect to the canonical basis $(\theta_i^{\Theta_{\mathcal{L}}})_{i \in K_1(\mathcal{L})}$.

Moreover, if $d_1 = \ldots = d_g$, we say that both the theta structure $\Theta_{\mathcal{L}}$ and the projective theta coordinates of a point x are of level n.

3.2.3 Compatible Theta Structures and the Action of Symplectic Isomorphisms

Let $\mathcal{L}$ be a totally symmetric line bundle on A of type δ. We denote the type of $\mathcal{L}^2$ as 2δ. Let $\Theta_{\mathcal{L}}$ and $\Theta_{\mathcal{L}^2}$ be two symmetric theta structures on A. In order to define the notion of compatible theta structures, we first introduce several necessary homomorphisms defined by Mumford in [60, p.309-310].

First, let $\epsilon_2\colon \mathcal{G}(\mathcal{L}) \to \mathcal{G}(\mathcal{L}^2)$ be a homomorphism given by:

$$\epsilon_2(x, \phi_x) = \left(x, \phi_x^{\otimes 2}\right),$$

where $x \in K(\mathcal{L}) \subset K(\mathcal{L}^2)$ and $\phi_x^{\otimes 2}\colon \mathcal{L}^2 \to t_x^* \mathcal{L}^2$. Second, let $\psi\colon \mathcal{L}^4 \to [2]^*\mathcal{L}$ and let $\eta_2\colon \mathcal{G}(\mathcal{L}^2) \to \mathcal{G}(\mathcal{L})$ be a homomorphism given by:

$$\eta_2(x, \phi_x) = (2x, \rho)$$

where $\rho\colon \mathcal{L} \to t_{2x}^* \mathcal{L}$ is the unique isomorphism such that $[2]^*\rho = t_x^*\psi \circ \phi_x^{\otimes 2} \circ \psi^{-1}$.

Immediately, the following diagrams commute

$$\begin{tikzcd}
0 \arrow[r] & \overline{k}^{\times} \arrow[r] \arrow[d, "squaring"'] & \mathcal{G}(\text{Ł}) \arrow[r] \arrow[d, "\epsilon_2"'] & K(\mathcal{L}) \arrow[r] \arrow[d, hook, "\text{inclusion}"] & 0 \\
0 \arrow[r] & \overline{k}^{\times} \arrow[r] & \mathcal{G}(\mathcal{L}^2) \arrow[r] & K(\mathcal{L}^2) \arrow[r] & 0
\end{tikzcd}$$

and

$$\begin{tikzcd}
0 \arrow[r] & \overline{k}^{\times} \arrow[r] \arrow[d, "squaring"'] & \mathcal{G}(\text{Ł}^2) \arrow[r] \arrow[d, "\eta_2"'] & K(\mathcal{L}^2) \arrow[r] \arrow[d, "\texttt{doubling}"] & 0 \\
0 \arrow[r] & \overline{k}^{\times} \arrow[r] & \mathcal{G}(\mathcal{L}) \arrow[r] & K(\mathcal{L}) \arrow[r] & 0
\end{tikzcd}$$

Mumford defines also similar maps over the Heisenberg groups. First, let $E_2\colon H(\delta) \to H(2\delta)$ be of the form $E_2((\alpha, x, y)) = (\alpha^2, x, y')$ where $y' \in \hat{K}(2\delta)$ is a unique element such that $y'(x) = y(2x)$ for all $x \in K(2\delta)$. Second, let $D_2\colon H(2\delta) \to H(\delta)$ be given by $N_2((\alpha, x, y)) = (\alpha^2, 2x, \overline{y})$, where $\overline{y}$ is the canonical image of y in $\hat{K}(\delta)$.

By definition [60, p.317], a compatible pair of theta structures $\Theta_{\mathcal{L}}$ and $\Theta_{\mathcal{L}^2}$ for the line bundle $\mathcal{L}$ and $\mathcal{L}^2$ respectively satisfy:

$$\begin{aligned}
\Theta_{\mathcal{L}^2}^{-1} \circ \epsilon_2 &= E_2 \circ \Theta_{\mathcal{L}}^{-1} \\
\Theta_{\mathcal{L}}^{-1} \circ \eta_2 &= N_2 \circ \Theta_{\mathcal{L}^2}^{-1}.
\end{aligned} \tag{3.13}$$

We denote by $\overline{\epsilon}_2 \colon K(\mathcal{L}) \to K(\mathcal{L}^2)$ and $\overline{E}_2 \colon K(\delta) \to K(2\delta)$ the inclusion maps that are restrictions of ϵ_2 and E_2 respectively. Similarly, let $\overline{\eta}_2 \colon K(\mathcal{L}^2) \to K(\mathcal{L})$ and $\overline{N}_2 \colon K(2\delta) \to K(\delta)$ denote the other corresponding maps. The map η_2 is surjective and its kernel consists of the 2-torsion points $\mathcal{G}(\mathcal{L})[2]$ (equal to $\mathcal{G}(\mathcal{L})$ when the type of $\mathcal{L}$ is 4). Hence, there exists an induced isomorphism $\mathcal{G}(\mathcal{L}) \to \mathcal{G}(\mathcal{L}^2)/\mathcal{G}(\mathcal{L})[2]$. Similarly, N_2 is also surjective and gives an isomorphism of $\mathcal{G}(\delta) \to \mathcal{G}(2\delta)/\mathcal{G}(\delta)[2]$. This argument [60, p.318] proves that given a theta structure $\Theta_{\mathcal{L}^2}$ of level 4 and the doubling functions η_2 and N_2, one can deduce a unique theta structure $\Theta_{\mathcal{L}}$ of level 2.

A stronger result is proved by Mumford [60, p.319] and Robert [66, Prop. 4.3.1]:

Lemma 3.2.5. *For a principally polarized abelian variety $(A, \mathcal{L}_0)$ of dimension g, with a totally symmetric line bundle $\mathcal{L} = \mathcal{L}_0^2$, it is sufficient to have a symplectic isomorphism $\overline{\Theta} \colon K(\mathcal{L}^2) \to K(2\delta)$ that is compatible with a symplectic isomorphism of $K(\mathcal{L}) \to K(\delta)$ in order to fix a unique symmetric theta structure of level 2 corresponding to the two isomorphisms and coming from any theta structure of level 4 that induces $\overline{\Theta}$.*

Here, the compatibility between isomorphisms $K(\mathcal{L}) \to K(\delta)$ and $K(\mathcal{L}^2) \to K(2\delta)$ signifies that the first and second relation in (3.13) hold for the restriction maps $\overline{\eta}_2, \overline{N}_2, \overline{\epsilon}_2, \overline{E}_2$ and the given pair of isomorphisms.

3.2.3.1 Transformation Formula of a Symplectic Automorphism

We consider a principally polarized abelian variety $(A, \mathcal{L}_0)$ of dimension g, with a totally symmetric line bundle $\mathcal{L} = \mathcal{L}_0^2$ and a level 2 symmetric theta structure $\Theta_{\mathcal{L}}$ coming from a symplectic decomposition of the 4-torsion points $\overline{\Theta} \colon K(2\delta) \to K(\mathcal{L}^2)$ (see Lemma 3.2.5). We fix a symplectic basis of $K(2\delta)$ with respect to $\overline{\Theta}$ and consider a symplectic automorphism S acting on $K(2\delta)$ that induces an automorphism of $K_1(2\delta)$.

The goal is to find an analogue formula to (3.11) for a general automorphism S. Notice that the formula over $\mathbf{C}$ can be easily written in case of level $(2,2)$ Riemann theta functions for both isomorphic tori. In case of a matrix representation of S with rational vectors $\mathbf{e}', \mathbf{e}''$, working with level 4 seems to be the immediate choice.

First, we identify $K(2\delta) \simeq \mathbf{Z}(4) + \mathbf{Z}(4)$ via an isomorphism. Let $\mathbf{Z}(2,2) := \left(\frac{1}{2}\mathbf{Z}^g/\mathbf{Z}^g\right)^2$, consider a bijection map $\upsilon \colon \mathbf{Z}(2,2) \times \mathbf{Z}(2,2) \to K(2\delta)$ and let

$$\kappa = \overline{\Theta} \circ \upsilon \colon \mathbf{Z}(2,2) \times \mathbf{Z}(2,2) \to K(\mathcal{L}^2).$$

Let $\overline{\Theta}' = \overline{\Theta} \circ S$ be the new symplectic isomorphism. Consider the bijection map $\kappa' = \overline{\Theta}' \circ \upsilon \colon \mathbf{Z}(2,2) \times \mathbf{Z}(2,2) \to K(\mathcal{L}^2)$. Let $\overline{S} \in \mathbf{Sp}_{2g}(\mathbf{Z})$ be the matrix representation of the symplectic isomorphism S acting on $\mathbf{Z}(2,2)$ (induced by κ, κ') and write $\overline{S} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ for some matrices a, b, c, d.

The theta coordinates of the new theta structure $\Theta'_{\mathcal{L}}$ of level 2 corresponding to $\overline{\Theta}'$ [60, p.319] are computed for each point $S \cdot z$ as follows (z and $S \cdot z$ represent the same point, but for two different theta structures). First, the level 2 theta structure $\Theta_{\mathcal{L}}$ determines the squares of level 4 theta coordinates for any compatible level 4 theta structure $\Theta_{\mathcal{L}^2}$ (in the sense of lemma 3.2.5). The same statement holds for $\Theta'_{\mathcal{L}}$ and any compatible level 4 theta structure $\Theta'_{\mathcal{L}^2}$. Hence, we write the analogue of (3.11) for the squares of level 4 algebraic theta coordinates.

There exists a constant λ such that for every $\mathbf{u}, \mathbf{v}, \mathbf{u}', \mathbf{v}' \in \frac{1}{2}\mathbf{Z}^g/\mathbf{Z}^g$, with $\begin{pmatrix} \mathbf{u} \\ \mathbf{v} \end{pmatrix} = \begin{pmatrix} a & c \\ b & d \end{pmatrix}^{-1} \cdot \begin{pmatrix} \mathbf{u}' - \mathbf{e}' \\ \mathbf{v}' - \mathbf{e}'' \end{pmatrix}$, with $\mathbf{e}' = \frac{1}{2}\operatorname{diag}(a^t c)$ and $\mathbf{e}'' = \frac{1}{2}\operatorname{diag}(d^t b)$ and

$$\xi_{\mathbf{u},\mathbf{v}} = e\left(-\frac{1}{2} \cdot (\mathbf{u}^t a b^t \mathbf{u} + \mathbf{v}^t c d^t \mathbf{v}) - (a^t \mathbf{u} + c^t \mathbf{v} + \mathbf{e}')^t \mathbf{e}'' - \mathbf{u}^t b c^t \mathbf{v}\right),$$

we have

$$\left(\theta^{\Theta'_{\mathcal{L}^2}}_{\kappa'(\mathbf{u}',\mathbf{v}')}(z)\right)^2 = \lambda \cdot \xi^2_{\mathbf{u},\mathbf{v}} \cdot \left(\theta^{\Theta_{\mathcal{L}^2}}_{\kappa(\mathbf{u},\mathbf{v})}(z)\right)^2. \tag{3.14}$$

Since we are given the symplectic isomorphism $\overline{\Theta}$, we are also given a symplectic basis of $K_1(\mathcal{L})$ and its abstract representation in $\mathbf{Z}(2)$. Then, any index $\mathbf{i} \in \frac{1}{2}\mathbf{Z}^g/\mathbf{Z}^g$ is identified with $2\mathbf{i} \in \mathbf{Z}(2)$ (via an isomorphism) and a unique element in $K_1(\mathcal{L})$ (via $\overline{\Theta}$). We denote by $\mu\colon \frac{1}{2}\mathbf{Z}^g/\mathbf{Z}^g \to K_1(\mathcal{L})$. Similarly, we denote by $\mu'\colon \frac{1}{2}\mathbf{Z}^g/\mathbf{Z}^g \to K_1(\mathcal{L})$ the isomorphism corresponding to $\overline{\Theta}'$.

The projective theta coordinates of level 2 of $z \in A$, that correspond to $\Theta_{\mathcal{L}}$ are denoted by $\theta^{\Theta_{\mathcal{L}}}_{\mu(\mathbf{u})}(z)$ for $\mathbf{u} \in \frac{1}{2}\mathbf{Z}^g/\mathbf{Z}^g$. The new theta coordinates of level 2, that correspond to the new $\Theta'_{\mathcal{L}}$ are denoted by $\theta^{\Theta'_{\mathcal{L}}}_{\mu'(\mathbf{u})}(z)$ for $\mathbf{u} \in \frac{1}{2}\mathbf{Z}^g/\mathbf{Z}^g$. The new theta coordinates are linked to the squares of level 4 theta coordinates from (3.14), via [12, eq.(3.12–13)]:

$$\theta^{\Theta'_{\mathcal{L}}}_{\mu'(\mathbf{v}')}(z)\theta^{\Theta'_{\mathcal{L}}}_{\mathbf{0}}(0) = \sum_{\mathbf{u}' \in \frac{1}{2}\mathbf{Z}^g/\mathbf{Z}^g} \left(\theta^{\Theta'_{\mathcal{L}^2}}_{\kappa'(\mathbf{u}',\mathbf{v}')}(z)\right)^2 \tag{3.15}$$

and

$$\left(\theta^{\Theta'_{\mathcal{L}^2}}_{\kappa'(\mathbf{u},\mathbf{v})}(z)\right)^2 = \frac{1}{2^g} \sum_{\mathbf{i} \in \left(\frac{1}{2}\mathbf{Z}/\mathbf{Z}\right)^g} e(-2\mathbf{u}^t \mathbf{i})\theta^{\Theta'_{\mathcal{L}}}_{\mu'(\mathbf{v}+\mathbf{i})}(z)\theta^{\Theta'_{\mathcal{L}}}_{\mu'(\mathbf{i})}(0). \tag{3.16}$$

We first apply (3.15) and afterwards (3.14) (where we compute parameters $\mathbf{u}, \mathbf{v}$ for given indexes $\mathbf{u}', \mathbf{v}' \in \frac{1}{2}\mathbf{Z}^g/\mathbf{Z}^g$). In the end, we use (3.15) to go back to theta coordinates of level 2 for the theta structure $\Theta_{\mathcal{L}}$. We obtain:

$$\begin{aligned} \theta^{\Theta'_{\mathcal{L}}}_{\mu'(\mathbf{v}')}(z)\theta^{\Theta'_{\mathcal{L}}}_{\mathbf{0}}(0) &= \sum_{\mathbf{u}' \in \frac{1}{2}\mathbf{Z}^g/\mathbf{Z}^g} \left(\theta^{\Theta'_{\mathcal{L}^2}}_{\kappa'(\mathbf{u}',\mathbf{v}')}(z)\right)^2 \\ &= \sum_{\mathbf{u}' \in \frac{1}{2}\mathbf{Z}^g/\mathbf{Z}^g} \lambda \cdot \xi^2_{\mathbf{u},\mathbf{v}} \left(\theta^{\Theta_{\mathcal{L}^2}}_{\kappa(\mathbf{u},\mathbf{v})}(z)\right)^2 \\ &= \frac{\lambda}{2^g} \sum_{\mathbf{u}' \in \frac{1}{2}\mathbf{Z}^g/\mathbf{Z}^g} \xi^2_{\mathbf{u},\mathbf{v}} \sum_{\mathbf{i} \in \frac{1}{2}\mathbf{Z}^g/\mathbf{Z}^g} e(-2\mathbf{u}^t \mathbf{i})\theta^{\Theta_{\mathcal{L}}}_{\mu(\mathbf{b}+\mathbf{i})}(z)\theta^{\Theta_{\mathcal{L}}}_{\mu(\mathbf{i})}(0). \end{aligned} \tag{3.17}$$

We summarize in the following proposition:

Proposition 3.2.6. *Consider a principally polarized abelian variety $(A, \mathcal{L})$ with a level 2 theta structure $\Theta_{\mathcal{L}}$ coming from a symplectic decomposition of the 4-torsion points $\overline{\Theta}\colon K(2\delta) \to K(\mathcal{L}^2)$. Let S be a symplectic automorphism acting on $K(2\delta)$. Consider the isomorphism $\mu\colon \frac{1}{2}\mathbf{Z}^g/\mathbf{Z}^g \to K_1(\mathcal{L})$ corresponding* *to $\overline{\Theta}$.*

Then, there exists a unique metaplectic automorphism in $\mathrm{Aut}(H(\delta))$ *corresponding to S such that the new theta structure $\Theta'_{\mathcal{L}}$ of level 2 comes from $\overline{\Theta}' = \overline{\Theta} \circ S$. Consider the isomorphism $\mu' \colon \frac{1}{2}\mathbf{Z}^g/\mathbf{Z}^g \to K_1(\mathcal{L})$ that is corresponding to $\overline{\Theta}'$. Let $\mathbf{e}' = \frac{1}{2}\,\mathrm{diag}(a^t c)$ and $\mathbf{e}'' = \frac{1}{2}\,\mathrm{diag}(d^t b)$. There exists a constant λ for which the new theta coordinates are*

$$\theta^{\Theta'_{\mathcal{L}}}_{\mu'(\mathbf{v}')}(z)\theta^{\Theta'_{\mathcal{L}}}_{\mathbf{0}}(0) \quad = \quad \frac{\lambda}{2^g} \sum_{\mathbf{u}' \in \frac{1}{2}\mathbf{Z}^g/\mathbf{Z}^g} \xi^2_{\mathbf{u},\mathbf{v}} \sum_{\mathbf{i} \in \frac{1}{2}\mathbf{Z}^g/\mathbf{Z}^g} e(-2\mathbf{u}^t\mathbf{i})\theta^{\Theta_{\mathcal{L}}}_{\mu(\mathbf{b}+\mathbf{i})}(z)\theta^{\Theta_{\mathcal{L}}}_{\mu(\mathbf{i})}(0) \tag{3.18}$$

where $\mathbf{u}, \mathbf{v}, \mathbf{u}', \mathbf{v}' \in \frac{1}{2}\mathbf{Z}^g/\mathbf{Z}^g$ *such that* $\begin{pmatrix}\mathbf{u}\\ \mathbf{v}\end{pmatrix} = \begin{pmatrix}a & c\\ b & d\end{pmatrix}^{-1} \cdot \begin{pmatrix}\mathbf{u}' - \mathbf{e}'\\ \mathbf{v}' - \mathbf{e}''\end{pmatrix}$, *and*

$$\xi_{\mathbf{u},\mathbf{v}} = e\left(-\frac{1}{2} \cdot (\mathbf{u}^t ab^t\mathbf{u} + \mathbf{v}^t cd^t\mathbf{v}) - (a^t\mathbf{u} + c^t\mathbf{v} + \mathbf{e}')^t\mathbf{e}'' - \mathbf{u}^t bc^t\mathbf{v}\right).$$

3.2.4 The Isogeny Theorem for Symmetric Theta Structures

Consider an isogeny of polarized abelian varieties $f \colon (A, \mathcal{L}) \to (B, \mathcal{M})$ over k that has kernel G. By definition, the line bundles $f^*\mathcal{M}$ and $\mathcal{L}$ are algebraically equivalent. Moreover, according to [66, Prop.4.2.12], if $\mathcal{L}$ is a totally symmetric line bundle, then there exists a symmetric line bundle $\mathcal{M}$ in the algebraic equivalence class of the polarization on B with $f^*\mathcal{M}$ isomorphic to $\mathcal{L}$. Let $K(\mathcal{L})$ be the kernel of the isogeny $\varphi_{\mathcal{L}} \colon A \to A^\vee$.

In this section, we first focus on a condition for $G \subset K(\mathcal{L})$ (with respect to $\mathcal{L}$) that is necessary for f to be an isogeny of polarized abelian varieties. More precisely, G needs to be a maximal isotropic subgroup of $K(\mathcal{L})$ with respect to the commutator pairing $e_{\mathcal{L}}$. First, if $\alpha \colon f^*\mathcal{M} \xrightarrow{\sim} \mathcal{L}$ is fixed, then for each $x \in G$ there exists an isomorphism $\phi_x \colon \mathcal{L} \to t_x^*\mathcal{L}$ of the form:

$$\mathcal{L} \xrightarrow{\alpha^{-1}} f^*\mathcal{M} = (f \circ t_x)^*\mathcal{M} = t_x^*(f^*\mathcal{M}) \xrightarrow{t_x^*\alpha} t_x^*\mathcal{L},$$

and hence $G \subset K(\mathcal{L})$.

Consider a lift of the form $(x, \phi_x) \in \mathcal{G}(\mathcal{L})$ for any $x \in G$. The set of all such elements (x, ϕ_x) above all $x \in G$ form a subgroup $\widetilde{G}$ of $\mathcal{G}(\mathcal{L})$, called a level subgroup. Moreover, $\widetilde{G}$ is isomorphic to G via the projection map $\mathcal{G}(\mathcal{L}) \to K(\mathcal{L})$ and there exists a 1-to-1 correspondence between level subgroups $\widetilde{G}$ and pairs (f, α), and consequently line bundles $\mathcal{M}$ on B. Let $\mathcal{Z}(\widetilde{G})$ denote the centralizer of $\widetilde{G}$ in the group $\mathcal{G}(\mathcal{L})$. According to [60, Thm. 3.2.2], the theta group $\mathcal{G}(\mathcal{M})$ is isomorphic to $\mathcal{Z}(\widetilde{G})/\widetilde{G}$. Let $\alpha_f \colon \mathcal{Z}(\widetilde{G}) \to \mathcal{G}(\mathcal{M})$ be the morphism induced by this isomorphism.

The data of $\widetilde{G}$ is called the Grothendieck's descent data for $\mathcal{L}$ with respect to f [60, pp.290–291]. Moreover, Mumford [60, pp.294] proves that there exists a level group $\widetilde{G}$ over G if and only if G is isotropic with respect to $e_{\mathcal{L}}$, i.e., $e_{\mathcal{L}} \equiv 1$ on G. Given a theta structure $\Theta_{\mathcal{L}}$ on A, we can define the level groups $\widetilde{K}_i(\mathcal{L})$ above $K_i(\mathcal{L})$ via the group sections $s_{K_i(\mathcal{L})} \colon K_i(\mathcal{L}) \to \mathcal{G}(\mathcal{L})$ for $i = 1, 2$ [66, Prop.3.3.3]. A level structure on $\mathcal{G}(\mathcal{L})$ is by definition a particular choice of level groups $\widetilde{K}_i(\mathcal{L})$ above $K_i(\mathcal{L})$.

The definition [66, 3.6.1] introduces the important notion of compatible theta structures with respect to an isogeny of polarized abelian varieties. A theta structure $\Theta_{\mathcal{M}}$ on $(B, \mathcal{M})$ is said to be f-compatible to

$\Theta_{\mathcal{L}}$ on $(A, \mathcal{L})$ if the following condition holds:

* The induced level structure on $\mathcal{G}(\mathcal{L})$ is compatible with the induced level structure on $\mathcal{G}(\mathcal{M})$ via f, i.e., the symplectic decomposition of $\widetilde{G}$ is $(\widetilde{G} \cap \widetilde{K}_1(\mathcal{L})) \oplus (\widetilde{G} \cap \widetilde{K}_2(\mathcal{L}))$. Reciprocally, the level structure on $\mathcal{G}(\mathcal{M})$ is also compatible with the level structure on $\mathcal{G}(\mathcal{L})$ via the isogeny f, i.e., $\alpha_f(\widetilde{K}_i(\mathcal{L}) \cap \mathcal{Z}(\widetilde{G})) \subset \widetilde{K}_i(\mathcal{M})$ for $i = 1, 2$.

** The kernel is of the form $G = G_1 \oplus G_2$, where $G_i = K_i(\mathcal{L}) \cap G$ for $i = 1, 2$. Equivalently, if $G^{\perp} \subset K(\mathcal{L})$ be the orthogonal complement of G with respect to $e_{\mathcal{L}}$. Then, $G^{\perp} = G^{\perp,1} \oplus G^{\perp,2}$ is the decomposition induced by the symplectic decomposition of G.

The set of theta structures $\Theta_{\mathcal{M}}$ on $(B, \mathcal{M})$ that are compatible with a fixed $\Theta_{\mathcal{L}}$ on $(A, \mathcal{L})$ is in bijection with the set of isomorphisms $\sigma \colon G^{\perp,1}/G_1 \to \mathbf{Z}(\delta_0)$ where δ_0 is the type of $\Theta_{\mathcal{M}}$ [66, Prop.3.6.2]. Given the canonical α_f associated to the level group $\widetilde{G}$, if $\Theta_{\mathcal{L}}$ is symmetric, then following [66, Rem. 4.2.15], any compatible theta structure $\Theta_{\mathcal{M}}$ on B is necessarily symmetric.

Theorem 3.2.7. *(Isogeny Theorem) Consider an isogeny of polarized abelian varieties $f \colon (A, \mathcal{L}) \to (B, \mathcal{M})$ of kernel G, with $\mathcal{L}$ totally symmetric and of type δ and $\mathcal{M}$ totally symmetric and of type δ_0. Let $\Theta_{\mathcal{L}}$ on $(A, \mathcal{L})$ and $\Theta_{\mathcal{M}}$ on $(B, \mathcal{M})$ be compatible symmetric theta structures with respect to f. Let $\sigma \colon G^{\perp,1}/G_1 \xrightarrow{\sim} \mathbf{Z}(\delta_0)$ be the isomorphism corresponding to the choice of $\Theta_{\mathcal{M}}$.*

Consider the canonical basis $(\theta_i^{\Theta_{\mathcal{L}}})_{i \in \mathbf{Z}(\delta)}$ of $\Gamma(A, \mathcal{L})$ and $(\theta_i^{\Theta_{\mathcal{M}}})_{i \in \mathbf{Z}(\delta_0)}$ of $\Gamma(B, \mathcal{M})$ respectively. There exists $\lambda \in \overline{k}^{\times}$ such that for all $i \in K_1(\mathcal{M})$ we have

$$f^* \theta_i^{\Theta_{\mathcal{M}}} = \lambda \sum_{j \in \sigma^{-1}(i)} \theta_j^{\Theta_{\mathcal{L}}}. \tag{3.19}$$

3.2.5 Canonical Affine Lifts

We can explicitly obtain the projective theta coordinates of a point x given in Mumford coordinates, via the method in [12, §5.3]. As in the complex case, the projective coordinates are unique up to multiplication by a constant (see Section 3.2.2.1).

Let $(A, \mathcal{L}, \Theta_{\mathcal{L}})$ be a polarized abelian variety with theta structure and projective embedding into $\mathbf{P}(\Gamma(A, \mathcal{L}))$. Let $\theta_i^{\Theta_{\mathcal{L}}} : A \to \mathbf{P}(\Gamma(A, \mathcal{L}))$ be a fixed basis of the projective embedding. Let $p_A \colon \mathbf{A}(\Gamma(A, \mathcal{L})) \setminus \{0\} \to \mathbf{P}(\Gamma(A, \mathcal{L}))$ be the canonical projection of an affine space onto the corresponding projective space. An affine lift of $x \in A$ is an element of $\widetilde{A} := p_A^{-1}(A)$. In the case of an element x in $K(\mathcal{L})$, we are able to fix a particular affine lift that comes from the theta structure, and more precisely from an affine lift of the theta constant.

Following [66, p.72], we define an affine lift of $x \in K(\mathcal{L})$ as corresponding to a trivialization (isomorphism) $\gamma_x \colon \mathcal{L}(x) \to k$ and consequently, to a constant $\gamma_x(\theta_i^{\Theta_{\mathcal{L}}}(x)) \in k^*$. In [66, p.51], as $\mathcal{L}$ is very ample, the author proves that given an affine lift of 0, we can compute affine lifts of all the other $x \in K(\mathcal{L})$ by using the action of the Heisenberg group on $K(\delta)$. For that, consider the section $s_{K(\mathcal{L})} \colon K(\mathcal{L}) \to \mathcal{G}(\mathcal{L})$ induced by the theta structure $\Theta_{\mathcal{L}}$ and the canonical section $s_{\delta} \colon K(\delta) \to H(\delta)$, where

$$s_{\delta}(x_1, x_2) = (1, x_1, x_2).$$

If $(x, \phi) = s_{K(\mathcal{L})}(x)$ then for any $y \in A$, we have $\phi(y) \colon \mathcal{L}(y) \to t_x^*(\mathcal{L}(y))$ and hence,

$$\mathcal{L}(x) = t_x^*(\mathcal{L}(0)) \xrightarrow{\phi^{-1}(0)} \mathcal{L}(0) \xrightarrow{\gamma_0} k.$$

So, the trivialization $\gamma_0\colon \mathcal{L}(0) \to \overline{k}$ induces a trivialization $\gamma_x\colon \mathcal{L}(x) \to \overline{k}$ for all $x \in K(\mathcal{L})$ of the form

$$\gamma_x = \gamma_0 \circ (\phi^{-1}(0)).$$

Let $\gamma_0\colon \mathcal{L}(0) \to \overline{k}$ be a fixed trivialization and let $\widetilde{0}_\mathcal{L}$ be the corresponding affine lift of the theta null point. The theta coordinates of $\widetilde{x}$, where $x = x_1 + x_2 \in K(\mathcal{L})$, are determined precisely via the action of the Heisenberg group on $\widetilde{0}_\mathcal{L}$ [66, Eq. (3.9)], namely:

$$\theta_i^{\Theta_\mathcal{L}}(\widetilde{x}) = e_\delta(i, x_2)\theta_{i-x_1}^{\Theta_\mathcal{L}}(\widetilde{0}_\mathcal{L}). \tag{3.20}$$

Definition 3.2.8. The induced affine lifts $\widetilde{x}$ of $x \in K(\mathcal{L})$ are called canonical affine lifts or compatible affine lifts for the choice of $\widetilde{0}_\mathcal{L}$.

For an arbitrary point $z \in A(k)$, that is not in $K(\mathcal{L})$, if an affine lift $\widetilde{z} \in p_A^{-1}(z)$ is fixed, then any other affine lift of z is of the form $\lambda_z \cdot \widetilde{z}$ for some constant $\lambda_z \in \overline{k}^*$. The coordinates of an affine lift $\widetilde{z}$ are called affine theta coordinates.

When working over the affine space $\mathbf{A}(\Gamma(A, \mathcal{L}))$, Robert proved in [66, Section 4.4] that we can define rigorously an affine correspondent to $f\colon (A, \mathcal{L}, \Theta_\mathcal{L}) \to (B, \mathcal{M}, \Theta_\mathcal{M})$ (satisfying the conditions in the Isogeny Theorem 3.2.7) when we are given affine lifts of the theta constants for both A and B.

Definition 3.2.9. Given the isogeny $f\colon (A, \mathcal{L}, \Theta_\mathcal{L}) \to (B, \mathcal{M}, \Theta_\mathcal{M})$ together with the affine system of theta coordinates $\theta_i^{\Theta_\mathcal{L}}\colon \widetilde{A} \to \overline{k}$ and $\theta_i^{\Theta_\mathcal{M}}\colon \widetilde{B} \to \overline{k}$ (corresponding to the canonical choice of basis $(\theta_i^{\Theta_\mathcal{L}})_{i\in K_1(\mathcal{L})}$ and $(\theta_j^{\Theta_\mathcal{M}})_{j\in K_1(\mathcal{M})}$), the canonical affine isogeny $\widetilde{f}$ is the isogeny $\widetilde{f}\colon \widetilde{A} \to \widetilde{B}$ such that for each $i \in K_1(\mathcal{M})$ and $j \in K_1(\mathcal{L})$ and for each x, we have:

$$\theta_i^{\Theta_\mathcal{M}}(\widetilde{f(x)}) = \sum_{j\in\sigma^{-1}(i)} \theta_j^{\Theta_\mathcal{L}}(\widetilde{x}) \tag{3.21}$$

where $\sigma\colon K_1(\mathcal{L}) \to K_1(\mathcal{M})$.

Moreover, the affine isogeny $\widetilde{f}$ is an isogeny that corresponds to f in the sense that the following diagram is commutative:

$$\begin{tikzcd}
(\widetilde{A}, \widetilde{0}_\mathcal{L}) \arrow[r, "p_A"] \arrow[d, "\widetilde{f}"'] & (A, \mathcal{L}, \Theta_\mathcal{L}) \arrow[d, "f"'] \\
(\widetilde{B}, \widetilde{0}_\mathcal{M}) \arrow[r, "p_B"] & (B, \mathcal{M}, \Theta_\mathcal{M})
\end{tikzcd} \tag{3.22}$$

Definition 3.2.10. Consider the canonical affine isogeny with theta structures $\widetilde{f}\colon (\widetilde{A}, \mathcal{L}, \Theta_\mathcal{L}) \to (\widetilde{B}, \mathcal{M}, \Theta_\mathcal{M})$ and a choice of affine theta null point $\widetilde{0}_\mathcal{L}$. If $\widetilde{x} \in \widetilde{A}$ is a canonical affine lift of $x \in K(\mathcal{L})$ for the choice of $\widetilde{0}_\mathcal{L}$, we say that $\widetilde{y} = \widetilde{f}(\widetilde{x}) \in \widetilde{B}$ is a compatible affine lift of $y = f(x)$ with respect to $\widetilde{f}$.

Example:

In [66, Ch.7], the author shows how to compute (ℓ, ℓ)-isogenies between abelian varieties A and B. For that, one fixes canonical affine lifts of the isogeny kernel inside the ℓ-torsion points when provided with a certain choice of affine theta constants for A. More precisely, let $A[\ell] = A_1[\ell] \oplus A_2[\ell]$ be a symplectic decomposition with respect to the Weil pairing $e_\ell \colon A[\ell] \times A[\ell] \to \mu_\ell$ and let $G = A_1[\ell]$.

Consider the isogeny $f \colon A \to B$ of kernel G. Since G is maximal isotropic with respect to e_ℓ, then B admits a principal polarization $\mathcal{M}_0$ (section 3.2.4). Let $\mathcal{M} = \mathcal{M}_0^{\otimes n}$ be a totally symmetric line bundle and consider the ℓ-contragradient isogeny $\widehat{f} \colon (B, \mathcal{M}^\ell) \to (A, \mathcal{L})$ of f, where $\mathcal{M}^\ell \simeq \widehat{f}^* \mathcal{L}$ is of type $\delta_{\ell n}$. The isogeny $\widehat{f}$ has kernel $G' = B_2[\ell] = f(A_2[\ell])$. Moreover, $B_1[\ell] = K_1(\mathcal{M}^\ell)[\ell]$ and so, the elements of the kernel admit compatible affine lifts with the choice of an affine lift $(\theta_i^{\Theta_{\mathcal{M}^\ell}}(\widetilde{0}))_{i \in K_1(\mathcal{M}^\ell)}$. Since $\widehat{f}(B_1[\ell]) = G$, then by definition of the canonical affine isogeny $\widetilde{\widehat{f}}$, the elements of the kernel G admit compatible affine lifts with respect to $\Theta_{\mathcal{M}^\ell}$. The (ℓ, ℓ)-isogeny case is particularly useful in Chapter 4 of our thesis where we explain how to fix compatible affine lifts of a cyclic subgroup of the ℓ-torsion points.

3.2.6 Main Operations on Points in Affine Theta Coordinates

In this section, we introduce the main operations on points in affine theta coordinates on a principally polarized abelian variety A defined over k, namely chain addition and chain multiplication on the affine cone $\widetilde{A}$. When computing a certain operation on affine points, we consider two different affine lifts for each point $z_i \in A$ in the input, one fixed $\widetilde{z}_i$ and one that differs by a factor λ_{z_i}. We compute the factor that differentiate between the two affine lifts that result, one corresponding to $\widetilde{z}_i$ and the other one corresponding to $\lambda_{z_i} \widetilde{z}_i$.

First, over $\mathbf{C}$ a classical theorem states that the Riemann theta functions with characteristics (equation (3.2)) satisfy the so-called Generalized Riemann Relations. The Riemann relations allow us to define operations of chain addition and chain multiplication on complex points given in level n (affine or not) theta coordinates (see for instance [49] for more details). The chain addition operation outputs the level n theta coordinates of $x + y$ given the level n theta coordinates of x, y, $x - y$ and 0. The chain multiplication algorithm determines the level n theta coordinates of ax given the level n theta coordinates of x and 0.

We present below the generalized Riemann relations in the case of a principally polarized abelian variety $(A, \mathcal{L}_0)$ over k, with a totally symmetric line bundle $\mathcal{L} = \mathcal{L}_0^n$, where $n = 2n' \geq 2$, and a symmetric theta structure $\Theta_{\mathcal{L}}$ of level n. Let δ be the type of $\mathcal{L}$. Recall that $\overline{\Theta}_{\mathcal{L}} \colon K(\delta) \to K(\mathcal{L})$ denotes the isomorphism corresponding to $\Theta_{\mathcal{L}}$ and that the group $K(\delta)$ is $\mathbf{Z}(n) + \hat{\mathbf{Z}}(n)$ (see Section 3.2.2). We follow the exposition in [66, Section 4.4]. Any $t \in \mathbf{Z}(2)$ is identified with an element in $\mathbf{Z}(n)$ via the canonical map $t \to n't$. For any affine lifts $\widetilde{x}, \widetilde{y} \in \widetilde{A}$, indexes $i, j \in \mathbf{Z}(n)$ and character $\chi \in \hat{\mathbf{Z}}(2)$ we denote by

$$L_{i,j}(\widetilde{x}, \widetilde{y}) := \sum_{t \in \mathbf{Z}(2)} \chi(t) \theta_{i+t}^{\Theta_{\mathcal{L}}}(\widetilde{x}) \theta_{j+t}^{\Theta_{\mathcal{L}}}(\widetilde{y}) \tag{3.23}$$

Then, [66, Thm. 4.4.6] summarizes the Generalized Riemann relations for a theta structure of level n.

Theorem 3.2.11. *Let $x_1, y_1, u_1, v_1 \in A$ and let $z \in A$ be such that $x_1 + y_1 + u_1 + v_1 = 2z$. Let*

$$x_2 := z - x_1,\ y_2 := z - y_1,\ u_2 := z - u_1,\ v_2 := z - v_1. \tag{3.24}$$

Then there exist affine lifts of $x_1, x_2, y_1, y_2, u_1, u_2, v_1, v_2$ such that for all characters χ in $\hat{\mathbf{Z}}(2)$, and $i, j, k, l, m \in \mathbf{Z}(n)$ with $i + j + k + l = 2m$ and $i' = m - i, j' = m - j, k' = m - k$ and $l' = m - l$,

$$L_{i,j}(\widetilde{x}_1, \widetilde{y}_1) L_{k,l}(\widetilde{u}_1, \widetilde{v}_1) = L_{i',j'}(\widetilde{x}_2, \widetilde{y}_2) L_{k',l'}(\widetilde{u}_2, \widetilde{v}_2). \tag{3.25}$$

We first obtain the theta coordinates of $\widetilde{x+y}$ (corresponding to $\Theta_{\mathcal{L}}$) from the theta coordinates of $\widetilde{x}$, $\widetilde{y}$ and $\widetilde{0}$ (again corresponding to $\Theta_{\mathcal{L}}$). Next, we replace the variables in (3.25) such that the theta coordinates of $\widetilde{x+y}$ are on the left-hand side, whereas the theta coordinates of $\widetilde{x}$ and $\widetilde{y}$ are on the right-hand side. Then, in (3.24) the variable $z \leftarrow x$ and so, $u_1 = 0$, $v_1 = 0$, $x_2 = -y$, $y_2 = y$, $u_2 = x$ and $v_2 = x$. The Riemann relations become

$$L_{i,j}(\widetilde{x+y}, \widetilde{x-y})L_{k,l}(\widetilde{0}, \widetilde{0}) = L_{-i',j'}(\widetilde{y}, \widetilde{y})L_{k',l'}(\widetilde{x}, \widetilde{x}). \tag{3.26}$$

The theta coordinates of $\widetilde{x+y}$ are determined uniquely from the affine theta coordinates of $\widetilde{x}, \widetilde{y}, \widetilde{x-y}, \widetilde{0}$ via (3.26) if and only if $L_{k,l}(\widetilde{0}, \widetilde{0})$ is non-zero for some k, ℓ such that $i + j + k + l = 2\mathbf{Z}(n)$. This is indeed true for the case $4|\delta$ following the proof of the Riemann relations in [66, Thm.4.4.6]. Otherwise, if only $2|\delta$ we assume that we are in the so-called generic case [22, 50].

Similarly to [66, p.77], we denote by `chain_add` an algorithm that given $\widetilde{0}, \widetilde{x}, \widetilde{y}, \widetilde{x-y}$ as input, outputs $\widetilde{x+y}$ based on (3.26), namely

$$\texttt{chain\_add}(\widetilde{x}, \widetilde{y}, \widetilde{x-y}, \widetilde{0}) \to \widetilde{x+y}.$$

For convenience, we also write $\widetilde{x+y} = \texttt{chain\_add}(\widetilde{x}, \widetilde{y}, \widetilde{x-y}, \widetilde{0})$.

Remark 8. For instance, the algorithm [66, Alg.4.4.10] is such a method and is a direct application of the Riemann relations from [60, p.334-335]. The **complexity of the algorithm** for the general case is $\#\mathbf{Z}(\delta) + 2^g$ multiplications, $\#\mathbf{Z}(\delta) + 2^g$ squares, $\#\mathbf{Z}(\delta)$ inversions and $\mathcal{O}(4^g \#\mathbf{Z}(\delta)^2)$ additions.

Due to [66, Lemma 4.5.3], if we consider distinct affine lifts for each point $x, y, 0$ and $x-y$, that differ from $\widetilde{x}, \widetilde{y}, \widetilde{0}, \widetilde{x-y}$ by some non-zero factors $\lambda_x, \lambda_y, \lambda_0$ and λ_{x-y} respectively, then any `chain_add` algorithm satisfies

$$\texttt{chain\_add}(\lambda_x\widetilde{x}, \lambda_y\widetilde{y}, \lambda_{x-y}\widetilde{x-y}, \lambda_0\widetilde{0}) = \frac{\lambda_x^2\lambda_y^2}{\lambda_{x-y}\lambda_0^2}\texttt{chain\_add}(\widetilde{x}, \widetilde{y}, \widetilde{x-y}, \widetilde{0}). \tag{3.27}$$

Starting with $a = 2$ and afterwards, for each $a \leftarrow a + 1$, we define

$$\widetilde{ax+y} := \texttt{chain\_add}(\widetilde{(a-1)x+y}, \widetilde{x}, \widetilde{(a-2)x+y}, \widetilde{0}).$$

We call `chain_multadd` a method that computes $\widetilde{ax+y}$ (as defined above), out of $\widetilde{x}, \widetilde{y}$, $\widetilde{x+y}$ and scalar $a > 1$, namely:

$$\texttt{chain\_multadd}(a, \widetilde{x}, \widetilde{x+y}, \widetilde{y}, \widetilde{0}) \to \widetilde{ax+y}.$$

For convenience we also write $\widetilde{ax+y} = \texttt{chain\_multadd}(a, \widetilde{x}, \widetilde{x+y}, \widetilde{y}, \widetilde{0})$ as the result is unique, independent of the choice of method [66, p.87].

Remark 9. Such a method is algorithm [66, Alg.4.4.12] that uses the base 2 decomposition of a and a classical Montgomery ladder. The algorithm requires $3\lceil \log a \rceil$ chain additions plus another initial chain addition for the Montgomery ladder. So the **complexity of the algorithm** is of $\mathcal{O}(\log a)$ chain additions in the field of definition.

As before, we consider other affine lifts of the form $\lambda_x\widetilde{x}, \lambda_y\widetilde{y}, \lambda_{x+y}\widetilde{x+y}, \lambda_0\widetilde{0}$ where $\lambda_x, \lambda_y, \lambda_{x+y}, \lambda_0 \in \overline{k}^*$.

Then, we obtain by induction that:

$$\begin{aligned}\texttt{chain\_multadd} \quad & (a, \lambda_x\widetilde{x}, \lambda_{x+y}\widetilde{x+y}, \lambda_y\widetilde{y}, \lambda_0\widetilde{0}) = \\ & = \frac{\lambda_{x+y}^{a}\lambda_x^{a(a-1)}}{\lambda_y^{a-1}\lambda_0^{a(a-1)}}\texttt{chain\_multadd}(a, \widetilde{x}, \widetilde{x+y}, \widetilde{y}, \widetilde{0}).\end{aligned} \tag{3.28}$$

In the particular case of $y = 0$, we denote by

$$\widetilde{ax} := \texttt{chain\_mult}(a, \widetilde{x}, \widetilde{0}),$$

as in [66, p.81] and we have

$$\texttt{chain\_mult}(a, \lambda_x\widetilde{x}, \lambda_0\widetilde{0}) = \frac{\lambda_x^{a^2}}{\lambda_0^{a^2-1}}\texttt{chain\_mult}(a, \widetilde{x}, \widetilde{0}). \tag{3.29}$$

If we fix $\widetilde{ax}$, $\widetilde{ax+y}$, $\widetilde{y}$, then we similarly define for each integer $b > 1$,

$$\widetilde{ax+by} := \texttt{chain\_add}(\widetilde{ax+(b-1)y}, \widetilde{y}, \widetilde{ax+(b-2)y}, \widetilde{0}).$$

A method `chain_multiadd` is an algorithm that computes $\widetilde{ax+by}$ directly from $\widetilde{x}$, $\widetilde{y}, \widetilde{0}$ and $\widetilde{x+y}$ and scalars a, b, namely:

$$\texttt{chain\_multiadd}(a, b, \widetilde{x}, \widetilde{x+y}, \widetilde{y}, \widetilde{0}) \to \widetilde{ax+by}$$

Equations (3.28) and (3.29) determine:

$$\begin{aligned}&\texttt{chain\_multiadd}(a, b, \lambda_x\widetilde{x}, \lambda_{x+y}\widetilde{x+y}, \lambda_y\widetilde{y}, \lambda_0\widetilde{0}) = \\ &= \frac{\lambda_{x+y}^{ab}\lambda_x^{a(a-b)}\lambda_y^{b(b-a)}}{\lambda_0^{a^2+b^2-ab-1}}\texttt{chain\_multiadd}(a, b, \widetilde{x}, \widetilde{x+y}, \widetilde{y}, \widetilde{0}).\end{aligned} \tag{3.30}$$

We apply [49, Prop.1] in the case of abelian varieties over k. Consider the principally polarized abelian variety $(A, \mathcal{L}_0)$ and let $x_1, x_2 \in A$. Then, for any point $x \in A$, if we are given affine lifts $\widetilde{x}_1$, $\widetilde{x}_2$, $\widetilde{x}$, $\widetilde{x_1+x_2}$, $\widetilde{x_1+x}$, $\widetilde{x_2+x} \in \widetilde{A}$ of level n, then there exists a unique affine lift $x_1 + x_2 + x$ of level n that satisfies the Riemann relations (3.25):

$$\begin{aligned}&L_{i+j,i-j}(\widetilde{x+x_1+x_2}, \widetilde{x_1})L_{k+l,k-l}(\widetilde{x}_2, \widetilde{x}) = \\ &= L_{i+k,i-k}(\widetilde{0}, \widetilde{x_2+x})L_{j+l,j-l}(\widetilde{x_1+x}, \widetilde{x_1+x_2})\end{aligned} \tag{3.31}$$

Similarly to the chain addition algorithm, we presume that for all $x \in A$ and k, ℓ such that $i+j+k+\ell = 2\mathbf{Z}(n)$ we have $L_{k+l,k-l}(\widetilde{x}_2, \widetilde{x}) \neq 0$ (see proof of [49, Prop.1]). We denote by `three_way_add` the algorithm that computes the affine lift of $x + x_1 + x_2$, namely

$$\widetilde{x+x_1+x_2} = \texttt{three\_way\_add}(\widetilde{x}, \widetilde{x}_1, \widetilde{x}_2, \widetilde{x+x_1}, \widetilde{x+x_2}, \widetilde{x_1+x_2}) \tag{3.32}$$

3.2.7 Action of the Heisenberg Group on Affine Lifts

Consider the polarized abelian variety $(A, \mathcal{L}, \Theta_{\mathcal{L}})$ together with an affine lift $\widetilde{0}_{\mathcal{L}} \in \widetilde{A}$, where the line bundle $\mathcal{L} = \mathcal{L}_0^2$ is of type δ. Similarly to the case of complex theta constants (see (3.9)), we define canonical affine theta coordinates for elements in $K(\mathcal{L})$ out of the affine theta constants $\widetilde{0}_{\mathcal{L}}$. An element $(\alpha, u_1, u_2) \in H(\delta)$ is identified via the theta structure $\Theta_{\mathcal{L}}$ with $u \in \mathcal{G}(\mathcal{L})$. The action of (α, u_1, u_2) on the theta coordinates of an affine point $\widetilde{x} \in \widetilde{A}$ is denoted by $(\alpha, u_1, u_2) \cdot \widetilde{x}$ is given by:

$$(\alpha, u_1, u_2) \cdot \theta_i^{\Theta_{\mathcal{L}}}(\widetilde{x}) = \alpha e_\delta(-i - u_1, u_2)\theta_{i+u_1}^{\Theta_{\mathcal{L}}}(\widetilde{x}). \tag{3.33}$$

Let $\widetilde{x+y} = \texttt{chain\_add}(\widetilde{x}, \widetilde{y}, \widetilde{x-y})$. Here we omit the affine theta null point as it remains constant for now.

By translating the theta indexes in the Riemann relations via some properly chosen elements in $\mathbf{Z}(\delta)$, Robert proved in [66, Prop.4.5.4] that $((1, u_1 + v_1, 0) \cdot \widetilde{x+y}$, $(1, u_1, 0) \cdot \widetilde{x}$, $(1, v_1, 0) \cdot \widetilde{y}$,$(1, u_1 - v_1, 0) \cdot \widetilde{x-y})$ and $((1, 0, u_2 + v_2) \cdot \widetilde{x+y}$, $(1, 0, u_2) \cdot \widetilde{x}$, $(1, 0, v_2) \cdot \widetilde{y}$, $(1, 0, u_2 - v_2)\widetilde{x-y})$ satisfy the Riemann relations for the case of chain addition.

In the end, together with equation (3.28) and the addition law on $H(\delta)$, Robert proved in [66, §4.5] that if $u = (\alpha, u_1, u_2)$ and $v = (\alpha, v_1, v_2)$, then

$$(uv) \cdot \texttt{chain\_add}(\widetilde{x}, \widetilde{y}, \widetilde{x-y}) = \frac{e_\delta(v_1, v_2)}{\beta^2}\texttt{chain\_add}(u \cdot \widetilde{x}, v \cdot \widetilde{y}, (uv^{-1}) \cdot \widetilde{x-y}). \tag{3.34}$$

The action of the theta group is really useful when computing an affine lift of $\widetilde{mt+x}$, where $\widetilde{t}$ is an affine lift of an ℓ-torsion point t, $\widetilde{x}$ is an affine lift of $x \in A$ is of large order, and the affine lift of $\widetilde{mt+x}$ is computed from $\widetilde{t}$, $\widetilde{x}$,$\widetilde{t+x}$.

4 Computing Cyclic Isogenies in Genus 2

4.1 Introduction

In this chapter, we focus on computing cyclic isogenies of prime degree ℓ between Jacobians of genus 2 hyperelliptic curves defined over a finite field $\mathbf{F}_q$ of large characteristic. This work was completed in collaboration with Dimitar Jetchev and Damien Robert. The algorithm is related to prior work of Cosset and Robert [13] where they proposed an efficient method (polynomial in $\log q$ and ℓ) that computes (ℓ, ℓ)-isogenies, namely isogenies whose kernel is not cyclic, but is a maximal isotropic subgroup for the Weil pairing e_ℓ on the source variety. In this case, the target variety B is principally polarizable via the Grothendieck descent argument (see Section 3.2.4)

In the case of (ℓ, ℓ)-isogenies of polarized abelian varieties $f\colon (A, \mathcal{L}) \to (B, \mathcal{M})$, the CM description of the abelian varieties A, B (see Section 3.1.4) is unnecessary when computing the theta constants of the target variety B or the image of a point on B. Given a symmetric theta structure $\Theta_{\mathcal{L}}$ on A, a set of affine theta constants and the kernel of the isogeny in certain affine theta coordinates (for $\Theta_{\mathcal{L}}$), the algorithm computes an affine theta null point of B for a compatible symmetric theta structure $\Theta_{\mathcal{M}}$ on B [13, Thm. 3.1]. The authors compute also a set of affine theta coordinates of $f(x)$, for $x \in A$, out of a set of affine theta coordinates of the points $x + t$, where $t \in G$ [13, Prop. 4.1.].

In our case, let $f\colon A \to A/G$ be a cyclic isogeny of kernel G over a finite field $\mathbf{F}_q$. Naturally, we want to find similar equations to the formulas in [13]. First, let $\mathcal{L}_0$ be a principal polarization on A. Let $\mathrm{End}(A)^+$ denote the ring of real multiplication endomorphisms inside the endomorphism ring $\mathrm{End}(A)$. Next, for the cyclic isogeny f to be an isogeny of polarized abelian varieties we need that the kernel of f is contained in the kernel of a suitable polarization isogeny $A \to A^\vee$. According to Sections 4.3 and 4.4, there exists a principal polarization $\mathcal{M}_0$ on B if and only if there exists a totally positive real endomorphism $\beta \in \mathrm{End}(A)^+$ such that $G \subset \ker(\varphi_{\mathcal{L}_0^\beta})$ is a maximal isotropic subgroup for the commutator pairing $e_{\mathcal{L}_0^\beta}$ (here, $\varphi_{\mathcal{L}_0^\beta}$ denotes the composition $\beta \circ \varphi_{\mathcal{L}_0}$). Let $\alpha_1, \ldots, \alpha_r \in K_0$ such that $\beta = \sum_{s=1}^r \alpha_s^2$.

In our case, we have the following result:

Theorem 4.1.1. *Consider the following* ***input*** *for computing a cyclic isogeny over a finite field:*

I1. a finite field $\mathbf{F}_q$, an odd prime number ℓ with $(\ell, q) = 1$;

I2. a smooth hyperelliptic curve C of genus 2 over $\mathbf{F}_q$ in Rosenhain form, with $A = \mathrm{Jac}(C)$ and $\mathcal{L}_0$

its canonical principal polarization;

I3. a CM-type (K, Φ) of A,[1] *where K is a quartic CM field, with real quadratic field $K_0 \subset K$ of discriminant D;*

I4. a generator t of the isogeny kernel $G \subset A[\ell]$ with $\pi(t) \in G$,[2] *given in Mumford coordinates defined over an extension field $\mathbf{F}/\mathbf{F}_q$;*

I5. a point $x \in A(\mathbf{F}_q)$ of order Q that is prime to q, ℓ, given in Mumford coordinates.

We assume the following conditions with respect to real multiplication on A

H1. $\mathrm{End}(A) \simeq \mathcal{O} \subset K$ *of* ***maximal real multiplication****, i.e., $\mathcal{O}_0 = \mathcal{O} \cap K_0$ is the ring of integers of K_0 ;*

H2. the ***index of*** $[\mathcal{O} \colon \mathbf{Z}[\pi, \overline{\pi}]]$ *is* ***prime*** *to $2\ell Q$;*

H3. there ***exists a totally positive element*** *$\beta \in \mathcal{O}_0$ of* ***norm*** *ℓ such that $\beta(t) = 0$.*

Then there ***exists*** *an algorithm of* ***output:***

O1. an equation of C' over $\mathbf{F}_q$, such that $\mathrm{Jac}(C') \sim_{\mathbf{F}_q} (B, \mathcal{M}_0)$ *(as a principally polarized abelian variety), where $\mathcal{M}_0$ is the principal polarization on B such that $f^*\mathcal{M}_0$ is algebraically equivalent to $\mathcal{L}_0^{\beta}$.*

O2. the point $f(x) \in$ $\mathrm{Jac}(C')$*, in Mumford coordinates.*

Given certain pre-computed data[3]*, the cost of computing a target curve is of $\mathcal{O}(\ell^2)$ operations in the extension field $\mathbf{F}$ over which the elements in G are defined.*

Given certain pre-computed data[4]*, the cost of computing $f(x)$ is of $\mathcal{O}(\ell^2)$ operations in the field of definition over which the affine theta coordinates of the points $\alpha_s x + at$, with $a \in \mathbf{Z}/\ell\mathbf{Z}$ and $\sum_{s=1}^{r} \alpha_s^2 = \beta$, are defined.*

This chapter is organized as follows. Given the input of the algorithm, we compute an affine theta null point of A via Thomae's formulae. The theta constants implicitly correspond to a totally symmetric line bundle $\mathcal{L}$ and a symmetric theta structure of level 2 on A, namely they correspond to $(A, \mathcal{L}, \Theta_{\mathcal{L}})$. We denote them by $\widetilde{0}_{\mathcal{L}}$. Following Section 3.2.7, we obtain canonical level 2 affine theta coordinates for a symplectic basis of $A[2]$ (compatible with the choice of $\widetilde{0}_{\mathcal{L}}$ as defined in 3.2.8). We also compute an affine theta null point $\widetilde{0}_{\mathcal{L}^2}$ of level 4 and the corresponding affine theta coordinates of a symplectic basis of $A[4]$ for a compatible theta structure $\Theta_{\mathcal{L}^2}$ with $\Theta_{\mathcal{L}}$ (in the sense of Section 3.2.3). The choice of level 4 theta constants and of basis for the 4-torsion points is done by fixing once and for all an additional choice of signs (see Section 4.2).

Next section proves that the target variety B is indeed principally polarizable and that the pullback of the principal polarization $\mathcal{M}_0$ via f is indeed algebraically equivalent to $\mathcal{L}_0^{\beta}$. Ultimately, we wish to compute, using Theorem 3.2.7, the canonical theta constants for a suitably chosen symmetric theta structure $\Theta_{\mathcal{M}}$ on $(B, \mathcal{M})$, where $\mathcal{M} = \mathcal{M}_0^2$. One possible way is to first compute the theta constants for a symmetric theta structure $\Theta_{\mathcal{L}^\beta}$ on $(A, \mathcal{L}^\beta)$ in order to apply the isogeny theorem to $f \colon (A, \mathcal{L}^\beta) \to (B, \mathcal{M})$

[1] We fix an isomorphism $\iota \colon K \to \mathrm{End}^0(A)$, and let $\chi(\pi)$ (associated to $K/\mathbf{Q}$) be the polynomial of the Frobenius endomorphism π. To simplify notations, ι is omitted when referring to the image of an endomorphism as an element in K_0.

[2] G is stable under Frobenius

[3] The pre-computed data consists of certain affine theta coordinates for all points in G, together with the action of $\alpha_1, \ldots, \alpha_r$ on the abstract representation of the 2-torsion points. Check Section 4.8 for more details.

[4] The pre-computed data consists of certain affine theta coordinates of $\alpha_s x + at$, for all $s = 1, \ldots, r$ and $a \in \mathbf{Z}/\ell\mathbf{Z}$, together with the action of $\alpha_1, \ldots, \alpha_r$ on the abstract representation of the 2-torsion points. Check Section 4.8 for more details.

that would expresses the theta constants of a symmetric theta structure $\Theta_{\mathcal{M}}$ compatible with $\Theta_{\mathcal{L}^\beta}$ (via f) in terms of those for $\Theta_{\mathcal{L}^\beta}$. Unfortunately, in order to compute the relation between the theta coordinates for the polarizations $\mathcal{L}$ and $\mathcal{L}^\beta$ we cannot simply apply the endomorphism β on A as $\beta^*\mathcal{L}$ is not algebraically equivalent to $\mathcal{L}^\beta$ (the latter have different degrees, $2\ell^4$ and $2\ell^2$ respectively). Moreover, in general there exists no endomorphism $u\colon (A, \mathcal{L}^\beta) \to (A, \mathcal{L})$ such that $u\overline{u} = \beta$. To resolve this issue, we use the idea of [13], based on Zarhin's trick [55, Thm 13.12]. Given the polarized abelian variety $(A, \mathcal{L}^\beta)$, there exists a principal polarization on A^r, with $r = 2, 4$, coming from the decomposition of β as a sum of r squares in K_0 (see the definition 3.2.1 of a polarization $\mathcal{L}^{\star r}$ on A^r given $(A, \mathcal{L})$).

Next, we compute 4 elements $\alpha_i \in K_0$ such that $\alpha_1^2 + \ldots + \alpha_4^2 = \beta$ (when 2 of them, then A^2 is principally polarized). In general, the α_i's need not be integral and hence, need not be endomorphisms of A. Yet, assuming that they yield endomorphisms of the β-torsion points, of $\langle x \rangle$ and the 2-torsion points (i.e., the denominators are prime to $2\ell Q$), one can take F to be the matrix corresponding to multiplication by $\alpha_1 + \alpha_2 i + \alpha_3 j + \alpha_4 k$ on the Hamilton quaternions over K_0 and observe that $F^t F = \beta I_4$. The decomposition is naturally not unique but in Section 4.5, we propose a deterministic method of computing α_i's based on the Euler's four-square identity. In Sections 4.3 and 4.4 we prove that the isogeny F descends the polarization $(A^r, (\mathcal{L}^\beta)^{\star r})$ to $(A^r, \mathcal{L}^{\star r})$.

In the end, if we assume that the above approach works and we obtain the theta constants for $\Theta_{\mathcal{L}^\beta}$ via F, the isogeny theorem applied to $f\colon (A, \mathcal{L}^\beta) \to (B, \mathcal{M})$ expresses the theta constants for $\Theta_{\mathcal{L}^\beta}$ as polynomials on the theta constants for $\Theta_{\mathcal{M}}$, thus requiring one to solve a polynomial system. Therefore, this method may be too expensive in practice. To resolve this issue, we proceed again as in the case of (ℓ, ℓ)-isogenies [13] and consider the β-contragredient isogeny $\widehat{f}\colon (B, \mathcal{M}^\beta) \to (A, \mathcal{L})$. In this case, we descend to a principal polarization on B^r via the isogeny $F\colon (B^r, (\mathcal{M}^\beta)^{\star r}) \to (B^r, \mathcal{M}^{\star r})$. Unfortunately, the resulting theta structure on B^r is not a product theta structure and hence we apply a symplectic isomorphism on B^r in order to determine the theta constants for $\Theta_{\mathcal{M}}$. The entire argument is presented in Section 4.6, including the explicit computation of the theta constants of B and the image of a point $x \in A$ via an affine version of the isogeny $\widehat{f}$ and F. In the last section, we estimate the complexity of the algorithm in Theorem 4.1.1 but we also analyze the cost of computing the pre-computed data.

4.2 Computing Theta Constants via Thomae's Formulas

The goal of this section is to present the classical method [22, 13] of computing an affine theta null point of level 2 and 4 out of the Rosenhain invariants λ, μ, ν [68] of the input curve C introduced in Theorem 4.1.1. To simplify the formulas presented in this section, we assume that the curve C is already given by its Rosenhain model, with $\{0, 1, \lambda, \mu, \nu \in \overline{\mathbf{F}}_q\}$ being the roots of the defining polynomial.

In order to compute an affine theta null point of level 2 and 4, we first give the analogue of complex theta functions of level $(2, 2)$ (see equation (3.5)). Consider the principally polarized abelian variety $(A, \mathcal{L}_0)$ together with the totally symmetric line bundle $\mathcal{L} = \mathcal{L}_0^2$ that were introduced in the previous section. Consider an arbitrary symmetric theta structure $\Theta_{\mathcal{L}^2}$ and let $\overline{\Theta}\colon \mathbf{Z}(4) \xrightarrow{\sim} K_1(\mathcal{L}^2)$ be the induced isomorphism. Let $\{\theta_b^{\Theta_{\mathcal{L}^2}} : A \to \overline{\mathbf{F}}_q \mid b \in K_1(\mathcal{L}^2)\}$ be the canonical basis for the space of global sections $\Gamma(A, \mathcal{L}^2)$. Each $b \in K_1(\mathcal{L}^2)$ is identified with a unique element in $\mathbf{Z}(4)$ via the isomorphism $\overline{\Theta}^{-1}$ and hence, we can index the basis by elements in $\mathbf{Z}(4)$ instead. Consider a map $\kappa_1\colon \mathbf{Z}(2) \to \mathbf{Z}(4)$ sending the vector components 0 and 1 to 0 and 1 respectively. Consider an embedding $\kappa_2\colon \mathbf{Z}(2) \to \mathbf{Z}(4)$ sending the vector components 0 and 1 to 0 and 2 respectively.

Definition 4.2.1. Given the theta structure $\Theta_{\mathcal{L}^2}$ of level 4 together with the maps $\kappa_1, \kappa_2 \colon \mathbf{Z}(2) \to \mathbf{Z}(4)$, the induced isomorphism $\overline{\Theta}\colon \mathbf{Z}(4) \xrightarrow{\sim} K_1(\mathcal{L}^2)$ and the basis $\{\theta_b^{\Theta_{\mathcal{L}^2}} : A \to \overline{\mathbf{F}}_q \mid b \in \mathbf{Z}(4)\}$ of $\Gamma(A, \mathcal{L}^2)$, we define the projective theta coordinates of level $(2,2)$ of $x \in A$ as being $\left(\theta_{a,b}^{\Theta_{\mathcal{L}^2}}(x)\right)_{a,b\in\mathbf{Z}(2)}$, where for each $a, b \in \mathbf{Z}(2)$ we have:

$$\theta_{a,b}^{\Theta_{\mathcal{L}^2}}(x) := \frac{1}{4}\sum_{c\in\mathbf{Z}(2)} (-1)^{a^t c}\theta^{\Theta_{\mathcal{L}^2}}_{\kappa_1(b)+\kappa_2(c)}(x). \tag{4.1}$$

Next, we also use a bijection map between theta indexes in $\mathbf{Z}(2)\times\mathbf{Z}(2)$ and elements of $\{0, 1, \cdots, 15\}$ identical to the one of Dupont [17] (and also used by [74, 12]):

$$\begin{array}{cccc}
0 \leftarrow \begin{bmatrix}(0,0)^t\\(0,0)^t\end{bmatrix} & 1 \leftarrow \begin{bmatrix}(0,0)^t\\(1,0)^t\end{bmatrix} & 2 \leftarrow \begin{bmatrix}(0,0)^t\\(0,1)^t\end{bmatrix} & 3 \leftarrow \begin{bmatrix}(0,0)^t\\(1,1)^t\end{bmatrix}\\
4 \leftarrow \begin{bmatrix}(1,0)^t\\(0,0)^t\end{bmatrix} & 5 \leftarrow \begin{bmatrix}(1,0)^t\\(1,0)^t\end{bmatrix} & 6 \leftarrow \begin{bmatrix}(1,0)^t\\(0,1)^t\end{bmatrix} & 7 \leftarrow \begin{bmatrix}(1,0)^t\\(1,1)^t\end{bmatrix}\\
8 \leftarrow \begin{bmatrix}(0,1)^t\\(0,0)^t\end{bmatrix} & 9 \leftarrow \begin{bmatrix}(0,1)^t\\(1,0)^t\end{bmatrix} & 10 \leftarrow \begin{bmatrix}(0,1)^t\\(0,1)^t\end{bmatrix} & 11 \leftarrow \begin{bmatrix}(0,1)^t\\(1,1)^t\end{bmatrix}\\
12 \leftarrow \begin{bmatrix}(1,1)^t\\(0,0)^t\end{bmatrix} & 13 \leftarrow \begin{bmatrix}(1,1)^t\\(1,0)^t\end{bmatrix} & 14 \leftarrow \begin{bmatrix}(1,1)^t\\(0,1)^t\end{bmatrix} & 15 \leftarrow \begin{bmatrix}(1,1)^t\\(1,1)^t\end{bmatrix}.
\end{array}$$

Next, by applying Thomae's formulae [12, Ex.6.2.2], we obtain:

$$\begin{array}{ll}
\left(\dfrac{\theta_1}{\theta_0}\right)^4 = \dfrac{\mu(\lambda-1)(\nu-1)}{\lambda\nu(\mu-1)}, & \left(\dfrac{\theta_2}{\theta_0}\right)^4 = \dfrac{\mu(\lambda-1)(\nu-\mu)}{\lambda(\mu-1)(\nu-\lambda)},\\
\left(\dfrac{\theta_4}{\theta_0}\right)^4 = \dfrac{\mu}{\lambda\nu}, & \left(\dfrac{\theta_8}{\theta_0}\right)^4 = \dfrac{\mu(\lambda-\mu)(\nu-1)}{\nu(\mu-1)(\lambda-\nu)}.
\end{array}$$

For each element $(\theta_i/\theta_0)^4$ with $i \in 1, 2, 4, 8$, making a choice of a square root corresponds to a symplectic isomorphism. More precisely, for each root choice there exists a corresponding element $\gamma \in \Gamma_2/\Gamma_{2,4}$ that changes the sign of $(\theta_i/\theta_0)^2$ but preserves the squares of all the other theta constants of level $(2,2)$. Hence, we are allowed to take arbitrary square roots of the above formulas and in addition, we obtain the squares of all other non null theta constants via:

$$\left(\frac{\theta_6}{\theta_0}\right)^2 = \frac{1}{\nu}\left(\frac{\theta_2}{\theta_0}\right)^2\cdot\left(\frac{\theta_0}{\theta_4}\right)^2, \quad \left(\frac{\theta_{12}}{\theta_0}\right)^2 = \frac{1}{\lambda}\left(\frac{\theta_8}{\theta_0}\right)^2\cdot\left(\frac{\theta_0}{\theta_4}\right)^2$$

and

$$\begin{aligned}
\left(\frac{\theta_3}{\theta_0}\right)^2 &= (\nu-1)\left(\frac{\theta_4}{\theta_0}\right)^2\cdot\left(\frac{\theta_6}{\theta_0}\right)^2\cdot\left(\frac{\theta_0}{\theta_1}\right)^2,\\
\left(\frac{\theta_9}{\theta_0}\right)^2 &= (\lambda-1)\left(\frac{\theta_4}{\theta_0}\right)^2\cdot\left(\frac{\theta_{12}}{\theta_0}\right)^2\cdot\left(\frac{\theta_0}{\theta_1}\right)^2,\\
\left(\frac{\theta_{15}}{\theta_0}\right)^2 &= \frac{\nu-\mu}{\nu-1}\left(\frac{\theta_1}{\theta_0}\right)^2\cdot\left(\frac{\theta_{12}}{\theta_0}\right)^2\cdot\left(\frac{\theta_0}{\theta_2}\right)^2.
\end{aligned}$$

In order to obtain theta constants of level $(2,2)$, we need to further choose square roots in the above formulas. Each root choice corresponds to a certain isomorphism $\gamma \in \Gamma_{2,4}/\Gamma_{4,8}$ (that preserves all the other theta coordinates of level 4).

Given the squares of the theta constants $\widetilde{0}_{\mathcal{L}^2}$ of level $(2,2)$, we compute an affine theta null point for the compatible theta structure $\Theta_{\mathcal{L}}$ on $(A, \mathcal{L})$ of level 2. First, the isomorphism $\overline{\Theta}$ induces an isomorphism $\overline{\Theta}_{\mathcal{L}} \colon \mathbf{Z}(2) \xrightarrow{\sim} K_1(\mathcal{L})$. The projective theta coordinates of a point x are of the form $\left(\theta_b^{\Theta_{\mathcal{L}}}(x)\right)_{b \in \mathbf{Z}(2)}$, where b corresponds to a unique element in $K_1(\mathcal{L})$ via $\Theta_{\mathcal{L}}$.

For each $b \in \mathbf{Z}(2)$, there exists a transformation formula [12, p.39]:

$$\theta_b^{\Theta_{\mathcal{L}}}(0) \cdot \theta_0^{\Theta_{\mathcal{L}}}(0) = \sum_{a \in \mathbf{Z}(2)} \theta_{a,b}^{\Theta_{\mathcal{L}^2}}(0)^2. \tag{4.2}$$

We are allowed to choose any affine theta null point and therefore, to avoid unnecessary inversions, we could compute directly $\theta_b^{\Theta_{\mathcal{L}}}(\widetilde{0}_{\mathcal{L}}) = \sum_{a \in \mathbf{Z}(2)} \theta_{a,b}^{\Theta_{\mathcal{L}^2}}(\widetilde{0}_{\mathcal{L}^2})^2$ for all $b \in \mathbf{Z}(2)$.

Remark 10. To do operations of chain addition and chain multiplication on the Kummer surface $\widetilde{A}/\pm 1$, we assume that we are in the generic case [22, 50], namely, for all $a, b \in \mathbf{Z}(2)$ we have:

$$\sum_{c \in \mathbf{Z}(2)} (-1)^{a^t c} \theta_{b+c}^{\Theta_{\mathcal{L}}}(\widetilde{0}_{\mathcal{L}}) \theta_c^{\Theta_{\mathcal{L}}}(\widetilde{0}_{\mathcal{L}}) \neq 0. \tag{4.3}$$

Recall that $\widetilde{0}_{\mathcal{L}^2}$ is a level $(2, 2)$ affine theta null point for a compatible symmetric theta structure $\Theta_{\mathcal{L}^2}$. We notice that for each $a, b \in \mathbf{Z}(2)$ the sum in (4.3) corresponds to the squares $4\left(\theta_{a,b}^{\Theta_{\mathcal{L}^2}}(\widetilde{0}_{\mathcal{L}^2})\right)^2$, and therefore the sums are a priori computed from the Rosenhain invariants. To reduce the cost of computing chain additions, we rescale the theta coordinates such that $\left(\theta_{a,b}^{\Theta_{\mathcal{L}^2}}(\widetilde{0}_{\mathcal{L}^2})\right)^2 = 1$, when $a = b = (0\,0)$ [50, §. 5].

4.3 Principal Polarizations and Totally Positive Real Endomorphisms

Recall from Section 4.1.1 that the Jacobian variety A is ordinary, of CM-type (K, Φ) and admits maximal real multiplication. As before, let $\mathcal{L}_0$ be the canonical principal polarization on A for which the map $\varphi_{\mathcal{L}_0} \colon A \to A^\vee$ is the corresponding polarization isomorphism.

According to [56, p.61], the principal polarization $\mathcal{L}_0$ on A yields a Rosati involution on the endomorphism algebra $\mathrm{End}(A) \otimes \mathbf{Q}$ defined by

$$f \mapsto f^\dagger := \varphi_{\mathcal{L}_0}^{-1} \circ f^\vee \circ \varphi_{\mathcal{L}_0},$$

where $f^\vee \colon A^\vee \to A^\vee$ is the dual isogeny [56, §. 9].

Let $A[\ell]$ denote the space of ℓ-torsion points on A that are defined over the algebraic closure $\overline{\mathbf{F}}_q$. If ℓ is a prime different from the residue characteristic of $\mathbf{F}_q$, we define the Weil pairing as the bilinear map $e_\ell \colon T_\ell A \times T_\ell A \to \mathbf{Z}_\ell(1)$, where $T_\ell A$ is the Tate module, $\mathbf{Z}_\ell(1) = \lim_{\leftarrow}(\mu_{\ell^n})$ [56, p.58]. Given any isogeny $\varphi \colon A \to A^\vee$, we define the pairing $e_\ell^\varphi \colon T_\ell A \times T_\ell A \to \mathbf{Z}_\ell(1)$ as

$$e_\ell^\varphi(x, y) = e_\ell(x, \varphi y).$$

Note that φ is an isogeny arising from a polarization on A if and only if e_ℓ^φ is an alternating form[56, Prop.13.6]. We extend the pairing to $e_\ell^\varphi \colon T_\ell A \otimes \mathbf{Q} \times T_\ell A \otimes_{\mathbf{Z}_\ell} \mathbf{Q} \to \mathbf{Z}_\ell(1)$.

The following results describe all polarizations on A (up to algebraic equivalence) in terms of the subring of endomorphisms $\mathrm{End}(A)^{++} \subset \mathrm{End}(A)^{+}$ consisting of totally positive endomorphisms [6, p.123], namely the endomorphisms that are symmetric for the Rosati involution. Recall that $\mathrm{NS}(A)$ is identified with the group of symmetric line bundles on A up to algebraic equivalence (see Section 3.2.1).

Proposition 4.3.1. *There is an isomorphism between $NS(A) \otimes \mathbf{Q}$ and $\mathrm{End}(A)^{+} \otimes \mathbf{Q}$ given by $\mathcal{L} \mapsto \varphi_{\mathcal{L}_0}^{-1} \circ \varphi_{\mathcal{L}}$. Moreover, the symmetric (for the Rosati involution) totally positive endomorphisms $\mathrm{End}(A)^{++} \subset \mathrm{End}(A)^{+}$ act simply transitively on the group of symmetric ample line bundles (polarizations) on A, taken up to algebraic equivalence.*

Proof. Let $\mathcal{L}$ be an ample line bundle on A and let $\beta = \varphi_{\mathcal{L}_0}^{-1} \circ \varphi_{\mathcal{L}}$ so that the following diagram commutes:

$$\begin{tikzcd}
A \arrow[dr, "\varphi_{\mathcal{L}_0}"'] & A \arrow[l, "\beta"'] \arrow[d, "\varphi_{\mathcal{L}}"] \\
& A^{\vee}.
\end{tikzcd} \tag{4.4}$$

The statement [56, Prop. 14.2] proves that $\mathrm{NS}(A) \otimes \mathbf{Q}$ is identified with the subset of $\mathrm{End}(A) \otimes \mathbf{Q}$ that is stable under the action of †. We similarly prove that $\beta = \varphi_{\mathcal{L}_0}^{-1} \circ \varphi_{\mathcal{L}}$ is stable under the Rosati involution, i.e., $\beta^{\dagger} = \beta$. To do this, we fix a prime ℓ different from the characteristic of $\mathbf{F}_q$ and show that for β as :

$$e_\ell(x, \varphi_{\mathcal{L}_0} \circ \beta x') = e_\ell(x, \beta^{\vee} \circ \varphi_{\mathcal{L}_0} x'), \qquad \forall x \in T_\ell A \otimes \mathbf{Q}, \forall x' \in T_\ell A \otimes \mathbf{Q}.$$

The above equation is indeed true. We write

$$\begin{aligned} e_\ell(x, \beta^{\vee} \circ \varphi_{\mathcal{L}_0} x') &= e_\ell(\beta x, \varphi_{\mathcal{L}_0} x') = \quad e_\ell^{\varphi_{\mathcal{L}_0}}(\beta x, x') \\ &= -e_\ell^{\varphi_{\mathcal{L}_0}}(x', \beta x) = \quad -e_\ell^{\varphi_{\mathcal{L}_0} \circ \beta}(x', x) = \quad e_\ell(x, \varphi_{\mathcal{L}_0} \circ \beta x'), \end{aligned}$$

where the last equality holds since $e_\ell^{\phi_0 \circ \beta}$ is alternating (as corresponds to the polarization $\mathcal{L}$). Consequently, $\beta^{\vee} \circ \varphi_{\mathcal{L}_0} = \varphi_{\mathcal{L}_0} \circ \beta$ or equivalently, $\varphi_{\mathcal{L}_0}^{-1} \circ \beta^{\vee} \circ \varphi_{\mathcal{L}_0} = \beta$ and so, β is stable under the Rosati involution.

Next, we check that since A is ordinary then β is a totally positive in $\mathrm{End}^{+}(A)$. We do this via the canonical lifting of Serre–Tate [69] that allows us to lift A, together with $\mathrm{End}(A)$, to an abelian variety $\widetilde{A}$ over the ring $W(k)$ of Witt vectors of $\mathbf{F}_q$. We next fix an embedding $\imath \colon W(\overline{\mathbf{F}}_q) \hookrightarrow \mathbf{C}$ and let $\widetilde{A}_{\mathbf{C}}$ be the complex abelian variety $\widetilde{A} \otimes_\imath \mathbf{C}$. The polarizations $\mathcal{L}$ and $\mathcal{L}_0$ lift to unique polarizations $\widetilde{\mathcal{L}}$ and $\widetilde{\mathcal{L}_0}$ of $\widetilde{A}_{\mathbf{C}}$, we can apply the results from the last paragraph of Section 3.1.4 dedicated to complex abelian varieties with CM. Let $\xi \in K$ with $\Phi(\xi) \in (i\mathbf{R}_{>0})^2$ be an element corresponding to $\widetilde{\mathcal{L}_0}$ and $\xi' \in K$ with $\Phi(\xi') \in (i\mathbf{R}_{>0})^2$ be an element corresponding to $\widetilde{\mathcal{L}}$ (unique up to multiplication by a totally positive unit in K_0). Then there exists $\beta \in K$ such that $\beta = \xi'/\xi$ with $\varphi(\beta) > 0$ for all $\varphi \in \Phi$, that is β is totally positive.

Conversely, given an endomorphism β satisfying the conditions of the proposition, there exists a polarization $\widetilde{\mathcal{L}_0}^{\beta}$ fitting in the commutative diagram:

$$\begin{tikzcd}
\widetilde{A}_{\mathbf{C}} \arrow[dr, "\varphi_{\widetilde{\mathcal{L}}_0}"'] & \widetilde{A}_{\mathbf{C}} \arrow[l, "\beta"'] \arrow[d, "\varphi_{\widetilde{\mathcal{L}_0}^{\beta}}"] \\
& \widetilde{A}^{\vee}_{\mathbf{C}}.
\end{tikzcd} \tag{4.5}$$

To conclude, we use[6, Prop.5.2.1 and Thm.5.2.4], applied to $\widetilde{A}_{\mathbf{C}}$. The results show that β is indeed a (totally positive) element in K_0. More precisely, the action of all real endomorphisms on $\widetilde{A}_{\mathbf{C}}$ gives an isomorphism between $\mathrm{End}(\widetilde{A}_{\mathbf{C}})^{+}$ (up to equivalence given by units) and $\mathrm{NS}(\widetilde{A}_{\mathbf{C}})$. This isomorphism restrict to an isomorphism between $\mathrm{End}(\widetilde{A}_{\mathbf{C}})^{++}$ and the polarizations on $\widetilde{A}_{\mathbf{C}}$ considered up to algebraic equivalence.

The polarizations $\mathcal{L}_0, \mathcal{L}$ that correspond to $\widetilde{\mathcal{L}}_0$ and $\widetilde{\mathcal{L}}_0^{\beta}$ satisfy the same property above, namely there exists a totally positive element in K_0 such that $\varphi_{\mathcal{L}_0} \circ \beta = \varphi_{\widetilde{\mathcal{L}}}$. Since any endomorphism $\mathrm{End}(\widetilde{A}_{\mathbf{C}})$ over $\mathbf{C}$ correspond to a unique endomorphism over $\mathbf{F}_q$, we conclude that any polarization on A arises from an element in $\mathrm{End}(A)^{++}$. □

Corollary 4.3.2. *If α is a totally positive endomorphism of A, then $\alpha^*\mathcal{L}_0$ is algebraically equivalent to $\mathcal{L}_0^{\overline{\alpha}\alpha}$.*

4.4 Principal Polarizations on A/G Induced from Principal Polarizations on A

In this section, we want to prove that the target $B := A/G$ is principally polarizable and moreover, we want to explicitly describe such a polarization $\mathcal{M}_0$ in a way that allows us to compute theta null points of level 4 for a suitable theta structure $\Theta_{\mathcal{M}_0^4}$. In the end, that allows us to recover the Rosenhain invariants of a curve C' whose Jacobian is isomorphic to $(B, \mathcal{M}_0)$. The main tool for achieving this will be the following lemma that is valid over any field $\mathbf{F}_q$.

Lemma 4.4.1. *Let $(A, \mathcal{L}_0)$ be a principally polarized abelian variety defined over a field $\mathbf{F}_q$. Let $G \subset A$ be a finite $\mathbf{F}_q$-rational subgroup, and $f\colon A \to B = A/G$ be the corresponding isogeny. Then B admits a principal polarization if and only if there exists a totally positive real endomorphism $\beta \in \mathrm{End}(A)^{++}$ such that G is a maximal isotropic subgroup for the commutator pairing $e_{\mathcal{L}_0^{\beta}}$.*

Proof. If B admits a principal polarization $\mathcal{M}_0$, we apply the proposition 4.3.1 to $f^*\mathcal{M}_0$, so there exists an endomorphism β making the following diagram commute:

$$\begin{tikzcd}
A \arrow[dr, "\varphi_{\mathcal{L}_0}"'] & A \arrow[l, "\beta"'] \arrow[r, "f"] \arrow[d, "\varphi_{f^*\mathcal{M}_0}"] & B \arrow[d, "\varphi_{\mathcal{M}_0}"] \\
& A^{\vee} & B^{\vee}. \arrow[l, "f^{\vee}"']
\end{tikzcd} \tag{4.6}$$

It is easy to check that β is symmetric, it is positive because $\mathcal{L}_0^{\beta} \cong f^*\mathcal{M}_0$ is ample (see Proposition 4.3.1), and G is maximal isotropic inside $\ker(\phi_{\mathcal{L}_0^{\beta}})$ for degree reasons with respect to $e_{\mathcal{L}_0^{\beta}}$. Conversely, given an endomorphism β satisfying the conditions of the lemma, let $\mathcal{L}_0^{\beta}$ be a line bundle corresponding to

$\varphi_{\mathcal{L}_0} \circ \beta$. Then $\mathcal{L}_0^\beta$ descends under f to a polarization $\mathcal{M}_0$ by descent theory [66, Prop.2.4.7], and the following diagram is commutative

$$\begin{tikzcd}
A \arrow[dr, "\varphi_{\mathcal{L}_0}"'] & A \arrow[l, "\beta"'] \arrow[r, "f"] \arrow[d, "\varphi_{\mathcal{L}_0^\beta}"] & B \arrow[d, "\varphi_{\mathcal{M}_0}"] \\
 & A^\vee & B^\vee . \arrow[l, "f^\vee"']
\end{tikzcd} \tag{4.7}$$

Thus, $f^*\mathcal{M}_0$ is algebraically equivalent to $\mathcal{L}_0^\beta$. Finally, since the degree of β is equal to $\deg f \deg f^\vee = \deg f^2$, then the degree of $\varphi_{\mathcal{M}_0}$ is 1 and hence, $\mathcal{M}_0$ is a principal polarization. □

Remark 11. There is a principal polarization on A/G if and only if there exists a totally positive real element $\beta \in \mathrm{End}(A)^+$ of norm ℓ such that $G \subset A[\beta]$ is a maximal isotropic subgroup for the commutator pairing $e_{\mathcal{L}_0^\beta}$. In our case, given the input of the algorithm 4.1.1, there exists such real endomorphism β and the kernel G is cyclic.

4.5 Real Endomorphisms

Recall the conditions 4.8.2 regarding real multiplication on A (in the statement of Theorem 4.1.1). In this section, we aim to compute the action of $\omega = \sqrt{D}$ on 2-torsion points, ℓ-torsion points and $\mathbf{F}_q$-rational subgroup $\langle x \rangle$.

First, we present a naive method of computing $\beta = a + b\sqrt{D} \in \mathcal{O}_0$, where $a, b > 0$ are the smallest integers such that β is of norm ℓ and totally positive. The method works if and only if there exists a totally positive element $\beta \in \mathcal{O}_0$ of norm ℓ.

4.5.1 Precomputation Phase: $\beta \in K_0$

If it exists, the endomorphism β of degree ℓ^2 is identified with an element in $\mathcal{O}_0$ that has norm ℓ. In the case of the fundamental discriminant being 0 modulo 4 ($D = 2, 3 \pmod 4$), the endomorphism corresponds to some totally positive element $\beta = a + b\sqrt{4D} \in \mathcal{O}_0$, with integers $a, b > 0$, of norm ℓ. Choosing a suitable β first amounts to finding integers $a, b > 0$ such that $a^2 - 4b^2D = \ell$. One naive approach is to pick the smallest even b such that $b^2D + \ell$ is a square. Next, the parameter a is equal to the positive square root of $b^2D + \ell$ and it is easy to verify that $\beta = \sqrt{b^2D + \ell} + b/2\sqrt{4D} \in \mathcal{O}_0$ is indeed totally positive and of norm ℓ. In the case of $D = 1 \pmod 4$, the element is of the form $\beta = a + \frac{b}{2}(1 + \sqrt{D})$. The norm of β is ℓ if and only if there exists b such that $b^2D/4 + \ell$ is a square. One naive approach is to pick again the smallest even number b that satisfies this condition. If $b' = b/2$, the parameter a becomes $\sqrt{b'^2D + \ell} - b'$ and in the end, the endomorphism has a similar form of $\beta = \sqrt{b'^2 + \ell} + b'\sqrt{D}$ for the smallest positive integer b'.

4.5.2 A Suitable Decomposition of β as Sum of r-squares

Following Section 4.1, we need to compute a matrix $F \in M_r(K_0)$ that satisfies $FF^t = \beta\mathrm{Id}$, where $r = 2, 4$. This allows us to obtain a principal polarization on the target B in section 4.6. In this paragraph, we present a method that decomposes $\beta \in \mathcal{O}_0$ as a sum of 4 squares in K_0 (where some of them might be 0). The idea is based on the equality $\beta^2 + \ell - 2c\beta = \beta(\beta + \beta^c) - 2c\beta = 2(\mathrm{Tr}(\beta) - c)\beta$, for any positive integer $c < Tr(\beta)$. Afterwards, let $\ell = \sum_{s=1}^{4} \ell_s^2$ for some integers $\ell_i \geq 0$. We notice that $m = 2\,\mathrm{Tr}(\beta) - 2\ell_1 = 2(\sqrt{b^2 D + \ell} - \ell_1)$ is also a strictly positive integer and so, we write it as a sum of 4 squares of the form $m = \sum_{s=1}^{4} m_s$, for some integers $m_s \geq 0$ that are not all zero. Next, we consider a 4-by-4 integer matrix N with $m_1, \ldots, m_4$ on the first column. Then, if $z = (\beta - \ell_1, \ell_2, \ell_3, \ell_4)$, we have $z \cdot z^t = m\beta$. The decomposition of $mI_4 = N \cdot N^t$ implies that $1/m = (N^t)^{-1} N^{-1}$. We pick $(\alpha_1, \ldots, \alpha_4) = z \cdot (N^t)^{-1} \in K_0^r$ and β is indeed equal to the sum of 4 squares $\alpha_1^2 + \ldots + \alpha_s^2$. As $(N^t)^{-1}$ is equal to $1/mN \in M_4(\mathbf{Q})$, we notice that the denominators in the expression of α_s are most likely even. Here, the assumption that the index of $\mathbf{Z}[\pi, \overline{\pi}]$ in $\mathcal{O}$ is odd will guarantee that the polynomial in Frobenius of α_s has odd denominators. On the other hand, if we choose ℓ_1 such that m is prime to ℓ and Q, we can compute the expression of α_s on ℓ-torsion points and on the rational subgroup of $A(\mathbf{F}_q)$ of order Q.

4.5.3 Computing Real Endomorphisms on Certain Points of A

First we understand the action of a real endomorphism on the isogeny kernel G and on the rational subgroup of order Q. For that we consider the Frobenius polynomial

$$\chi_\pi(T) = T^4 - s_1 T^3 + (s_2 + 2q)T^2 - q s_1 T + q^2, \tag{4.8}$$

where s_1 and s_2 satisfy $s_1^2 - 4s_2 > 0$ and $s_2 + 4q > 2|s_1|\sqrt{q}$ (Rück bounds) and $|s_1| \leq 4\sqrt{q}$ and $|s_2| \leq 4q$ (Weil bounds). Given an endomorphism $\gamma \in \mathrm{End}^0(A)$, let $f_\gamma = a_0 + a_1 T + a_2 T^2 + a_3 T^3$ be the degree 3 polynomial that satisfies $\gamma = f_\gamma(\pi)$. The goal is to compute the endomorphism ω by using the fact that ω^2 is scalar multiplication by $D = s_1^2 - 4s_2$. In addition, $\omega = 2\pi + 2\overline{\pi} - s_1$, where $\overline{\pi}$ is the complex conjugate (in K) of π. We can now write $\overline{\pi}$ as a polynomial in π and derive the requested polynomial. More precisely,

$$\pi^3 - s_1\pi^2 + (s_2 + 2q)\pi - q s_1 = -\frac{q^2}{\pi} = -q\overline{\pi},$$

and hence,

$$\omega = -2q^{-1}\pi^3 + 2q^{-1}s_1\pi^2 - 2(q^{-1}s_2 + 1)\pi + s_1, \tag{4.9}$$

i.e., $f_\omega(T) = -2q^{-1}T^3 + 2q^{-1}s_1 T^2 - 2(q^{-1}s_2 + 1)T + s_1$. Given a prime p, we denote by $f_{\omega,p}(T)$ the polynomial $f_\omega(T)$ whose coefficients are reduced modulo p.

Let x be a rational point of order Q and let t be a generator of $G = \mathrm{Ker}(f)$. Consider a real endomorphism $\gamma = u + v\sqrt{D} \in \mathcal{O}_0$. If we reduce both coefficients modulo ℓ, namely $u_\ell = u \pmod{\ell}$ and $v_\ell = v \pmod{\ell}$, then $u_\ell + v_\ell f_{\omega,\ell}(T)$ represents the action of γ on ℓ-torsion points and in particular on $\langle t \rangle$. In addition, the group $\langle t \rangle$ is stable under Frobenius and hence, in this particular case, there exists a scalar s_t in $\mathbf{Z}/\ell\mathbf{Z}$ such that $\pi(t) = s_t \cdot t$. We denote by $c_t = f_{\omega,\ell}(s_t) \in \mathbf{Z}/\ell\mathbf{Z}$ the action of $\sqrt{D}$ on any point in G. Consequently, any real endomorphism γ acts on G as multiplication by a scalar $c_{\gamma,t} = u_\ell + v_\ell c_t$.

In the other case, we proceed in a similar manner as the Frobenius (with respect to $\mathbf{F}_q$) is the identity on the rational group $\langle x \rangle$. Hence, to compute $\sqrt{D}$ on x we evaluate the polynomial $f_{\omega,Q}$ at 1, i.e., $c_Q = f_{\omega,Q}(1) \in \mathbf{Z}/Q\mathbf{Z}$. Then, the endomorphism γ is once again multiplication by a scalar, more precisely $c_{\gamma,x} = u_Q + v_Q c_Q$.

Naturally the next question is how to compute real endomorphisms in practice. In the case of x and t in theta coordinates, we use the methods of chain addition and chain multiplication from Section 3.2.6.

4.6 Computing the Target Isogeny

Following the arguments given in Section 4.1, we use the β-contragrediant isogeny $\widehat{f}\colon B \to A$ instead of $f\colon A \to B$ in order to compute the target variety B. Following the argument from Section 4.4 there exists a principal polarization on B whose pullback via isogeny f is algebraically equivalent to $\mathcal{L}_0^\beta$. Moreover, as β is totally positive then the line bundle $\mathcal{M}_0^\beta$ is indeed an ample line bundle. Next lemma proves there exists a connection between the line bundles $\mathcal{M}_0^\beta$ and $\mathcal{L}_0$ given by the β-contragredient isogeny $\widehat{f}$.

Lemma 4.6.1. *Let $\mathcal{M}_0$ be the principal polarization on B and let $\mathcal{M}_0^\beta$ be the ample line bundle on B whose polarization isogeny $\varphi_{\mathcal{M}_0^\beta}$ is $\varphi_{\mathcal{M}_0} \circ \beta\colon B \to B^\vee$. Then $\widehat{f}^*\mathcal{L}_0$ is algebraically equivalent to $\mathcal{M}_0^\beta$.*

Proof. By Proposition 4.3.1 applied to $(B, \mathcal{M}_0)$, there exists $\gamma \in \mathrm{End}(B)^{++}$ such that $\widehat{f}^*\mathcal{L}_0$ is algebraically equivalent to $\mathcal{M}_0^\gamma$. Now, we have $f^*\mathcal{M}_0^\gamma = \mathcal{L}_0^{\beta\gamma}$ and $f^*\mathcal{M}_0^\gamma = (f \circ \widehat{f})^*\mathcal{L}_0 = \beta^*\mathcal{L}_0 = \mathcal{L}_0^{\beta^2}$ where the last equality comes from Corollary 4.3.2 and the fact that β is a real endomorphism. By applying Proposition 4.3.1 again, we get that $\beta = \gamma$. □

Remark 12. The line bundles satisfy $(\widehat{f}^*\mathcal{L}_0)^2 = \widehat{f}^*\mathcal{L}_0^2 = \widehat{f}^*\mathcal{L}$, as $2 \nmid \ell$, and $(\mathcal{M}_0^\beta)^2 = \mathcal{M}^\beta$. Therefore, $\widehat{f}^*\mathcal{L}$ is algebraically equivalent to $\mathcal{M}^\beta$. Since $\mathcal{L}_0$ and $\mathcal{M}_0$ are symmetric, it implies that $\widehat{f}^*\mathcal{L}$ is linearly equivalent to $\mathcal{M}^\beta$ that is also totally symmetric as $\mathcal{M}$ is totally symmetric.

The advantage of this approach is that expressing a choice of theta constants for $(B, \mathcal{M}^\beta, \Theta_{\mathcal{M}^\beta})$ from a choice of theta constants for $(A, \mathcal{L}, \Theta_{\mathcal{L}})$ via $\widehat{f}$ no longer involves solving systems of polynomial equations as explained in the subsection below.

4.6.1 Isogeny Theorem for $\widehat{f}$

Lemma 4.6.1 shows that $\widehat{f}\colon (B, \mathcal{M}^\beta) \to (A, \mathcal{L})$ is indeed an isogeny of polarized abelian varieties. Let $\Theta_{\mathcal{M}^\beta}$ be a theta structure on $(B, \mathcal{M}^\beta)$ compatible with the theta structure $\Theta_{\mathcal{L}}$, i.e., such that the isogeny $\widehat{f}\colon (B, \mathcal{M}^\beta, \Theta_{\mathcal{M}^\beta}) \to (A, \mathcal{L}, \Theta_{\mathcal{L}})$ is an isogeny of polarized abelian varieties with theta structures. The theta structure $\Theta_{\mathcal{M}^\beta}$ induces a symplectic decomposition of the 2β-torsion points $K(\mathcal{M}^\beta) = K_1(\mathcal{M}^\beta) \oplus K_2(\mathcal{M}^\beta)$. Since $K_i(\mathcal{M}^\beta) = K_i(\mathcal{M}^\beta)[\beta] \oplus K_i(\mathcal{M}^\beta)[2]$, we have a symplectic decomposition $K_1(\mathcal{M}^\beta)[2] \oplus K_2(\mathcal{M}^\beta)[2]$ of $B[2]$ which yields (via $\widehat{f}$) the symplectic decomposition on $K(\mathcal{L}) = A[2]$ determined by the theta structure $\Theta_{\mathcal{L}}$.

If we assume that the kernel $\widehat{G}$ of $\widehat{f}$ is $K_2(\mathcal{M}^\beta)[\beta]$ (which we can always do since the compatibility requirement on $\Theta_{\mathcal{M}^\beta}$ is only on the 2-torsion and not on the β-torsion points), the kernel G of f coincides with $\widehat{f}(K_1(\mathcal{M}^\beta)[\beta])$. Moreover, the isogeny $\widehat{f}$ induces an isomorphism between $K_1(\mathcal{M}^\beta)[2]$ and $K_1(\mathcal{L})$ and significantly simplifies the formula appearing in the isogeny theorem (3.2.7) applied to $\widehat{f}$.

Given the theta structures $\Theta_{\mathcal{L}}$ and $\Theta_{\mathcal{M}^\beta}$, consider the corresponding affine systems of coordinates $\theta_i^{\Theta_{\mathcal{L}}}\colon \widetilde{A} \to \overline{\mathbf{F}}_q$ and $\theta_j^{\Theta_{\mathcal{M}^\beta}}\colon \widetilde{B} \to \overline{\mathbf{F}}_q$. Let $\widetilde{\widehat{f}}\colon \widetilde{B} \to \widetilde{A}$ be the canonical affine isogeny corresponding to $\widehat{f}$ and the systems of coordinates (check Definition 3.2.9). We fix an affine lift $\widetilde{y}$ of a point $y \in B$ for the theta structure $\Theta_{\mathcal{M}^\beta}$. Let $\widetilde{\widehat{f}(y)}$ be the affine lift of $\widehat{f}(y) \in A$ such that for all $i \in K_1(\mathcal{L})$, we have:

$$\theta_i^{\Theta_{\mathcal{L}}}(\widetilde{\widehat{f}(y)}) = \theta_j^{\Theta_{\mathcal{M}^\beta}}(\widetilde{y}), \tag{4.10}$$

where $j \in K_1(\mathcal{M}^\beta)[2]$ is the unique preimage of i via $\widehat{f}$ (note that $\widehat{G}^{1,\perp} = K_1(\mathcal{M}^\beta)[2]$ and $\widehat{G}_1 = 0$ since $\widehat{G} \subset K_2(\mathcal{M}^\beta)$).

4.6.2 Isogeny Theorem for F

Let F be the r-by-r matrix from Section 4.1. Assuming that the elements of F are identified with polynomials in the Frobenius π with $\mathbf{Q}$-coefficients whose denominators are prime to ℓ as in Section 4.5.3, it is possible to compute the action of the corresponding endomorphism F on the ℓ-torsion points of B^r by simply inverting all denominators modulo ℓ.

We first prove that under the endomoprhism F, the totally symmetric line bundle $\mathcal{M}^{\star r}$ pulls back to $(\mathcal{M}^\beta)^{\star r}$ up to algebraic equivalence:

Lemma 4.6.2. *Given the isogeny $F\colon B^r \to B^r$, the line bundles $F^*\mathcal{M}_0^{\star r}$ and $(\mathcal{M}_0^\beta)^{\star r}$ are algebraically equivalent.*

Proof. From Corollary 4.3.2, the line bundle $F^*\mathcal{M}_0^{\star r}$ is algebraically equivalent to $(\mathcal{M}_0^{\star r})^{F^\dagger F}$, where $F^\dagger$ denotes the action of the Rosati involution on $\mathrm{End}(B^r)$ which is given components by components as the Rosati involution acting on the coefficients of the transpose of F. Since F is composed of totally positive real quadratic endomorphisms α, then $\alpha^\dagger = \alpha$ and consequently, $F^\dagger = F^t$. Furthermore since $F^t F = \beta \mathrm{Id}$ we get that $F^*\mathcal{M}_0^{\star r}$ is algebraically equivalent to $(\mathcal{M}_0^\beta)^{\star r}$. □

Since $\mathcal{L}_0$ and $\mathcal{M}_0$ are symmetric, then the line bundles $\mathcal{L}$ and $\mathcal{M}$ are totally symmetric. In addition, as $F^*\mathcal{M}_0^{\star r}$ is algebraically equivalent to $(\mathcal{M}_0^\beta)^{\star r}$, the two line bundles $F^*\mathcal{M}^{\star r}$ and $(\mathcal{M}^\beta)^{\star r}$ are totally symmetric. This means that we have an isogeny $F\colon (B^r, (\mathcal{M}^\beta)^r) \to (B^r, \mathcal{M}^{\star r})$ of polarized abelian gr-folds. Consider the r-fold product theta structure $\Theta_{(\mathcal{M}^\beta)^{\star r}}$ on $(B^r, (\mathcal{M}^\beta)^r)$ (determined by $\Theta_{\mathcal{M}^\beta}$ by Definition 3.2.3) and let $\widetilde{\Theta}_{\mathcal{M}^{\star r}}$ be a compatible (for the isogeny F) theta structure on $(B, \mathcal{M}^{\star r})$. We apply the isogeny theorem for the isogeny

$$F\colon (B^r, (\mathcal{M}^\beta)^{\star r}, \Theta_{(\mathcal{M}^\beta)^{\star r}})) \to (B^r, \mathcal{M}^{\star r}, \widetilde{\Theta}_{\mathcal{M}^{\star r}})$$

of principally polarized abelian varieties with compatible theta structures to first compute the theta constants for $\widetilde{\Theta}_{\mathcal{M}^{\star r}}$. The theta structure $\widetilde{\Theta}_{\mathcal{M}^{\star r}}$ induces a symplectic decomposition of $K(\mathcal{M}^{\star r})$ into a direct sum of $K_i(\mathcal{M}^{\star r})$, for $i = 1, 2$.

Since $K_i(\mathcal{M}^\beta) = K_i(\mathcal{M}^\beta)[\beta] \oplus K_i(\mathcal{M}^\beta)[2]$ for $i = 1, 2$, any $k \in K_i(\mathcal{M}^\beta)$ can be written uniquely as $k = t' + j$ where $t' \in K_i(\mathcal{M}^\beta)[\beta]$ and $j \in K_i(\mathcal{M}^\beta)[2]$. The isogeny F has kernel that is a subgroup of the β-torsion points of the form $F_1 \oplus F_2$ with $F_i \subset K_i((\mathcal{M}^\beta)^{\star r})[\beta]$ and hence, F is an isomorphism at the level of 2-torsion points.

As in the previous section, given the theta structures $\widetilde{\Theta}_{\mathcal{M}^{\star r}}$ and $\Theta_{(\mathcal{M}^\beta)^{\star r}}$, we consider the corresponding affine systems of coordinates, $\theta_{\mathbf{i}}^{\widetilde{\Theta}_{\mathcal{M}^{\star r}}} : \widetilde{B}^r \to \overline{\mathbf{F}}_q^r$ and $\theta_{\mathbf{j}}^{\Theta_{(\mathcal{M}^\beta)^{\star r}}} : \widetilde{B}^r \to \overline{\mathbf{F}}_q^r$ respectively. Consider the canonical affine isogeny $\widetilde{F}\colon \widetilde{B} \to \widetilde{B}$ corresponding to F and the given affine system of coordinates (see Definition 3.2.9). Let $\widetilde{y^{\star r}}$ be an arbitrary affine lift of $y^{\star r} \in B^r$ for the theta structure $\Theta_{(\mathcal{M}^\beta)^{\star r}}$. Let

$\widetilde{F(y^{\star r})}$ be the affine lift of $F(y^{\star r})$ such that for all $\mathbf{k} \in K_1(\mathcal{M}^{\star r})$, the following relation holds

$$\theta_{\mathbf{k}}^{\widetilde{\Theta}_{\mathcal{M}^{\star r}}}(\widetilde{F(y^{\star r})}) = \sum_{\substack{\mathbf{t'} \in K_1((\mathcal{M}^{\beta})^{\star r})[\beta] \\ F(\mathbf{t'})=0}} \theta_{\mathbf{j}+\mathbf{t'}}^{\Theta_{(\mathcal{M}^{\beta})^{\star r}}}(\widetilde{y^{\star r}}), \tag{4.11}$$

where $\mathbf{j} \in K_1((\mathcal{M}^{\beta})^{\star r})[2]$ is the unique element satisfying $F(\mathbf{j}) = \mathbf{k}$.

4.6.3 Computing the Theta Constants of B

In this section, we focus on how to compute affine theta constants of the target variety B from an affine theta null point $\widetilde{0}_{\mathcal{L}}$.

Let $\widetilde{0}_{\mathcal{L}}$ be an affine lift of the theta null point of A for the theta structure $\Theta_{\mathcal{L}}$ (computed with Thomae's formulae in Section 4.2). According to the definition of the affine isogeny $\widetilde{\widehat{f}}$, there exists a unique affine theta null point $\widetilde{0}_{\mathcal{M}^{\beta}}$ of $\widetilde{B}$ such that (4.10) holds, namely for all $i \in K_1(\mathcal{L})$,

$$\theta_i^{\Theta_{\mathcal{L}}}(\widetilde{0}_{\mathcal{L}}) = \theta_j^{\Theta_{\mathcal{M}^{\beta}}}(\widetilde{0}_{\mathcal{M}^{\beta}}), \tag{4.12}$$

where $j \in K_1(\mathcal{M}^{\beta})[2]$ is the unique preimage of i via $\widehat{f}$.

Let $\widetilde{t'}$ be an affine lift of $t' \in K_1(\mathcal{M}^{\beta})$ that is compatible with the choice of the affine lift of $\widetilde{0}_{\mathcal{M}^{\beta}}$ (see definition 3.2.8). Then, by definition of compatibility, for any $j \in K_1(\mathcal{M}^{\beta})[2]$ we have

$$\theta_{j+t'}^{\Theta_{\mathcal{M}^{\beta}}}(\widetilde{0}_{\mathcal{M}^{\beta}}) = \theta_j^{\Theta_{\mathcal{M}^{\beta}}}(\widetilde{t'}). \tag{4.13}$$

Following equation (4.10) with $t' \in K_1(\mathcal{M}^{\beta})$, then there exists a unique affine lift of $\widehat{f}(t')$ such that for any index $j \in K_1(\mathcal{M}^{\beta})[2]$ we have:

$$\theta_j^{\Theta_{\mathcal{M}^{\beta}}}(\widetilde{t'}) = \theta_i^{\Theta_{\mathcal{L}}}(\widetilde{\widehat{f}(t')}), \tag{4.14}$$

where $i \in K_1(\mathcal{L})$ with $\widehat{f}(j) = i$. Since $\widehat{G} \subset K_2(\mathcal{M}^{\beta})[\beta]$, then $\widehat{f}(t') \in G$ for any $t' \in \widehat{G}$. Then, the affine lift $\widetilde{\widehat{f}(t')}$ of $t \in G$ satisfying equation (4.14) is compatible with respect to the affine isogeny $\widetilde{\widehat{f}}$ (check definition 3.2.10).

Since $\Theta_{(\mathcal{M}^{\beta})^{\star r}}$ is a product theta structure, let $\widetilde{0}_{(\mathcal{M}^{\beta})^{\star r}}$ be the affine theta null point of $(B^r, (\mathcal{M}^{\beta})^{\star r}, \Theta_{(\mathcal{M}^{\beta})^{\star r}})$ that is determined by $\widetilde{0}_{\mathcal{M}^{\beta}}$. Then, given compatible affine lifts $(\widetilde{t}'_1, \ldots, \widetilde{t}'_r)$ of any $\mathbf{t'} = (t'_1, \ldots, t'_r) \in \widehat{G}^r$, we have that for any index $\mathbf{j} = (j_1, \ldots, j_r) \in K_1((\mathcal{M}^{\beta})^{\star r})[2]$ the following relation holds

$$\theta_{\mathbf{j}+\mathbf{t'}}^{\Theta_{(\mathcal{M}^{\beta})^{\star r}}}(\widetilde{0}_{(\mathcal{M}^{\beta})^{\star r}} = \prod_{s=1}^{r} \theta_{j_s+t'_s}^{\Theta_{\mathcal{M}^{\beta}}}(\widetilde{0}_{\mathcal{M}^{\beta}}) \overset{(4.13)}{=} \prod_{s=1}^{r} \theta_{j_s}^{\Theta_{\mathcal{M}^{\beta}}}(\widetilde{t}'_s) \overset{(4.14)}{=} \prod_{s=1}^{r} \theta_{i_s}^{\Theta_{\mathcal{L}}}(\widetilde{\widehat{f}(t')}), \tag{4.15}$$

where $i_s = \widehat{f}(j_s) \in K_1(\mathcal{L})$ for $s = 1, \ldots r$.

Let $\widetilde{0}_{\mathcal{M}^{\star r}}$ be the affine theta null point for $(B^r, \mathcal{M}^{\star r}, \widetilde{\Theta}_{\mathcal{M}^{\star} r})$ such that for all $\mathbf{k} \in K_1(\mathcal{M}^{\star r})$, equation

(4.11) (with $y^{\star r} = \widetilde{0}_{(\mathcal{M}^\beta)^{\star r}}$) is satisfied

$$\begin{aligned} \theta_{\mathbf{k}}^{\widetilde{\Theta}_{\mathcal{M}^{\star r}}}(\widetilde{0}_{\mathcal{M}^{\star r}}) &= \sum_{\substack{\mathbf{t}'=(t_1',\dots,t_r')\in K_1((\mathcal{M}^\beta)^{\star r})[\beta] \\ F(\mathbf{t}')=0}} \theta_{\mathbf{j}+\mathbf{t}'}^{\Theta_{(\mathcal{M}^\beta)^{\star r}}}(\widetilde{0}_{(\mathcal{M}^\beta)^{\star r}}) \\ &\overset{(4.15)}{=} \sum_{\substack{\mathbf{t}=(t_1,\dots,t_r)\in G^r \\ F(\mathbf{t})=0}} \prod_{s=1}^{r} \theta_{i_s}^{\Theta_{\mathcal{L}}}(\widetilde{t}_s) \end{aligned} \tag{4.16}$$

where $\mathbf{j} = (j_1, \dots, j_r) \in K_1((\mathcal{M}^\beta)^{\star r})[2]$ is the unique preimage of $\mathbf{k}$ under F, index $i_s \in K_1(\mathcal{L})$ is the image of $j_s \in K_1(\mathcal{M}^\beta)[2]$ via $\widehat{f}$ and $\widetilde{t}_s$ is the compatible affine lift of $t_s = \widehat{f}(t_s') \in \mathrm{Ker}(f)$ with respect to $\widetilde{\widehat{f}}$ and $\widetilde{0}_{\mathcal{M}^\beta}$.

Remark 13. Let $\kappa\colon \mathcal{O}_0 \to \mathbf{Z}/\ell\mathbf{Z}$ be the ring homomorphism giving the action of the real multiplication endomorphisms on the points of G (note that κ induces a field isomorphism $\kappa\colon \mathcal{O}_0/\beta \xrightarrow{\sim} \mathbf{Z}/\ell\mathbf{Z}$). In Section 4.5.3, we compute $\alpha_1, \dots, \alpha_r \in K_0$, such that $\sum_{s=1}^r \alpha_s^2 = \beta$. We notice that the least positive integer d such that $d\alpha_s \in \mathcal{O}_0$ for all $s = 1, \dots, r$ is prime to ℓ. Let $d\alpha_s = \alpha_s^1 + \alpha_s^2\sqrt{D}$, where $\alpha_s^1, \alpha_s^2 \in \mathbf{Z}$ and let $b_s = \kappa(d\alpha_s)/\kappa(d) \in \mathbf{Z}/\ell\mathbf{Z}$ represent the action of α_s on elements in G.

In conclusion the matrix representation of the action of endomorphism F on G^r is a matrix in $\mathcal{M}_r(\mathbf{Z}/\ell Z)$. Furthermore, as the matrix satisfies $FF^t = \beta\mathrm{Id}$ and G^r is in the kernel of endomorphism β, there exists $\mathbf{t} = (t_1, \dots, t_r) \in G^r$ such that $F^t(\mathbf{t}) = (\widehat{f}(t_1'), \dots, \widehat{f}(t_r'))$. We notice that the kernel of F inside G^r is of size $\ell^{r/2}$. We distinguish two different cases depending on r. First, when $r = 4$, the kernel of F is of size ℓ^2 and so,

$$\mathrm{Ker}(F) = \{F^t(\mathbf{t}) \,|\, \mathbf{t} = (t_1, t_2, 0, 0),\ t_1, t_2 \in G\}.$$

Else, when $r = 2$, the kernel of F is of size ℓ and so,

$$\mathrm{Ker}(F) = \{F^t(\mathbf{t}) \,|\, \mathbf{t} = (t, 0),\ t \in G\}.$$

From now on, we consider the case $r = 4$ as the other case is immediately deduced from it. Since the matrix F^t is of the form

$$F^t = \begin{pmatrix} b_1 & -b_2 & -b_3 & -b_4 \\ b_2 & b_1 & b_4 & -b_3 \\ b_3 & -b_4 & b_1 & b_2 \\ b_4 & b_3 & -b_2 & b_1 \end{pmatrix},$$

then for any $t_1', \dots, t_4' \in K_1(\mathcal{M}^\beta)[\beta]$ we have

$$(\widehat{f}(t_1'), \dots, \widehat{f}(t_4')) = F^t(t_1, t_2, 0, 0)^t$$

for some $t_1, t_2 \in\ G$.

Remark 14. From now on, let t be a generator of G and let $\widetilde{t}_0$ be the compatible affine lift of t (in level 2 coordinates for $\Theta_{\mathcal{L}}$) with respect to the affine point $\widetilde{0}_{\mathcal{M}^\beta}$ and the isogeny $\widetilde{\widehat{f}}$. Given $t_1, t_2 \in G$, there exist unique $a_1, a_2 \in \mathbf{Z}/\ell\mathbf{Z}$ such that $a_1 t = t_1$ and $a_2 t = t_2$. We consider the compatible affine lift $\widetilde{a_1 t_0} = \texttt{chain\_mult}(a_1, \widetilde{t}_0, \widetilde{0}_{\mathcal{L}})$ of t_1 and the compatible affine lift $\widetilde{a_2 t_0} = \texttt{chain\_mult}(a_2, \widetilde{t}_0, \widetilde{0}_{\mathcal{L}})$ of $\widetilde{t}_2$. Moreover, as $b_1, \dots, b_r$ are also in $\mathbf{Z}/\ell\mathbf{Z}$, then $\widetilde{b_s \cdot a_1 t_0} = \texttt{chain\_mult}(b_s a_1, \widetilde{t}_0, \widetilde{0}_{\mathcal{L}})$ and $\widetilde{b_s \cdot a_2 t_0} = \texttt{chain\_mult}(b_s a_2, \widetilde{t}_0, \widetilde{0}_{\mathcal{L}})$ for any $s = 1, \dots, r$. Next, since we have the same affine lift $\widetilde{t}_0$ determining $\widetilde{b_s \cdot a_1 t_0}$ and $\widetilde{b_s \cdot a_2 t_0}$ for all $s = 1, \dots, r$, we also group all scalars together and consider the compatible affine lifts

$$\begin{array}{rcl} (b_1\widetilde{a_1 - b_2}a_2)t_0 & := & \texttt{chain\_mult}(b_1a_1 - b_2a_2, \widetilde{t_0}, \widetilde{0_{\mathcal{L}}}), \\ (b_2\widetilde{a_1 + b_1}a_2)t_0 & := & \texttt{chain\_mult}(b_2a_1 + b_1a_2, \widetilde{t_0}, \widetilde{0_{\mathcal{L}}}), \\ (b_3\widetilde{a_1 - b_4}a_2)t_0 & := & \texttt{chain\_mult}(b_3a_1 - b_4a_2, \widetilde{t_0}, \widetilde{0_{\mathcal{L}}}), \\ (b_4\widetilde{a_1 + b_3}a_2)t_0 & := & \texttt{chain\_mult}(b_4a_2 + b_3a_2, \widetilde{t_0}, \widetilde{0_{\mathcal{L}}}), \end{array} \tag{4.17}$$

After grouping the scalars as above, equation (4.16) is rewritten as follows. For any index $\mathbf{k} \in K_1(\mathcal{M}^{\star r})$:

$$\begin{array}{rcl} \theta_{\mathbf{k}}^{\widetilde{\Theta}_{\mathcal{M}^{\star r}}}(\widetilde{0}_{\mathcal{M}^{\star r}}) & = & \displaystyle\sum_{a_1,a_2 \in \mathbf{Z}/\ell\mathbf{Z}} \theta_{i_1}^{\Theta_{\mathcal{L}}}((b_1\widetilde{a_1 - b_2}a_2)t_0)\theta_{i_2}^{\Theta_{\mathcal{L}}}((b_2\widetilde{a_1 + b_1}a_2)t_0) \\ & \cdot & \theta_{i_3}^{\Theta_{\mathcal{L}}}((b_3\widetilde{a_1 - b_4}a_2)t_0)\theta_{i_4}^{\Theta_{\mathcal{L}}}((b_4\widetilde{a_1 + b_3}a_2)t_0) \end{array} \tag{4.18}$$

where $i_s = \widehat{f}(j_s) \in K_1(\mathcal{L})$, where $\mathbf{j} = (j_1, \ldots, j_r) \in K_1((\mathcal{M}^{\beta})^{\star r})[2]$ is unique such that $F(\mathbf{j}) = \mathbf{k}$.

Unfortunately in practice, we cannot compute compatible affine lifts of $t \in G$ from the very beginning, when we are given only the affine theta null point $\widetilde{0}_{\mathcal{L}}$ of level 2 together with the Mumford coordinates of t. We first change the coordinates of t from Mumford to theta and take any affine image of the resulting projective point. It yields an affine lift of the form $\widetilde{t} = \lambda_t\widetilde{t_0}$, where $\lambda_t \neq 0$ is unknown. Following previous work of [13, 49], the next step is to figure out how λ_t intervenes when evaluating the RHS of (4.18) when given the affine lifts of a_st as $\texttt{chain\_mult}(a_s, \widetilde{t}, \widetilde{0}_{\mathcal{L}})$ $(s = 1, 2)$. First, Lemma 4.6.3 proves that is necessary to at least compute λ_t^{ℓ} in order to apply equation (4.18).

Lemma 4.6.3. *Let t be a generator of G and let $\widetilde{t_0}$ be the compatible affine lift of t with respect to $\widetilde{0}_{\mathcal{L}}$ (of theta structure $\Theta_{\mathcal{L}}$). Let $\widetilde{t} = \lambda_t\widetilde{t_0}$, with $\lambda_t \in \overline{\mathbf{F}}_q^*$, be an arbitrary lift of t. Given the scalars $b_1, \ldots, b_r$ on the first row of F, and arbitrary $a_1, a_2 \in \mathbf{Z}/\ell\mathbf{Z}$, we denote by $(b_1\widetilde{a_1 - b_2}a_2)t :=$ $\texttt{chain\_mult}(b_1a_1 - b_2a_2, \widetilde{t}, \widetilde{0}_{\mathcal{L}})$, $(b_2\widetilde{a_1 + b_1}a_2)t :=$ $\texttt{chain\_mult}(b_2a_1 + b_1a_2, \widetilde{t}, \widetilde{0}_{\mathcal{L}})$, $(b_3\widetilde{a_1 - b_4}a_2)t :=$ $\texttt{chain\_mult}(b_3a_1 - b_4a_2, \widetilde{t}, \widetilde{0}_{\mathcal{L}})$, $(b_4\widetilde{a_1 + b_3}a_2)t :=$ $\texttt{chain\_mult}(b_4a_2 + b_3a_2, \widetilde{t}, \widetilde{0}_{\mathcal{L}})$. If the product*

$$\theta_{i_1}^{\Theta_{\mathcal{L}}}((b_1\widetilde{a_1 - b_2}a_2)t)\theta_{i_2}^{\Theta_{\mathcal{L}}}((b_2\widetilde{a_1 + b_1}a_2)t)\theta_{i_3}^{\Theta_{\mathcal{L}}}((b_3\widetilde{a_1 - b_4}a_2)t)\theta_{i_4}^{\Theta_{\mathcal{L}}}((b_4\widetilde{a_1 + b_3}a_2)t) \tag{4.19}$$

is defined symbolically as a polynomial in the variable λ_t, then it belongs to $\overline{\mathbf{F}}_q[\lambda_t^{\ell}]$.

Proof. Our proof is similar to the proof of [13, Lem.4.2]. The product (4.19) differs from the product with compatible affine lifts in the RHS of (4.18) by a factor equal to

$$\begin{array}{rcl} \lambda & = & (\lambda_t)^{(b_1a_1 - b_2a_2)^2} \cdot (\lambda_t)^{(b_2a_1 + b_1a_2)^2} \cdot (\lambda_t)^{(b_3a_1 - b_4a_2)^2} \cdot (\lambda_t)^{(b_4a_1 + b_3a_2)^2} = \\ & = & (\lambda_t)^{(b_1^2 + \cdots + b_4^2)(a_1^2 + a_2^2)} = (\lambda_t)^{\kappa(\beta)(a_1^2 + a_2^2)} = \lambda_t^{\ell(a_1^2 + a_2^2)}. \end{array} \tag{4.20}$$

Moreover, if we consider a transformation of $\overline{\mathbf{F}}_q[\lambda_t]$, taking $\lambda_t \mapsto \xi\lambda_t$ for some ℓth root of unity $\xi \in \overline{\mathbf{F}}_q^{\times}$, then the above factor λ remains unchanged as $\xi^{\ell} = 1$. As the ℓth root of unity is chosen arbitrarily, the product of theta coordinates is invariant under any transformation that acts on the generator λ_t of $\overline{\mathbf{F}}_q[\lambda_t]$ by an ℓth root of unity. It proves that given $\gamma_t = \lambda_t^{\ell}$ we can extract any ℓth root λ_t and the choice does not change the theta null point computed via equation (4.18). □

Now, we focus on finding γ_t and an easy method is by extracting an ℓth root out of $\lambda_t^{\ell^2}$ that is computed as follows. We know that $\widetilde{0}_{\mathcal{L}} = \texttt{chain\_mult}(\ell, \widetilde{t_0}, \widetilde{0}_{\mathcal{L}})$ and so, $\lambda_t^{\ell^2}\widetilde{0}_{\mathcal{L}} = \texttt{chain\_mult}(\ell, \widetilde{t}, \widetilde{0}_{\mathcal{L}})$. The final equality gives the factor $\lambda_t^{\ell^2}$. The problem with this approach is the introduction of another choice of ℓth root of unity ξ when computing γ_t. It induces a new transformation that is not among the transformations in the above lemma and it does not preserve the product of theta constants as a symbolical polynomial in γ_t. We are not guaranteed that a particular choice of root ξ such that $\gamma_t \to \xi\gamma_t$ gives the right theta null point.

To avoid the introduction of another ℓth root of unity, we use the criterion [66, Section 7.4] for choosing a particular affine lift $\widetilde{t}_e = \lambda_t \widetilde{t}_0$ of t such that the value $\gamma_t = \lambda_t^\ell$ is computed precisely. First we give the definition of this choice of affine lift and afterwards, we prove that we can indeed compute γ_t.

The prime ℓ is assumed odd in Theorem 4.1.1. Let $\ell' = (\ell - 1)/2$.

Definition 4.6.4. An excellent affine lift $\widetilde{t}_e$ is an affine lift of $t \in G$ such that the affine lifts of $(\ell' + 1)t$ and $\ell' t$, namely $\widetilde{(\ell' + 1)t_e} = \texttt{chain\_mult}(\ell' + 1, \widetilde{t}_e, \widetilde{0})$ and $\widetilde{-\ell' t_e} = \texttt{chain\_mult}(-\ell', \widetilde{t}_e, \widetilde{0})$, satisfy

$$\texttt{chain\_mult}(\ell' + 1, \widetilde{t}_e, \widetilde{0}) = \texttt{chain\_mult}(-\ell', \widetilde{t}_e, \widetilde{0}) \tag{4.21}$$

or equivalently,

$$\theta_i^{\Theta_{\mathcal{L}}}(\widetilde{(\ell' + 1)t_e}) = \theta_{-i}^{\Theta_{\mathcal{L}}}(\widetilde{\ell' t_e}) \text{ for all } i \in K_1(\mathcal{L}). \tag{4.22}$$

The next lemma is particularly useful in computing equation (4.18). We assume that we are given an arbitrary affine lift $\widetilde{t} = \lambda_t \widetilde{t}_e$ and we are interested in computing the ℓth power of λ_t.

Lemma 4.6.5. *If $\lambda_t \widetilde{t}_e$ is an affine lift of $t \in G$, then we can explicitly compute λ_t^ℓ.*

Proof. In the case of an arbitrary lift of the form $\lambda_t \widetilde{t}_e$, we have the equalities

$$\texttt{chain\_mult}(\ell' + 1, \lambda_t \widetilde{t}_e, \widetilde{0}_{\mathcal{L}}) = \lambda_t^{(\ell'+1)^2} \texttt{chain\_mult}(\ell' + 1, \widetilde{t}_e, \widetilde{0}_{\mathcal{L}})$$

and

$$\texttt{chain\_mult}(-\ell', \lambda_t \widetilde{t}_e, \widetilde{0}_{\mathcal{L}}) = \lambda_t^{\ell'^2} \texttt{chain\_mult}(-\ell', \widetilde{t}_e, \widetilde{0}_{\mathcal{L}})$$
$$= \lambda_t^{\ell'^2} \texttt{chain\_mult}(\ell' + 1, \widetilde{t}_e, \widetilde{0}_{\mathcal{L}}) = \lambda_t^{-\ell} \texttt{chain\_mult}(\ell' + 1, \lambda_t \widetilde{t}_e, \widetilde{0}_{\mathcal{L}})$$

Hence,

$$\lambda_t^\ell = \texttt{chain\_mult}(\ell' + 1, \lambda_t \widetilde{t}_e, \widetilde{0}_{\mathcal{L}}) / \texttt{chain\_mult}(\ell' + 1, \lambda_t \widetilde{t}_e, \widetilde{0}_{\mathcal{L}}) =: \gamma_t$$

Any other excellent affine lift is of the form $\xi \widetilde{t}_e$, where ξ is an ℓ-th root of unity (immediate from (3.29), with $\lambda_0 = 1$, and definition (4.21)).

□

Remark 15. Following [66, Prop.7.4.3], an excellent affine lift is compatible with a choice of level $2\ell^2$ theta constants on A, denoted by $\widetilde{0}_{[\ell]^*\mathcal{L}}$. The affine lift is uniquely determined up to multiplication by an ℓth root of unity. But $\beta \circ \beta^c = \ell$, where β^c is the endomorphism corresponding to the real quadratic conjugate of β. Consider two affine isogenies $\widetilde{\beta}$ and $\widetilde{\beta^c}$ and the theta null point $\widetilde{0}_{[\beta]^*\mathcal{L}} = \widetilde{\beta^c}(\widetilde{0}_{[\ell]^*\mathcal{L}})$. In addition, let $\widetilde{f} \circ \widetilde{\widehat{f}} = \widetilde{\beta}$. If we define the affine theta null points $\widetilde{0}_{\mathcal{M}^\beta} := \widetilde{f}(\widetilde{0}_{[\beta]^*\mathcal{L}})$ and $\widetilde{0}_{\mathcal{L}} := \widetilde{\widehat{f}}(\widetilde{0}_{\mathcal{M}^\beta}) = \widetilde{\beta}(\widetilde{0}_{[\beta]^*\mathcal{L}})$, then both theta null points are compatible with $\widetilde{0}_{[\ell]^*\mathcal{L}}$. We conclude that an excellent affine lift $\widetilde{t}_e \in G$

is also compatible with the choice of $\widetilde{\widehat{f}}$ and $\widetilde{0}_{\mathcal{M}^\beta}$, in the sense that it is equal to $\widetilde{t}_0$ up to multiplication by an ℓth root of unity.

Remark 16. Notice that it is possible to compute the theta coordinates of an excellent affine lift $\widetilde{t}_e$ above $t \in G$ given an arbitrary affine lift $\widetilde{t}$ and a fixed affine theta null point $\widetilde{0}_{\mathcal{L}}$. Here, both points are given in theta coordinates determined by the theta structure $\Theta_{\mathcal{L}}$ of level 2. We just need to compute $\widetilde{(\ell'+1)t}$ and $-\widetilde{\ell' t}$ via two chain multiplication (denoted by `chain_mult`) or via ℓ' chain additions to obtain $\widetilde{2t}, \widetilde{3t}, \dots, \widetilde{(\ell'+1)t}$. Then, as in Lemma 4.6.5, let $\gamma_t = \theta_i^{\Theta_{\mathcal{L}}}(\widetilde{(\ell'+1)t_e})^{-1} \cdot (\theta_{-i}^{\Theta_{\mathcal{L}}}(\widetilde{\ell' t_e}))$ for any $i \in K_1(\mathcal{L})$ such that $\theta_i^{\Theta_{\mathcal{L}}}(\widetilde{(\ell'+1)t_e}) \neq 0$.

Notice that $\gamma_t = \lambda_t^{-\ell}$ to reduce the number of inversions. We extract an arbitrary ℓth root λ_t of γ_t, and multiply $\widetilde{t}$ by it. In this manner we obtain an excellent affine lift $\widetilde{t}_e$ of t. If we use chain additions, given λ_t, we can deduce the affine lifts of $\widetilde{2t_e}, \widetilde{3t_e}, \dots, \widetilde{(\ell'+1)t_e}$ out of $\widetilde{2t}, \widetilde{3t}, \dots, \widetilde{(\ell'+1)t}$ just by multiplying via the corresponding factor from equation (3.29), namely, $\lambda_t^4, \lambda_t^9, \dots, \lambda_t^{(\ell'+1)^2}$. The affine lifts of the remaining elements of G are computed using equation (4.22), but with $m = 1, \dots, \ell' - 1$ instead of ℓ',

$$\theta_i^{\Theta_{\mathcal{L}}}(\widetilde{(\ell-m)t_e}) = \theta_{-i}^{\Theta_{\mathcal{L}}}(\widetilde{\ell' t_e}).$$

With this method, we determine excellent affine lifts of all elements in G as according to [66, Cor. 7.4.5] and these lifts can be used in computing the sum in (4.18).

Next step is to compute the theta coordinates of $(y, 0, 0, 0) \in B^4$. Again, the case $r = 2$ follows immediately from the case $r = 4$.

4.6.4 Evaluating the Isogeny on Points

The main goal of this section is to express affine theta coordinates of $y = f(x) \in B(\mathbf{F}_q)$ for the theta structure $\Theta_{\mathcal{M}}$ in terms of the affine theta coordinates of the rational point x for the theta structure $\Theta_{\mathcal{L}}$.

First, consider the rational subgroup $\langle x \rangle \subseteq A(\mathbf{F}_q)$ generated by x of order Q. The endomorphism β of A of degree ℓ^2, with ℓ prime to Q (see input 4.1.1, is restricted to an automorphism $\beta|_{\langle x \rangle}$ on $\langle x \rangle$. Consider the following subgroup of $A^r(\mathbf{F}_q)$:

$$X = \{(a_1 x, \dots, a_r x) \,|\, a_1, \dots, a_r \in \mathbf{Z}/Q\mathbf{Z}\}.$$

As $\beta = F \circ F^t$ is an automorphism of X, then both F and F^t are automorphisms of X. We prove the following result.

Lemma 4.6.6. *Let* $(x_1, \dots, x_r) = F^t(x, 0 \dots, 0) \in X$ *and let*

$$(x_1', \dots, x_r') = F^{-1}(x, 0, \dots, 0) \in X.$$

If $y_i = f(x_i') \in B$ *then,* $F(y_1, \dots, y_r) = (f(x), 0, \dots, 0)$ *and* $(x_1, \dots, x_r) = \widehat{f}^{\star r}(y_1, \dots, y_r)$.

Proof. Let $(y'_1, \dots, y'_r) = F^t(y, 0, \dots, 0)$. Then it follows:

$$\begin{tikzcd}
(x'_1,\dots,x'_r) & \in & A^r \arrow[r, "f^{\star r}"] \arrow[d, "F"] & B^r \arrow[d, "F"] & \ni & (y_1,\dots,y_r) \\
(x,0,\dots,0) & \in & A^r \arrow[r, "f^{\star r}"] \arrow[d, "F^t"] & B^r \arrow[d, "F^t"] & \ni & (y,0,\dots,0) \\
(x_1,\dots,x_r) & \in & A^r \arrow[r, "f^{\star r}"] & B^r & \ni & (y'_1,\dots,y'_r).
\end{tikzcd}$$

and consequently $F(y_1, \dots, y_r) = (y, 0 \dots, 0)$ and $(x_1, \dots, x_r) = \beta(x'_1, \dots, x'_r) = \widehat{f}^{\star r}(f^{\star r}(x'_1, \dots, x'_r)) = \widehat{f}^{\star r}(y_1, \dots, y_r)$. Moreover, $y'_s = \beta y_s$ and $x'_s = \beta^{-1} x_s \in X$, for all $s \in \{1, \dots, r\}$.

□

Consider a rational point $x \in A(\mathbf{F}_q)$ given in Mumford coordinates. We convert it to theta coordinates for the theta structure $\Theta_{\mathcal{L}}$ and consider an arbitrary affine lift $\widetilde{x} \in \mathbf{A}(\Gamma(A, \mathcal{L}))$. Similarly to the theta constants $\widetilde{0}_{\mathcal{L}}$, the theta coordinates of $\widetilde{x}$ are over an extension field of $\mathbf{F}_q$.

Consider the isogeny of polarized abelian varieties with theta structures $\widehat{f} \colon (B, \mathcal{M}^{\beta}, \Theta_{\mathcal{M}^{\beta}}) \to (A, \mathcal{L}, \Theta_{\mathcal{L}})$. Let $(y_1, \dots, y_r) \in B^r(\mathbf{F}_q)$, where $F(y_1, \dots, y_r) = (f(x), 0, \dots, 0)$ and let $t'_1, \dots, t'_r \in K_1(\mathcal{M}^{\beta})[\beta]$. Following equation (4.10), given an affine lift $\widetilde{y_s + t'_s}$ of $y_s + t'_s$, where $s \in \{1, \dots, r\}$, we consider the affine lift $\widetilde{\widehat{f}(y_s) + \widehat{f}(t'_s)}$ of $\widehat{f}(y_s) + \widehat{f}(t'_s)$, of the form

$$\theta_i^{\Theta_{\mathcal{L}}}(\widetilde{\widehat{f}(y_s) + \widehat{f}(t'_s)}) = \theta_j^{\mathcal{M}^{\beta}}(\widetilde{y_s + t'_s}), \tag{4.23}$$

for any $i \in K_1(\mathcal{L})$ and $j \in K_1(\mathcal{M}^{\beta})[2]$ is the unique point for which $\widehat{f}(j) = i$.

According to Lemma 4.6.6, for all $s = 1, \dots, r$, we have $\widehat{f}(y_s) = x_s$ where $(x_1, \dots, x_r) = F^t(x)$. Since endomorphism F^t has a matrix representation with $\alpha_1, \dots, \alpha_r$ on the first column we write $x_s = \alpha_s x$ for all $s = 1, \dots, r$. At the end of Section 4.6.2, we proved that $\widehat{f}(t'_s)$ is an element of the kernel $G = \mathrm{Ker} f$, that we denoted by t_s. For any $s = 1, \dots, r$ and $t_s = \widehat{f}(t'_s) \in G$, with $t'_s \in K_1(\mathcal{M}^{\beta})[\beta]$, we denote by $\widetilde{\alpha_s x + t_s}$ the affine lift of $\alpha_s x + t_s = \widehat{f}(y_s) + \widehat{f}(t'_s)$ of the form

$$\theta_i^{\Theta_{\mathcal{L}}}(\widetilde{\alpha_s x + t_s}) := \theta_i^{\Theta_{\mathcal{L}}}(\widetilde{\widehat{f}(y_s) + \widehat{f}(t'_s)}), \tag{4.24}$$

for all $i \in K_1(\mathcal{L})$.

Next, we need to fix a particular affine lift of $\widetilde{y_s + t'_s}$ to suit our purposes. Namely, given an affine lift of $\widetilde{y}_s$, we consider the affine lift $\widetilde{y_s + t'_s}$ of the form

$$\Theta_{j_s}^{\Theta_{\mathcal{M}^{\beta}}}(\widetilde{y_s + t'_s}) := \Theta_{j_s + t'_s}^{\Theta_{\mathcal{M}^{\beta}}}(\widetilde{y}_s). \tag{4.25}$$

for all $j_s \in K_1(\mathcal{M}^{\beta})[2]$ and all $t'_s \in K_1(\mathcal{M}^{\beta})[\beta]$.

In the end, we consider the isogeny of polarized abelian varieties

$$F\colon (B^r, (\mathcal{M}^\beta)^{\star r}, \Theta_{(\mathcal{M}^\beta)^{\star r}}) \to (B^r, \mathcal{M}^r, \widetilde{\Theta}_{\mathcal{M}^{\star r}}).$$

We consider equation (4.11), with $\widetilde{y}^{\star r} = (\widetilde{y_1}, \dots, \widetilde{y_r})$ for the theta structure $\Theta_{(\mathcal{M}^\beta)^{\star r}}$. For any index $\mathbf{k} \in K_1(\mathcal{M}^{\star r})$ we have:

$$\begin{aligned}
\theta_{\mathbf{k}}^{\widetilde{\Theta}_{\mathcal{M}^{\star r}}}(\widetilde{f(x)}, \widetilde{0}, \dots, \widetilde{0}) &= \sum_{\substack{\mathbf{t}' \in K_1((\mathcal{M}^\beta)^{\star r})[\beta] \\ F(\mathbf{t}')=0}} \theta_{\mathbf{j}+\mathbf{t}'}^{\Theta_{(\mathcal{M}^\beta)^{\star r}}}(\widetilde{y_1}, \dots, \widetilde{y_r}) \\
&\overset{(4.25)}{=} \sum_{\substack{t'_1, \dots, t'_r \in K_1(\mathcal{M}^\beta)[\beta] \\ F(t'_1, \dots, t'_r)=0}} \prod_{s=1}^{r} \theta_{j_s}^{\Theta_{\mathcal{M}^\beta}}(\widetilde{y_s + t'_s}) \\
&\overset{(4.23),(4.24)}{=} \sum_{\substack{t_1, \dots, t_r \in G \\ \widehat{f}(t'_1)=t_1, \dots, \widehat{f}(t'_r)=t_r \\ t'_1, \dots, t'_r \in K_1(\mathcal{M}^\beta)[\beta] \\ F(t'_1, \dots, t'_r)=0}} \prod_{s=1}^{r} \theta_{i_s}^{\Theta_{\mathcal{L}}}(\widetilde{\alpha_s x + t_s}).
\end{aligned} \tag{4.26}$$

where $i_s = \widehat{f}(j_s) \in K_1(\mathcal{L})$, with $\mathbf{j} = (j_1, \dots, j_r) \in K_1((\mathcal{M}^\beta)^{\star r})[2]$ is unique such that $F(\mathbf{j}) = \mathbf{k}$.

Next, similarly to the previous section we present the more complicated case of $r = 4$. First, recall that for any $t'_1, \dots, t'_4 \in K_1(\mathcal{M}^\beta)[\beta]$, with $F(t'_1, \dots, t'_4) = 0$, we have the equality $(\widehat{f}(t'_1), \dots, \widehat{f}(t'_4)) = F^t(t_1, t_2, 0, 0)$ for some $t_1, t_2 \in G$. As in Remark 14, given a generator t of G, we write elements $t_1, t_2 \in G$ as $t_1 = a_1 t$ and $t_2 = a_2 t$ for some unique $a_1, a_2 \in \mathbf{Z}/\ell\mathbf{Z}$. Following Remark 13, each component of the matrix F^t (when acting on G^r) is equal to $\pm b_s \in \mathbf{Z}/\ell\mathbf{Z}$ where multiplication by b_s represents the action of α_s on G. Furthermore, we group the scalars in $\mathbf{Z}/\ell\mathbf{Z}$ as in Remark 14, namely we write $(w_1 t, \dots, w_4 t) := F^t(a_1 t, a_2 t, 0, 0)$ where

$$\begin{aligned}
w_1(a_1, a_2) &:= b_1 a_1 - b_2 a_2, & w_2(a_1, a_2) &:= b_2 a_1 + b_1 a_2, \\
w_3(a_1, a_2) &:= b_3 a_1 - b_4 a_2, & w_4(a_1, a_2) &:= b_4 a_1 + b_3 a_2.
\end{aligned} \tag{4.27}$$

Then, in equation (4.24) we have $\alpha_s x + t_s = \alpha_s x + w_s(a_1, a_2)t$, for some $a_1, a_2 \in \mathbf{Z}/\ell\mathbf{Z}$ such that $F^t(a_1 t, a_2 t, 0, 0) = (t_1, \dots, t_4)$. From now on, we use a new notation for the affine lift of $\alpha_s x + t_s$ given by equation (4.24), i.e., $\alpha_s x + \widetilde{w_s(a_1}, a_2)t$.

The new notation has the advantage that, similarly to the case of (4.18), we sum over $a_1, a_2 \in \mathbf{Z}/\ell\mathbf{Z}$ (or equivalently over $t_1, t_2 \in G$) when evaluating the RHS of (4.26). More precisely, for all $\mathbf{k} \in K_1(\mathcal{M}^{\star r})$ we have

$$\theta_{\mathbf{k}}^{\widetilde{\Theta}_{\mathcal{M}^{\star 4}}}(\widetilde{f(x)}, \widetilde{0}, \dots, \widetilde{0}) = \sum_{a_1, a_2 \in \mathbf{Z}/\ell\mathbf{Z}} \prod_{s=1}^{4} \theta_{i_s}^{\Theta_{\mathcal{L}}}(\alpha_s x + \widetilde{w_s(a_1}, a_2)t) \tag{4.28}$$

where $i_s = \widehat{f}(j_s) \in K_1(\mathcal{L})$, with $\mathbf{j} = (j_1, \dots, j_4) \in K_1((\mathcal{M}^\beta)^{\star 4})[2]$ is unique such that $F(\mathbf{j}) = \mathbf{k}$.

Now, we want to evaluate the RHS of the above equation in practice. As in the previous section, we are given the affine theta null point $\widetilde{0}_{\mathcal{L}}$ of A and an affine lift $\widetilde{t}$ of the generator $t \in G$. In addition, we also consider an arbitrary affine lift $\widetilde{x} \in \widetilde{A}$ of the rational point $x \in A(\mathbf{F}_q)$ of order Q. Hence, we need to compute some affine lifts $\alpha_s x + \widetilde{w_s(a_1}, a_2)t$ for which equation (4.28) holds (up to multiplication by a known scalar in $\overline{\mathbf{F}}_q^*$).

Remark 17. First, following Section 4.5.3, we notice that the action of the endomorphism α_s on the point $x \in A(\mathbf{F}_q)$ of order Q is given by multiplication via a scalar $u_s + v_s c_Q \in \mathbf{Z}/Q\mathbf{Z}$, where $u_s = \alpha_s^1 \cdot d^{-1} \in \mathbf{Z}/Q\mathbf{Z}$, $v_s = \alpha_s^2 \cdot d^{-1} \in \mathbf{Z}/Q\mathbf{Z}$ and $c_Q = f_\omega(1) \in \mathbf{Z}/Q\mathbf{Z}$ is the action of $\sqrt{D}$ on x computed by using the Frobenius polynomial χ_π. In order to evaluate the RHS of (4.28), at first glance one would expect that it is sufficient to compute $\widetilde{\alpha_s x + w_s(a_1, a_2)t}$ via the method `chain_multiadd`$(u_s + v_s c_Q, w_s(a_1, a_2), \widetilde{x}, \widetilde{x+t}, \widetilde{t}, \widetilde{0}_{\mathcal{L}})$, for some affine lift of $\widetilde{x+t}$ (the method `chain_multiadd` is from Section 3.2.6). But, following [13, §4.2] we notice that we need to be careful when fixing affine lifts of $x + t$ and $\alpha_s x + t$ (to be made precise later on in Lemma 4.6.12).

Since the difference with respect to [13] is the presence of real endomorphisms α_s, we give the following definition for a method of computing the image of an affine points $\widetilde{z} \in \widetilde{A}$ via the endomorphism $\sqrt{D}$.

Definition 4.6.7. Let `chain_mult_RM` be a method that given the real endomorphism $\sqrt{D}$ on A and an affine lift $\widetilde{z}$ of $z \in A$ and a theta null point $\widetilde{0}_{\mathcal{L}}$, outputs an affine lift $\widetilde{\sqrt{D}z}$ of $\sqrt{D}z$. We write:

$$\widetilde{\sqrt{D}z} \leftarrow \texttt{chain\_mult\_RM}(\sqrt{D}, \widetilde{z}, \widetilde{0}_{\mathcal{L}}). \tag{4.29}$$

Moreover, given a second affine lift $\lambda_z \widetilde{z}$ of z, the new affine lift of $\sqrt{D}z$ computed via the method `chain_mult_RM` satisfies

$$\texttt{chain\_mult\_RM}(\sqrt{D}, \lambda_z \widetilde{z}, \widetilde{0}_{\mathcal{L}}) = \lambda_z^D \texttt{chain\_mult\_RM}(\sqrt{D}, \lambda_z \widetilde{z}, \widetilde{0}_{\mathcal{L}}). \tag{4.30}$$

We look for another method of computing affine lifts $\widetilde{\alpha_s x + w_s(a_1, a_2)t}$ out of arbitrary lifts $\widetilde{x}, \widetilde{t}, \widetilde{0}_{\mathcal{L}}$ that is not `chain_multiadd`. For that, we consider the method `three_way_add` defined in (3.32), satisfying the equation (3.31). More precisely, for $s = 1, \ldots, 4$ we write $\alpha_s x + w_s(a_1, a_2)t = u_s + v_s\sqrt{D}x + w_s(a_1, a_2)t$, with u_s, v_s, $w_s(a_1, a_2)$ viewed as elements in $\mathbf{Z}$. We need to consider arbitrary affine lifts $\widetilde{u_s x}$, $\widetilde{v_s\sqrt{D}x}$, $\widetilde{w_s(a_1, a_2)t}$, $\widetilde{u_s x + v_s\sqrt{D}x}$, $\widetilde{u_s x + w_s(a_1, a_2)t}$, $\widetilde{v_s\sqrt{D}x + w_s(a_1, a_2)t}$.

Then, via the method `three_way_add` we obtain:

$$\begin{aligned} \widetilde{\alpha_s x + w_s(a_1, a_2)t} \quad \leftarrow \quad & \texttt{three\_way\_add}(\widetilde{u_s x}, \widetilde{v_s\sqrt{D}x}, \widetilde{u_s x + v_s\sqrt{D}x}, \widetilde{w_s(a_1, a_2)t}, \\ & \widetilde{u_s x + w_s(a_1, a_2)t}, \widetilde{v_s\sqrt{D}x + w_s(a_1, a_2)t}). \end{aligned} \tag{4.31}$$

In order to evaluate (4.31), we need to compute the above arbitrary lifts out of $\widetilde{x}, \widetilde{t}, \widetilde{0_{\mathcal{L}}}$. First, we recall that in order to compute an affine lift of $u_s x + w_s(a_1, a_2)t$ via a method from Section 3.2.6, we need to fix once and for all an arbitrary lift of $x + t$. Let $\widetilde{x+t}$ be an arbitrary affine lift of $x + t$. For instance it is computed by changing the Mumford coordinates of $x + t \in A$ to theta coordinates for the theta structure $\Theta_{\mathcal{L}}$. Similarly, in order to compute an affine lift of $v_s\sqrt{D}x + w_s(a_1, a_2)t$, let $\widetilde{\sqrt{D}x + t}$ be an arbitrary affine lift of $\sqrt{D}x + t$. After we present the steps of computing affine lifts of $u_s x + w_s(a_1, a_2)t$ via the `three_way_add` above, we will consider certain criteria for fixing affine lifts of $x + t$ and $\sqrt{D}x + t$.

For each $s = 1, \ldots, r$ we consider the elements u_s, v_s, $w_s(a_1, a_2) \in \mathbf{Z}$ from before and the above affine lifts $\widetilde{\sqrt{D}x + t}, \widetilde{x+t}, \widetilde{x}, \widetilde{t}, \widetilde{0_{\mathcal{L}}}$. We proceed as follows:

1. We use the method `chain_mult` from Section 3.2.6 to compute
$$\widetilde{u_s x} \leftarrow \texttt{chain\_mult}(u_s, \widetilde{x}, \widetilde{0}_{\mathcal{L}}).$$
Next, both real endomorphisms $v_s\sqrt{D}$ and $(u_s + v_s\sqrt{D})$ act on x. Consider the scalar $c_Q \in \mathbf{Z}$ representing the action of $\sqrt{D}$ on x from Section 4.5.3. Since D is identified with c_Q^2 modulo Q and $\texttt{chain\_mult}(c_Q, \lambda_x\widetilde{x}, \widetilde{0}_{\mathcal{L}}) = \lambda_x^{c_Q^2}\texttt{chain\_mult}(c_Q, \widetilde{x}, \widetilde{0}_{\mathcal{L}})$, for any $\lambda_x \in \overline{\mathbf{F}}_q^*$, the method $\texttt{chain\_mult}(c_Q, \widetilde{x}, \widetilde{0}_{\mathcal{L}})$ is considered as a `chain_mult_RM` method for computing an affine image of the affine point $\widetilde{x}$ via the real endomorphism $\sqrt{D}$. In the end, let:
$$\widetilde{v_s\sqrt{D}x} \leftarrow \texttt{chain\_mult}(v_s c_Q, \widetilde{x}, \widetilde{0}_{\mathcal{L}})$$
$$\widetilde{(u_s + v_s\sqrt{D})x} \leftarrow \texttt{chain\_mult}(u_s + v_s c_Q, \widetilde{x}, \widetilde{0}_{\mathcal{L}}).$$
2. Let the action of $\sqrt{D}$ on G be given by $c_t \in \mathbf{Z}/\ell\mathbf{Z}$ (see Section 4.5.3). Then, similarly to computing $\widetilde{\sqrt{D}x}$, we can define an image of $\widetilde{t}$ via the real endomorphism $\sqrt{D}$ as given by $\widetilde{c_t t} \leftarrow \texttt{chain\_mult}(c_t, \widetilde{t}, \widetilde{0}_{\mathcal{L}})$. Then given $w_s(a_1, a_2) \in \mathbf{Z}$ (written in terms of c_t), we compute
$$\widetilde{w_s(a_1, a_2)t} \leftarrow \texttt{chain\_mult}(w_s(a_1, a_2), \widetilde{t}, \widetilde{0}_{\mathcal{L}}).$$
3. We compute the affine lift of $u_s x + w_s(a_1, a_2)t$ out of the fixed affine lifts $\widetilde{x}$, $\widetilde{x+t}$, $\widetilde{t}$ and $\widetilde{0}_{\mathcal{L}}$ via the method `chain_multiadd` from Section 3.2.6, namely:
$$\widetilde{u_s x + w_s(a_1, a_2)t} \leftarrow \texttt{chain\_multiadd}(u_s, w_s(a_1, a_2), \widetilde{x}, \widetilde{x+t}, \widetilde{t}, \widetilde{0}_{\mathcal{L}}).$$
4. We compute an affine lift of $v_s\sqrt{D}x + w_s(a_1, a_2)t$ as:
$$\widetilde{v_s\sqrt{D}x + w_s(a_1, a_2)t} \leftarrow \texttt{chain\_multiadd}(v_s, w_s(a_1, a_2), \widetilde{c_Q x}, \widetilde{\sqrt{D}x + t}, \widetilde{t}, \widetilde{0}_{\mathcal{L}}),$$
where $\widetilde{c_Q x}$ is defined in Step 1.
5. We compute the affine lift of $u_s x + v_s\sqrt{D}x + w_s(a_1, a_2)t$ via the `three_way_add` method of (4.31).

Following [13, §4.2], to compute the RHS of (4.26), we give the same criterion for choosing an affine lift of $x + t$. From now on, all affine coordinates (unless specified) are computed with respect to the theta structure $\Theta_{\mathcal{L}}$.

Definition 4.6.8 (suitable lifts)**.** We call an affine lift $\widetilde{x+t}$ of $x + t$ *suitable for the tuple* $(\widetilde{0}_{\mathcal{L}}, \widetilde{x}, \widetilde{t})$ if it satisfies:
$$\texttt{chain\_multadd}(\ell, \widetilde{t}, \widetilde{x+t}, \widetilde{x}, \widetilde{0}_{\mathcal{L}}) = \widetilde{x}, \tag{4.32}$$
where `chain_multadd` denotes the multiplication chain algorithm from Section 3.2.6.

Next, we give a result that proves that even in practice, we can determine a suitable affine lift $\widetilde{x+t}$ from an arbitrary affine lift $\widetilde{x+t}'$. As before, the arbitrary affine lift can be determined out of the Mumford coordinates of $x + t$.

Lemma 4.6.9. *Given an affine lift $\widetilde{x}$ of $x \in A(\mathbf{F}_q)$, an affine lift $\widetilde{t} = \lambda_t\widetilde{t}_e$ of the generator $t \in G$, $\widetilde{t}_e$ is an excellent affine lift of t and $\lambda_t^\ell = \gamma_t$ is known and, and an affine lift $\widetilde{x+t}'$ we can compute a suitable affine lift of the form $\widetilde{x+t} = \lambda_{x+t}\widetilde{x+t}'$, with λ_{x+t}^ℓ known.*

Proof. To compute a suitable lift of $x+t$, we take the arbitrary affine lift $\widetilde{x+t}'$ for $x+t$ and look for a factor $\lambda_{x+t} \in \overline{\mathbf{F}}_q^{\times}$ such that the rescaled lift $\lambda_{x+t}\widetilde{x+t}'$ is suitable. Using (3.28), we obtain that:

$$\lambda_t^{\ell(\ell-1)}\texttt{chain\_multadd}(\ell, \widetilde{t}_e, \widetilde{x+t}, \widetilde{x}, \widetilde{0}_{\mathcal{L}}) = \lambda_{x+t}^{\ell}\texttt{chain\_multadd}(\ell, \widetilde{t}, \widetilde{x+t}', \widetilde{x}, \widetilde{0}_{\mathcal{L}})$$

and equation (4.32),

$$\lambda_{x+t}^{\ell} = \lambda_t^{\ell(\ell-1)}\widetilde{x}/\texttt{chain\_multadd}(\ell, \widetilde{t}, \widetilde{x+t}', \widetilde{x}, \widetilde{0}_{\mathcal{L}})$$

Notice that the affine lift $\widetilde{x+\ell t}' = \texttt{chain\_multadd}(\ell, \widetilde{t}, \widetilde{x+t}', \widetilde{x}, \widetilde{0}_{\mathcal{L}})$ is computed as in Section 3.2.6. This determines λ_{x+t} up to an ℓth root of unity, namely $\gamma_{x+t} := \lambda_{x+t}^{\ell}$ as equal to $\gamma_t^{\ell-1}\theta_i^{\Theta_{\mathcal{L}}}(\widetilde{x})/\theta_i^{\Theta_{\mathcal{L}}}(\widetilde{x+\ell t}')$, for any $i \in K_1(\mathcal{L})$ with $\theta_i^{\Theta_{\mathcal{L}}}(\widetilde{x+\ell t}') \neq 0$. □

Next we define a criterion for choosing an affine lift of $\sqrt{D}x+t$.

Definition 4.6.10. Consider a deterministic `chain_mult_RM` method $\texttt{RM}_D$ of computing an affine lift of $\sqrt{D}x$ given the affine points $\widetilde{x}, \widetilde{0}_{\mathcal{L}} \in \widetilde{A}$. Consider an arbitrary affine lift $\widetilde{z}$ of $z = x + \sqrt{D}^{-1}t$. The affine lift

$$\widetilde{\sqrt{D}x+t} = \texttt{RM}_D(\sqrt{D}, \widetilde{z}, \widetilde{0}_{\mathcal{L}})$$

of $\sqrt{D}x+t$ is called *suitable for the method $\texttt{RM}_D$ and the affine lifts* $(\widetilde{0}_{\mathcal{L}}, \widetilde{z})$.

Furthermore, given another arbitrary affine lift $\lambda_z \cdot \widetilde{z}$ of $z = x + \sqrt{D}^{-1}t$, for some $\lambda_z \in \overline{\mathbf{F}}_q^{*}$, by definition of $\texttt{RM}_D$ the two affine lifts of $\sqrt{D}x+t$ satisfy:

$$\texttt{RM}_D(\sqrt{D}, \lambda_z\widetilde{z}, \widetilde{0}_{\mathcal{L}}) = \lambda_z^{D} \cdot \texttt{RM}_D(\sqrt{D}, \widetilde{z}, \widetilde{0}_{\mathcal{L}}). \tag{4.33}$$

Remark 18. Let $c_Q \in \mathbf{Z}$ and $c_t \in \mathbf{Z}$ represent the action of $\sqrt{D}$ on x and t as in Section 4.5.3. We notice that if we consider the affine lift $\widetilde{c'_t t} \leftarrow \texttt{chain\_mult}(c'_t, \widetilde{t}, \widetilde{0}_{\mathcal{L}})$, for the least positive integer $c'_t \equiv c_t^{-1} \pmod{\ell}$, and consider the affine lift $\widetilde{z} \leftarrow \texttt{chain\_multadd}(c'_t, \widetilde{t}, \widetilde{x+t}, \widetilde{x}, \widetilde{0}_{\mathcal{L}})$, then an affine lift of $\sqrt{D}x+t$ is given by the method $\texttt{chain\_multadd}(c_Q, \widetilde{x}, \widetilde{z}, \widetilde{c'_t t}, \widetilde{0}_{\mathcal{L}})$. On the other hand, given an arbitrary $\lambda_z \in \overline{\mathbf{F}}_q^{*}$, we have:

$$\lambda_z^{c_Q} \cdot \texttt{chain\_multadd}(c_Q, \widetilde{x}, \widetilde{z}, \widetilde{c'_t t}, \widetilde{0}_{\mathcal{L}}) = \texttt{chain\_multadd}(c_Q, \widetilde{x}, \lambda_z\widetilde{z}, \widetilde{c'_t t}, \widetilde{0}_{\mathcal{L}}).$$

Then, `chain_multadd` is a `chain_mult_RM` method if the action of $\sqrt{D}$ on x is given by multiplication via D on x (namely the case of $D \equiv 0, 1 \pmod{Q}$).

Next lemma proves that there exists a deterministic method $\texttt{RM}_D$ for any $D \geq 2$, with D square free. It follows from the observation that if $G_D \subset A[D]$ is the kernel of the endomorphism corresponding to $\sqrt{D} \in \mathcal{O}_0$, then G_D is of size D^2 and is maximal isotropic for the Weil pairing $e_D \colon T_D A \times T_D A \to \mu_D$. Hence, $\sqrt{D}$ on A is a (D, D)-isogeny. Then,

Lemma 4.6.11. *Consider $(A, \mathcal{L}, \Theta_{\mathcal{L}})$, where $\mathcal{L}$ is totally symmetric and $\Theta_{\mathcal{L}}$ is symmetric. Consider the isogeny $\sqrt{D} \colon (A, \sqrt{D}^{*}\mathcal{L}, \Theta_{\sqrt{D}^{*}\mathcal{L}}) \to (A, \mathcal{L}, \Theta_{\mathcal{L}})$ of polarized abelian varieties with symmetric theta structures, whose kernel G_D is maximal isotropic for the Weil pairing e_D.*

Consider an affine lift $\widetilde{0}_{\sqrt{D}^{*}\mathcal{L}}$ for the theta structure $\Theta_{\sqrt{D}^{*}\mathcal{L}}$. Let $\theta_i^{\Theta_{\sqrt{D}^{*}\mathcal{L}}} \colon \widetilde{A} \to \overline{\mathbf{F}}_q$ and let $\theta_i^{\Theta_{\mathcal{L}}} \colon \widetilde{A} \to \overline{\mathbf{F}}_q$ be the two canonical system of coordinates and consider the canonical $\widetilde{\sqrt{D}}$ corresponding to the isogeny

$\sqrt{D}$ *and the affine system of coordinates. Let* $\widetilde{0}_{\mathcal{L}}$ *be the affine theta null point of* $(A, \mathcal{L}, \Theta_{Ł})$ *given by the choice of* $\widetilde{0}_{\sqrt{D}^*\mathcal{L}}$ *and the isogeny* $\sqrt{D}$*.*

Let $\widetilde{x}$ *be an affine lift of* $x \in A$ *for the theta structure* $\Theta_{\mathcal{L}}$ *and for* $u \in G_D$*, let* $\widetilde{u}$ *be the compatible affine lift of* u *for the theta structure* $\Theta_{\mathcal{L}}$ *with respect to* $\widetilde{0}_{\sqrt{D}^*\mathcal{L}}$ *and the isogeny* $\widetilde{\sqrt{D}}$*. Given* $(\widetilde{u}, \widetilde{x}, \widetilde{0}_{\mathcal{L}})$*, let* $\widetilde{x+u}$ *be a suitable affine lift*[5] *of* $x+u$ *for the theta structure* $\Theta_{\mathcal{L}}$*. Let* $\widetilde{\sqrt{D}x}$ *be the affine lift of* $\sqrt{D}x$ *satisfying* (3.21)*.*

If we rescale the affine lift $\widetilde{x}$ *by a factor* $\lambda_x \in \overline{\mathbf{F}}_q^*$*, then the output* $\widetilde{\sqrt{D}x}$ *is rescaled by* λ_x^D*. Hence, the affine* (D, D)*-isogeny* $\widetilde{\sqrt{D}}$ *is a deterministic* `chain_mult_RM` *method.*

Proof. For any $u \in G_D$, we want a suitable affine lift $\lambda_{x+u}\widetilde{x+u}$ of $x+u$, i.e., the affine lift satisfies $\texttt{chain\_multadd}(D, \widetilde{u}, \lambda_{x+u}\widetilde{x+u}, \lambda_x\widetilde{x}, \widetilde{0}_{\mathcal{L}}) = \lambda_x\widetilde{x}$. We know $\lambda_x\widetilde{x} = \lambda_x\texttt{chain\_multadd}(D, \widetilde{u}, \widetilde{x+u}, \widetilde{x}, \widetilde{0}_{\mathcal{L}})$ by definition of $\widetilde{x+u}$. Following (3.28), we have that the factors satisfy $\lambda_x^D = \lambda_{x+u}^D$, and so $\lambda_{x+u} = \xi\lambda_x$ for some Dth root of unity ξ_D.

Following [13, §4.2], computing the image of the affine points $\widetilde{x}$ and $\lambda_x\widetilde{x}$ via the (D, D)-isogeny $\widetilde{\sqrt{D}}$ is done by evaluating the RHS of the equation in [13, Prop 4.1]. Following [13, Lem. 4.4], the product of affine theta coordinates that needs to be calculated in order to obtain $\widetilde{\sqrt{D}(\lambda_x\widetilde{x})}$ is equal to a polynomial in $\overline{\mathbf{F}}_q[\lambda_x^D]$ times the product of affine theta coordinates that needs to be calculated in order to obtain $\widetilde{\widetilde{x}})$. To be more precise, we are given compatible affine lifts of $u \in G_D$ and suitable affine lifts of $x+u$ and so, the other factors in the statement of the cited lemma are equal to 1. □

Next lemma proves we can compute the RHS of (4.26).

Lemma 4.6.12. *Consider affine lifts* $\widetilde{t} = \lambda_t\widetilde{t}_e$*,* $\widetilde{x}$ *and* $\widetilde{x+t}' = \lambda_{x+t}\widetilde{x+t}$*, where* $\widetilde{t}_e$ *is an excellent affine lift of generator* $t \in G$*,* $\widetilde{x+t}$ *is suitable, and* $\lambda_t^\ell = \gamma_t, \lambda_{x+t}^\ell = \gamma_{x+t}$ *are known. Then the term*

$$\theta_{i_1}^{\Theta_{\mathcal{L}}}\left(u_1x + v_1\widetilde{\sqrt{D}x} + w_1(a_1, a_2)t\right)\dots\theta_{i_4}^{\Theta_{\mathcal{L}}}\left(u_4x + v_4\widetilde{\sqrt{D}x} + w_4(a_1, a_2)t\right) \tag{4.34}$$

viewed as a polynomial in the unknown λ_t, λ_{x+t}*, belongs to* $\overline{\mathbf{F}}_q[\lambda_t^\ell, \lambda_{x+t}^\ell]$*.*

Proof. Now, we will compute affine lifts of the points $u_sx + v_s\sqrt{D}x + w_s(a_1, a_2)t$, where $u_s, v_s, w_s(a_1, a_2) \in \mathbf{Z}$, via the three-way addition equation 4.31. As seen before in Steps 1–4, to do that, we compute affine lifts for the pairwise sums $u_sx + v_s\sqrt{D}x$, $u_sx + w_s(a_1, a_2)t$ and $v_s\sqrt{D}x + w_s(a_1, a_2)t$ as well as for $u_sx, v_s\sqrt{D}x$ and $w_s(a_1, a_2)t$ for each $s = 1, \dots, 4$.

1. In Step 1, we compute $\widetilde{u_sx}$, $\widetilde{v_s\sqrt{D}}$ and $(\widetilde{u_s + v_s\sqrt{D}})x$ via `chain_mult` of input $\widetilde{x}$, $\widetilde{0}_{\mathcal{L}}$ and all three affine points do not depend on λ_t and λ_{x+t}.

[5] The affine lifts $\widetilde{x+u}$ are suitable in the sense that they satisfy $\texttt{chain\_multadd}(D, \widetilde{u}, \widetilde{x+u}, \widetilde{x}, \widetilde{0}_{\mathcal{L}}) = \widetilde{x}$, for given $(\widetilde{u}, \widetilde{x}, \widetilde{0}_{\mathcal{L}})$.

2. In Step 2, we compute $\widetilde{w_s(a_1,a_2)t}$ via the method `chain_mult` of input $\widetilde{t}$, $\widetilde{0}_{\mathcal{L}} \in \widetilde{A}$. Via (3.29), the result differs from the affine point $\widetilde{w_s(a_1,a_2)t_e} :=$ `chain_mult`$(w_s(a_1,a_2), \widetilde{t}_e, \widetilde{0}_{\mathcal{L}})$ by the factor

$$\lambda_{w_s(a_1,a_2)t} = \lambda_t^{w_s(a_1,a_2)^2}. \tag{4.35}$$

3. In Step 3, we compute $\widetilde{u_s x + w_s(a_1,a_2)t}$ out of the fixed affine lifts $\widetilde{x}$, $\widetilde{x+t}'$ and $\widetilde{t}$ via `chain_multiadd`. Following (3.30), the affine lift differs from the affine point

$$\widetilde{u_s x + w_s(a_1,a_2)t_e} := \texttt{chain\_multiadd}(u_s, w_s(a_1,a_2), \widetilde{x}, \widetilde{x+t}, \widetilde{t}_e, \widetilde{0}_{\mathcal{L}})$$

by a factor:

$$\lambda_{u_s x + w_s(a_1,a_2)t} = \lambda_{x+t}^{u_s w_s(a_1,a_2)} \lambda_t^{w_s(a_1,a_2)(w_s(a_1,a_2)-u_s)}. \tag{4.36}$$

4. In Step 4, we compute an affine lift of $v_s\sqrt{D}x + w_s(a_1,a_2)t$ after we consider an affine lifts of $\sqrt{D}x+t$.

First, recall $\sqrt{D}^{-1}t = c'_t t$, where $c'_t \in \mathbf{Z}_{>0}$ such that $c'_t = c_t^{-1} \pmod{\ell}$, and consequently, $\sqrt{D}(x + c'_t t) = \sqrt{D}x + t$.

Let $z = x + \sqrt{D}^{-1}t$. We compute $\widetilde{z} =$ `chain_multadd`$(c'_t, \widetilde{t}, \widetilde{x+t}', \widetilde{x}, \widetilde{0}_{\mathcal{L}})$ that differs from $\widetilde{x + c'_t t_e} :=$ `chain_multadd`$(c'_t, \widetilde{t}_e, \widetilde{x+t}, \widetilde{x}, \widetilde{0}_{\mathcal{L}})$ via (3.28), by the factor

$$\lambda_z = \lambda_{x+t}^{c'_t} \lambda_t^{c'_t(c'_t-1)}.$$

The image of $\widetilde{z}$ under an $\texttt{RM}_D$ method is a suitable affine lift for the method and the affine lifts $(\widetilde{0}_{\mathcal{L}}, \widetilde{z})$. By Section 4.6.11, we can consider the (D,D)-isogeny $\sqrt{D}\colon A \to A$ as the $\texttt{RM}_D$ method of choice. The affine lift $\widetilde{\sqrt{D}x+t} = \texttt{RM}_D(\widetilde{z})$ differs from the affine lift $\widetilde{\sqrt{D}x+t_e} = \texttt{RM}_D(\widetilde{x + c'_t t_e})$ by:

$$\lambda_{\sqrt{D}x+t} = \lambda_z^D = \lambda_{x+t}^{Dc'_t} \lambda_t^{Dc'_t(c'_t-1)}.$$

In the end, we compute an affine lift of $\widetilde{v_s\sqrt{D}x + w_s(a_1,a_2)t}$ via `chain_multiadd` as in Step 4 and using (3.30), the affine lift differs from $\widetilde{v_s\sqrt{D}x + w_s(a_1,a_2)t_e}$ given by `chain_multiadd` of input v_s, $w_s(a_1,a_2)$, $\widetilde{\sqrt{D}x}$, $\widetilde{\sqrt{D}x + t_e}$, $\widetilde{t}_e$, $\widetilde{0}_{\mathcal{L}}$ by the factor

$$\begin{aligned} \lambda_{v_s\sqrt{D}x+w_s(a_1,a_2)t} &= \lambda_{\sqrt{D}x+t}^{v_s w_s(a_1,a_2)} \lambda_t^{w_s(a_1,a_2)(w_s(a_1,a_2)-v_s)} \\ &= \lambda_{x+t}^{Dc'_t v_s w_s(a_1,a_2)} \lambda_t^{Dc'_t(c'_t-1)v_s w_s(a_1,a_2)+w_s(a_1,a_2)(w_s(a_1,a_2)-v_s)}. \end{aligned} \tag{4.37}$$

5. In Step 4, we compute $\widetilde{u_s x + v_s\sqrt{D}x + w_s(a_1,a_2)t}$ via equation (4.31), that differs from the point given by `three_way_add` of input $\widetilde{u_s x}$, $\widetilde{v_s\sqrt{D}x}$, $\widetilde{w_s(a_1,a_2)t_e}$, $\widetilde{0_{\mathcal{L}}}$, $\widetilde{u_s x + v_s\sqrt{D}x}$, $\widetilde{u_s x + w_s(a_1,a_2)t_e}$, $\widetilde{v_s\sqrt{D}x + w_s(a_1,a_2)t_e}$ by the factor

$$\lambda_{u_s x + v_s\sqrt{D}x + w_s(a_1,a_2)t} = \frac{\lambda_{u_s x + w_s(a_1,a_2)t} \cdot \lambda_{v_s\sqrt{D}x + w_s(a_1,a_2)t}}{\lambda_{w_s(a_1,a_2)t}}. \tag{4.38}$$

Using equations (4.36)–(4.35), we compute the exponents of λ_{x+t} and λ_t in (4.38) and obtain that

$$\begin{aligned}\textstyle\prod_{s=1}^4 \lambda_{u_s x+v_s\sqrt{D}x+w_s(a_1,a_2)t} = \ & \lambda_{x+t}^{\sum_{s=1}^4 \left(u_s w_s(a_1,a_2)+Dc'_t v_s w_s(a_1,a_2)\right)} \cdot \\ & \lambda_t^{\sum_{s=1}^4 \left(Dc'_t(c'_t-1)v_s w_s(a_1,a_2)+w_s(a_1,a_2)(w_s(a_1,a_2)-u_s-v_s)\right)}.\end{aligned} \tag{4.39}$$

Now, we reduce the exponents of λ_{x+t} and λ_t modulo ℓ and use the fact that $Dc'_t = \sqrt{D} \pmod{\ell}$. We notice that $u_s + v_s Dc'_t(\pmod{\ell}) = b_s$ and so, the exponent reduced modulo ℓ of λ_{x+t} becomes

$$\sum_s w_s(a_1,a_2)b_s = b_1(b_1a_1 - b_2a_2) + \ldots + b_4(b_3a_1 + b_4a_2) = a_1\sum_s b_s^2.$$

Also, the exponent of λ_t reduced modulo ℓ becomes

$$\sum_s (w_s(a_1,a_2)^2 - w_s(a_1,a_2)b_s) = (a_1+a_2)^2\sum_s b_s^2 - a_1\sum_s b_s^2,$$

where $\sum_s w_s(a_1,a_2)^2$ is easily computed as in (4.20).

In the end, equation (4.39) becomes:

$$\prod_{s=1}^4 \lambda_{u_s x+v_s\sqrt{D}x+w_s(a_1,a_2)t} = \lambda_{x+t}^{\ell M_1 a_1} \cdot \lambda_t^{\ell M_2((a_1+a_2)^2-a_1)},$$

for some integers M_1, M_2.

Hence, we proved that the product of $\widetilde{u_1x + v_1\sqrt{D}x + w_1(a_1,a_2)t}, \ldots, \widetilde{u_4x + v_4\sqrt{D}x + w_4(a_1,a_2)t}$ differs from the product in equation (4.26) (of suitable affine lifts) by a factor depending only on $\gamma_t = \lambda_t^\ell$ and $\gamma_{x+t} = \lambda_{x+t}^\ell$. Similarly to Lemma 4.6.5, taking arbitrary ℓth roots of γ_t and γ_{x+t} does not change the value of (4.34).

□

4.7 Modification of $\widetilde{\Theta}_{\mathcal{M}^{\star r}}$ on $(B^r, \mathcal{M}^{\star r})$ via a Metaplectic Isomorphism

The theta constants for the symmetric theta structure $\widetilde{\Theta}_{\mathcal{M}^{\star r}}$ on $\mathcal{M}^{\star r}$ from Section 4.6.2 do not automatically recover theta constants for $(B, \mathcal{M})$. It would do so if it were of the form $\Theta_{\mathcal{M}} \star \Theta_{\mathcal{M}^{\star(r-1)}}$ for theta structures $\Theta_{\mathcal{M}}$ and $\Theta_{\mathcal{M}^{\star(r-1)}}$ on $(B, \mathcal{M})$ and $(B^{r-1}, \mathcal{M}^{\star(r-1)})$, respectively.

In order to obtain information about a single polarized factor $(B, \mathcal{M})$, we need to modify $\widetilde{\Theta}_{\mathcal{M}^{\star r}}$ via a suitably chosen metaplectic automorphism (an automorphism of the corresponding Heisenberg group) so that it has the above form. The metaplectic automorphism comes from a symplectic automorphism acting on the 4-torsion points (via the argument in Lemma 3.2.5) whose action on the theta coordinates of level 2 for $\widetilde{\Theta}_{\mathcal{M}^{\star r}}$ is computed as in Section 3.2.3.1. We explain how to find a suitable automorphism of the 4 torsion points.

Lemma 4.7.1. *There exists a metaplectic automorphism $S \in \mathrm{Aut}(H(\delta^{\star r}))$ such that the theta structure*

$\widetilde{\Theta}_{\mathcal{M}^{\star r}} \circ S$ is a product theta structure

Proof. There exists a symmetric theta structure $\Theta_{\mathcal{M}}$ on $(B, \mathcal{M})$ which gives rise to an (r-fold) product theta structure $\Theta_{\mathcal{M}^{\star r}} = \Theta_{\mathcal{M}} \star \cdots \star \Theta_{\mathcal{M}}$ on $(B^r, \mathcal{M}^{\star r})$. Letting $S := \widetilde{\Theta}^{-1}_{\mathcal{M}^{\star r}} \circ \Theta_{\mathcal{M}^{\star r}}$, we see that $S \in \mathrm{Aut}(H(\delta^{\star r}))$ and that it satisfies the above property. □

Lemma 4.7.1 shows that we can always modify the resulting theta structure to a product theta structure. Yet, it does not tell us how to efficiently compute the metaplectic automorphism S since the above proof is non-constructive. In practice, we do not explicitly compute such an S, but instead, we only relate the theta constants of the new r-fold product theta structure $\Theta_{\mathcal{M}^{\star r}}$ to the theta constants of the old one $\widetilde{\Theta}_{\mathcal{M}^{\star r}}$.

Let $\overline{\Theta}\colon K((2\delta)^{\star r}) \to K((\mathcal{M}^2)^{\star r})$ be the symplectic automorphism (or basis) induced from the original choice of $\Theta_{\mathcal{L}^2}$ (recall that we have fixed a choice of 4th roots in the Thomae's formulas as explained in Section 4.2). By Section 3.2.3, to give the metaplectic automorphism S, it suffices to give a symplectic automorphism $\overline{S}\colon K((2\delta)^{\star r}) \to K((2\delta)^{\star r})$ (from Lemma 3.2.5) for which the symplectic basis determined by $\overline{\Theta} \circ \overline{S}\colon K((2\delta)^{\star r}) \to K((\mathcal{M}^2)^{\star r})$ is an r-fold product basis.

In order to apply Proposition 3.2.6, it seems that we require the theta coordinates of the points of $K((\mathcal{M}^2)^{\star r})$ of B^r (i.e., the points in $B^r[4]$). On the other hand, the isogeny $f^{\star r}\colon (A^r, (\mathcal{L}^{2\beta})^{\star r}) \to (B^r, (\mathcal{M}^2)^{\star r})$ (i.e., the isogeny obtained by using f on each factor) commutes with the action of $\overline{S}$ on the 4-torsion points of A^r and B^r as shown by the following diagram:

$$\begin{tikzcd}
\text{non } r\text{-fold, symplectic w.r.t. } e_{(\mathcal{L}^{2\beta})^{\star r}} \arrow[r, "f^{\star r}"'] \arrow[d, dashed, "\overline{S}"'] & \text{non } r\text{-fold, symplectic w.r.t. } e_{(\mathcal{M}^2)^{\star r}} \arrow[d, dashed, "\overline{S}"'] \\
r\text{-fold, symplectic w.r.t } e_{(\mathcal{L}^{2\beta})^{\star r}} \arrow[r, "f^{\star r}"'] & r\text{-fold, symplectic w.r.t. } e_{(\mathcal{M}^2)^{\star r}}
\end{tikzcd}$$

We are given a symplectic basis of $K(\mathcal{L}^2)$ on the original abelian surface A (i.e., $A[4]$) for which we can easily construct its corresponding r-fold basis. Moreover, we have defined two isogenies of p.a.v. $\widehat{f}^{\star r}\colon (B^r, (\mathcal{M}^{2\beta})^{\star r}) \to (A^r, (\mathcal{L}^2)^{\star r})$ and $F\colon (B^r, ((\mathcal{M}^2)^{\beta})^{\star r}) \to (B^r, (\mathcal{M}^2)^{\star r})$ that fix a basis of $K((\mathcal{L}^{2\beta})^{\star r}[4]$ as shown in the Lemma 4.7.2. Lemm 4.7.3 proves that in order to unfold the basis of $K((\mathcal{M}^2)^{\star r})$ it suffices to pick a symplectic automorphism $\overline{S} \in \mathbf{Sp}_{4r}(\mathbf{Z}/4\mathbf{Z})$ until one of them unfolds the basis of $K((\mathcal{L}^{2\beta})^{\star r})[4]$.

Lemma 4.7.2. *The symplectic basis of $K((\mathcal{L}^{2\beta})^{\star r})[4]$ (corresponding to the isogenies $f^{\star r}\colon (A^r, (\mathcal{L}^{2\beta})^{\star r}) \to (B^r, (\mathcal{M}^2)^{\star r})$ and $F\colon (B^r, (\mathcal{M}^{2\beta})^{\star r}) \to (B^r, (\mathcal{M}^2)^{\star r})$) is induced via the action of the matrix $F\beta^{-1}$ on the symplectic basis of $K((\mathcal{L}^2)^{\star r})$.*

Proof. First, we consider the r-fold product symplectic basis $\{e_i^{'}, e_i^{''}\}_{i=1}^{2r}$ for the 4-torsion points of $(A^r, (\mathcal{L}^2)^{\star r})$. Let $\{x_i', x_i''\}_{i=1}^{2r}$ be the r-fold product basis on $K((\mathcal{M}^{2\beta})^{\star r})[4]$ corresponding to the r-fold product theta structure $\Theta_{(\mathcal{M}^{2\beta})^{\star r}}$. We know that $\widehat{f}^{\star r}(x_i') = e_i'$ (and same for x_i''). Let $y_i' = F(x_i')$ and $y_i'' = F(x_i'')$.

The basis $\{y_i', y_i''\}_{i=1}^{2r}$ is then not an r-fold, but symplectic with respect to $e_{(\mathcal{M}^2)^{\star}}$. Define $f_i' = (f^{\star r})^{-1}(y_i')$ and $f_i'' = (f^{\star r})^{-1}(y_i'')$ where we note that $f^{\star r}|_{K((\mathcal{L}^{2\beta})^{\star r})[4]}$ is invertible and $(f^{\star r})^{-1}$ denotes the inverse of the restriction. Note that $\{f'_i, f''_i\}_{i=1}^{2r}$ is a non-r-fold and non-symplectic basis for $K((\mathcal{L}^2)^{\star r})$ with respect to $e_{(\mathcal{L}^2)^{\star}}$..

Indeed $F\beta^{-1}(e'_i) = f'_i$ and $F\beta^{-1}(e''_i) = f''_i$, following a simple diagram chasing argument:

$$\begin{tikzcd}
\{e'_i, e''_i\}_{i=1}^{2r} \in K(\mathcal{L}^2)^{\star r}) \arrow[d, dashed, "F\beta^{-1}"'] & \{x'_i, x''_i\}_{i=1}^{2r} \in K(\mathcal{M}^{2\beta})^{\star r})[2] \arrow[l, dashed, "\widehat{f^{\star r}}"'] \arrow[d, dashed, "F"'] \\
\{f'_i, f''_i\}_{i=1}^{2r} \in K((\mathcal{L}^{2\beta})^{\star r}) \arrow[r, dashed, "f^{\star r}"'] & \{y'_i, y''_i\}_{i=1}^{2r} \in K(\mathcal{M}^2)^{\star r})
\end{tikzcd}$$

□

Lemma 4.7.3. *Suppose that $\overline{S}$ is a symplectic automorphism of $K((\mathcal{L}^{2\beta})^{\star r})[4]$ for which $\{\overline{S}(f'_i), \overline{S}(f''_i)\}_{i=1}^{2r}$ (with f'_i, f''_i as above) is an r-fold product symplectic basis with respect to $e_{(\mathcal{L}^{2\beta})^{\star r}}$. Then the symplectic automorphism $\overline{S}$ unfolds the basis $\{y'_i, y''_i\}$ of $K((\mathcal{M}^2)^{\star r})$.*

Proof. Write

$$\overline{S}y'_i = \overline{S}f^{\star r}f'_i = f^{\star r}\overline{S}f'_i \qquad \text{and} \qquad \overline{S}y''_i = \overline{S}f^{\star r}f''_i = f^{\star r}\overline{S}f''_i.$$

Since $\overline{S}f'_i$ and $\overline{S}f''_i$ are both an r-fold product, so are $\overline{S}y'_i$ and $\overline{S}y''_i$. □

Next, we choose a symplectic automorphism $\overline{S}$ by looping over elements in $\mathbf{GL}_4(\mathbf{Z}/4\mathbf{Z})$ as follows. Let M be the matrix corresponding to the action of $F\beta^{-1}$ on the symplectic basis $\{e'_i, e''_i\}_{i=1}^{2r}$ of $A^r[4]$ (determined by the choice of theta structure $\Theta_{(\mathcal{L}^2)^{\star r}}$). Naturally, M is sent via $\overline{\Theta}_{(\mathcal{L}^2)^{\star r}}$ to an element of the general linear group of $\mathbf{GL}_{4r}(\mathbf{Z}/4\mathbf{Z})$. Let $\overline{S}$ denote the matrix representation of the automorphism $\overline{S}$ introduced above. Then there exists a unique matrix $S' \in \mathbf{Sp}_{4r}(\mathbf{Z}/4\mathbf{Z})$ such that $MS' = \overline{S}M$ that is acting on the basis of $K((2\delta_0)^r)$. According to the definition of an r-fold basis, $S' = M^{-1} \cdot \Delta(\mathbf{GL}_4(\mathbf{Z}/4\mathbf{Z}))$ where $\Delta\colon \mathbf{GL}_4(\mathbf{Z}/4\mathbf{Z}) \to \mathbf{GL}_{4r}(\mathbf{Z}/4\mathbf{Z})$ is the standard diagonal embedding. The computation is sufficiently simple by, e.g., going through all elements of $N \in \mathbf{GL}_4(\mathbf{Z}/4\mathbf{Z})$ and testing whether $M^{-1}\Delta(N)$ is symplectic. Once this condition is satisfied for a certain choice of $\Delta(N)$ and $S' = M^{-1}\Delta(N)$, the matrix representation of an unfolding symplectic automorphism $\overline{S}$ of $K((2\delta_0)^{\star r})$ is $\overline{S} = MS'M^{-1}$.

4.7.1 Applying the Transformation Formula

Consider an automorphism $\overline{S} \in \mathrm{Aut}(K((2\delta_0)^{\star r}))$ computed with the previous method. Recall that according to Section 3.2.3, there exists a unique metaplectic automorphism S of $H(\delta^{\star r})$ corresponding to $\overline{S}$ for which the theta structure $\Theta_{\mathcal{M}^{\star r}} := \widetilde{\Theta}_{\mathcal{M}^{\star r}} \circ S$ coming from $\overline{\Theta} \circ \overline{S}\colon K((2\delta_0)^{\star r}) \to K((\mathcal{M}^2)^{\star r})$ is indeed of the product form $\Theta_{\mathcal{M}} \star \Theta_{\mathcal{M}^{\star(r-1)}}$ for some theta structure $\Theta_{\mathcal{M}}$ on $(B, \mathcal{M})$ and a theta structure $\Theta_{\mathcal{M}^{\star(r-1)}}$ on $(B^{r-1}, \mathcal{M}^{\star(r-1)})$. Here, we chose the particular case of $\Theta_{\mathcal{M}^{\star(r-1)}}$ being the $(r-1)$-fold product of $\Theta_{\mathcal{M}}$.

We now apply the results of Section 3.2.3.1 to compute affine theta constants of the new theta structure $\Theta_{\mathcal{M}^{\star r}}$ out of affine theta constants for $\widetilde{\Theta}_{\mathcal{M}^{\star r}}$. First, we need to compute all affine theta coordinates $\theta_{\mathbf{i}}^{\widetilde{\Theta}_{\mathcal{M}^{\star r}}}(\cdot)$ with $\mathbf{i} \in K_1(\mathcal{M}^{\star r})$ via equation (4.18).

Given the canonical map $\frac{1}{2}\mathbf{Z}^2/\mathbf{Z}^2 \to \mathbf{Z}(2)$ sending $i \to 2i$, let $\kappa\colon \left(\frac{1}{2}\mathbf{Z}^2/\mathbf{Z}^2\right)^r \to K(\mathcal{M})^r$ be the bijective function corresponding to $\overline{\Theta}$ (and $\widetilde{\Theta}_{\mathcal{M}^{\star r}}$). Similarly, let $\kappa'\colon \left(\frac{1}{2}\mathbf{Z}^2/\mathbf{Z}^2\right)^r \to K_1(\mathcal{M})^r$ be the bijective function corresponding to $\overline{\Theta} \circ \overline{S}$ (and $\Theta_{\mathcal{M}^{\star r}}$). Let $\mathbf{Z}(2,2) = \frac{1}{2}\mathbf{Z}^2/\mathbf{Z}^2 \times \frac{1}{2}\mathbf{Z}^2/\mathbf{Z}^2$. Given a bijection map $\mathbf{Z}(2,2) \to \mathbf{Z}(4)$, a theta structure $\widetilde{\Theta}_{(\mathcal{M}^2)^{\star r}}$ of level 4 (compatible with $\widetilde{\Theta}_{\mathcal{M}^{\star r}}$) defines a bijective function $\mu\colon (\mathbf{Z}(2,2) \times \mathbf{Z}(2,2))^r \to K((\mathcal{M}^2)^{\star r})$. Furthermore, a new r-fold product theta structure of level 4 compatible with $\Theta_{\mathcal{M}^{\star r}}$ defines another bijective function of the form $\nu\colon (\mathbf{Z}(2,2) \times \mathbf{Z}(2,2))^r \to K((\mathcal{M}^2)^{\star r})$ (naturally $K((\mathcal{M}^2)^{\star r})$ has a new symplectic basis coming from the r-fold theta structure).

Let $R_{\overline{S}}$ be the automorphism making the following diagram commutative:

$$\begin{tikzcd}
(\mathbf{Z}(2,2) \times \mathbf{Z}(2,2))^r \arrow[r, "\mu"'] \arrow[d, "R_{\overline{S}}"'] & K((\mathcal{M}^2)^{\star r}) \arrow[d, "\overline{S}"] \\
(\mathbf{Z}(2,2) \times \mathbf{Z}(2,2))^r \arrow[r, "\nu"'] & K((\mathcal{M}^2)^{\star r}).
\end{tikzcd}$$

Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{Sp}_{4r}(\mathbf{Z})$ be the matrix representation of $R_{\overline{S}}$ on $\mathbf{Z}(2,2))^r$.

We first apply Proposition 3.2.6 for the case of $z = (0, \dots, 0)$ and then for the rational point $z = (y, 0, 0, 0)$. Let $\mathbf{e}' = \frac{1}{2}\operatorname{diag}(a^t c)$ and $\mathbf{e}'' = \frac{1}{2}\operatorname{diag}(d^t b)$. There exists a constant λ (containing the factor $\theta_{\mathbf{0}}^{\Theta_{\mathcal{M}^{\star r}}}(\widetilde{0})$) for which the new theta coordinates are

$$\theta_{\kappa'(\mathbf{v}')}^{\Theta_{\mathcal{M}^{\star r}}}(\widetilde{z}) = \frac{\lambda}{2^{2r}} \sum_{\mathbf{u}' \in (\frac{1}{2}\mathbf{Z}^2/\mathbf{Z}^2)^r} \xi_{\mathbf{u},\mathbf{v}}^2 \sum_{\mathbf{i} \in (\frac{1}{2}\mathbf{Z}^2/\mathbf{Z}^2)^r} e(-2\mathbf{u}^t\mathbf{i})\theta_{\kappa(\mathbf{b}+\mathbf{i})}^{\widetilde{\Theta}_{\mathcal{M}^{\star r}}}(\widetilde{z})\theta_{\kappa(\mathbf{i})}^{\widetilde{\Theta}_{\mathcal{M}^{\star r}}}(\widetilde{0}) \tag{4.40}$$

where $\mathbf{u}, \mathbf{v}, \mathbf{u}', \mathbf{v}' \in \frac{1}{2}(\mathbf{Z}^2/\mathbf{Z}^2)^r$ such that $\begin{pmatrix} \mathbf{u} \\ \mathbf{v} \end{pmatrix} = \begin{pmatrix} a & c \\ b & d \end{pmatrix}^{-1} \cdot \begin{pmatrix} \mathbf{u}' - \mathbf{e}' \\ \mathbf{v}' - \mathbf{e}'' \end{pmatrix}$, and

$$\xi_{\mathbf{u},\mathbf{v}} = e\left(-\frac{1}{2} \cdot (\mathbf{u}^t ab^t\mathbf{u} + \mathbf{v}^t cd^t\mathbf{v}) - (a^t\mathbf{u} + c^t\mathbf{v} + \mathbf{e}')^t\mathbf{e}'' - \mathbf{u}^t bc^t\mathbf{v}\right).$$

Suppose that we know the affine theta constants for the new (modified) theta structure $\Theta_{\mathcal{M}^{\star r}}$. Given an index $\mathbf{b}' := (b', 0, \dots, 0) \in (K_1(\mathcal{M}))^r$ with $b' \in K_1(\mathcal{M})$, then the affine theta constant at $\mathbf{b}'$ for the (symmetric) theta structure $\Theta_{\mathcal{M}^{\star r}}$ is equal to $\theta_{b'}^{\Theta_{\mathcal{M}}}(\widetilde{0}_{\mathcal{M}}) \cdot \left(\theta_{\mathbf{0}}^{\Theta_{\mathcal{M}}}(\widetilde{0}_{\mathcal{M}})\right)^{r-1}$. By varying over all $b' \in K_1(\mathcal{M})$ and by taking the factor $\left(\theta_{\mathbf{0}}^{\Theta_{\mathcal{M}}}(\widetilde{0}_{\mathcal{M}})\right)^{r-1} = 1$, we compute the affine theta constants $\widetilde{0}_{\mathcal{M}}$ for the principally polarized abelian surface $(B, \mathcal{M}, \Theta_{\mathcal{M}})$.

Next, we compute the affine theta coordinates of $z = (f(x), 0, 0, 0)$ for the theta structure $\widetilde{\Theta}_{(\mathcal{M})^{\star r}}$. We finish by applying the formula above and then, for each $b' \in K_1(\mathcal{M})$, compute $\theta_{b'}^{\Theta_{\mathcal{M}}}(\widetilde{f(x)})$ by taking the factor $\left(\theta_{\mathbf{0}}^{\Theta_{\mathcal{M}}}(\widetilde{0}_{\mathcal{M}})\right)^{r-1} = 1$ (common factor for all coordinates).

4.8 Algorithm

Remark 19. In this section, we use the classical notations, M for multiplications, S for squaring, I for inversion, and M_0 for multiplications by elements in the field of definition of the theta constants $\widetilde{0}_{\mathcal{L}}$ (depending on the theta constants of the Kummer surface). Furthermore, throughout this section, all operations that are not over (a finite field extension of) $\mathbf{F}_q$ are considered to be of constant time cost. If the number of operations in $\mathbf{F}_q$ (or in a finite field extension) is constant in ℓ and $\log q$, then we say that we have a constant number of operations in $\mathbf{F}_q$ (or in a finite field extension).

Computing chain additions or chain multiplications on the Kummer surface is quite expensive. According to [50, §5], we have the following complexity:

(i) computing $\widetilde{2x} = \texttt{chain\_mult}(2, \widetilde{x}, \widetilde{0}_{\mathcal{L}})$ requires $8S + 6M_0$ in the field of definition of x;

(ii) computing $\widetilde{x+y} = \texttt{chain\_add}(\widetilde{x}, \widetilde{y}, \widetilde{x-y}, \widetilde{0}_{\mathcal{L}})$ requires $4M + 8S + 3M_0 + 4I$ in the field of definition of x and y;

(iii) computing $\widetilde{x+y'}$ (after computing $\widetilde{x+y}$) requires $4M + 4S + 3M_0 + 4I$ in the field of definition of x and y.

We give the following theorem:

Theorem 4.8.1. *Consider the following* ***input data:***

I1. a finite field of definition $\mathbf{F}_q$, a prime degree ℓ;

I2. a smooth hyperelliptic curve C of genus 2 over $\mathbf{F}_q$, with $A = \mathrm{Jac}(C)$ and $\mathcal{L}_0$ its canonical principal polarization;

I3. a CM-type (K, Φ) of A, where $K = \mathbf{Q}(\pi)$ is a quartic CM field, containing a real quadratic field $K_0 \subset K$ of discriminant D;

I4. a generator t of the isogeny kernel $G \subset A[\ell]$ with $\pi(t) \in G$,[6] and $\beta(t) = 0$, given in Mumford coordinates defined over an extension field $\mathbf{F}/\mathbf{F}_q$;[7]

I5. a point $x \in A(\mathbf{F}_q)$ of order Q that is prime to q, ℓ, given in Mumford coordinates.

We assume the following conditions with respect to real multiplication on A

H1. $\mathrm{End}(A) \simeq \mathcal{O} \subset K$ of ***maximal real multiplication****, i.e., $\mathcal{O}_0 = \mathcal{O} \cap K_0$ is the ring of integers of K_0 ;*

H2. the ***index of*** *$[\mathcal{O} \colon \mathbf{Z}[\pi, \overline{\pi}]]$* ***is prime*** *to $2\ell Q$;*

H3. there ***exists a totally positive element*** *$\beta \in \mathcal{O}_0$ of* ***norm*** *ℓ such that $\beta(t) = 0$.*

Pre-compute data:

P1. *Compute an affine theta null point $\widetilde{0}_{\mathcal{L}}$ from the Rosenhain invariants λ, μ, ν of the curve C.[8] Compute an affine theta null point $\widetilde{0}_{\mathcal{L}^2}$ for a compatible theta structure of level $(2,2)$.*

P2. *Compute affine theta coordinates $\widetilde{t}$ of the generator $t \in G$ for the theta structure $\Theta_{\mathcal{L}}$ over some extension field $\mathbf{F}$ and compute an excellent affine lift $\widetilde{t}_e$ of t such that $\lambda_t \widetilde{t}_e = \widetilde{t}$, for $\lambda_t \in \overline{\mathbf{F}}_q^*$. Compute excellent affine lifts t_e for all $t \in G$.*

P3. *Compute affine theta coordinates $\widetilde{x}$ and $\widetilde{x+t}'$ for the theta structure $\Theta_{\mathcal{L}}$ (by changing coordinates Mumford to theta) and compute a suitable affine lift $\widetilde{x+t}$ of $x+t$.*

P4. *Compute a totally positive element $\beta = u + v\sqrt{D}$ of norm ℓ, where $u, v \in \mathbf{Z}$ are computed as in Section 4.5, and the matrix F, such that $F \cdot F^t = \beta \cdot I_4$, of first row elements $(\alpha_1, \ldots, \alpha_4)$. Store $\beta, \alpha_1, \ldots, \alpha_4$ as elements in K_0 and as rational polynomials in π.*

[6] G is stable under Frobenius.

[7] The extension is of degree polynomial in ℓ.

[8] We assume that we are in the generic case. Here recall (4.3).

P5. *Compute the canonical* 2*-torsion basis from* $\widetilde{0}_{\mathcal{L}}$*, change to Mumford coordinates and compute the action of the Frobenius endomorphism* π *and the endomorphisms* $\alpha_1, \ldots, \alpha_4$ *on the* 2*-torsion points as actions on the abstract representation of the* 2*-torsion basis, namely* $\mathbf{Z}(2) \times \widehat{\mathbf{Z}}(2)$*. Store the action of* F *on the abstract representation of* $(\mathbf{Z}(2) \times \widehat{\mathbf{Z}}(2))^r$ *of* $K(\mathcal{L}^{\star r})$*.*

Compute the canonical basis of the 4*-torsion points from* $\widetilde{0}_{\mathcal{L}^2}$*, change to Mumford coordinates, compute the action of the Frobenius endomorphism* π *and the endomorphisms* $\alpha_1, \ldots, \alpha_4$ *on the* 4*-torsion points as actions on the abstract representation of the* 4*-torsion basis* $\mathbf{Z}(4) \times \mathbf{Z}(4)$*.*

P6. *Compute the action of* π *on* t *and* c'_t *representing the action of* $\sqrt{D}^{-1}$ *on* t*. Store* c'_t *and the scalars* b_s *representing the action of* α_s *on* t*, for all* $s = 1, \ldots, 4$*.*

P7. *Compute and store the least positive integer* c_Q *representing the action of* $\sqrt{D}$ *on* x*. Compute integers* u_s*,* v_s*, such that the positive integer* $u_s + v_s c_Q$ *represents the action of* α_s *on* x*.*

P8. *Compute the kernel* G_D *of the* (D, D)*-isogeny representing* $\sqrt{D}$*-endomorphism on* A *in Mumford coordinates over an extension* $\mathbf{F}'/\mathbf{F}_q$*.*[9] *Compute excellent affine lifts of its elements for the theta structure* $\Theta_{\mathcal{L}}$*.*

P9. *Compute once and for all* $\widetilde{u_s + v_s\sqrt{D}x}$*,* $\widetilde{u_s x}$*,* $\widetilde{v_s\sqrt{D}x}$ *via* `chain_mult`*.*

P10. *Compute once and for all* $\widetilde{x + \sqrt{D}^{-1}t}$ *and* $\widetilde{u_s x + t}$ *via* `chain_multadd`*. Compute the affine point* $\widetilde{\sqrt{D}x + t} = \mathtt{RM}_D(\widetilde{x + c'_t t})$ *via the* (D, D)*-isogeny of kernel* G_D*. Compute the affine theta coordinates of the point* $\widetilde{v_s\sqrt{D}x + t}$ *via the method* `chain_multadd`*.*

P11. *Store a look-up table consisting of all affine theta points* $\widetilde{u_s x + v_s\sqrt{D}x + at}$*, where* $s = 1, \ldots, r$ *and* $a \in \mathbf{Z}/\ell\mathbf{Z}$*. They are computed from (4.31) when given* $\widetilde{u_s x}$*,* $\widetilde{v_s\sqrt{D}x}$*,* $\widetilde{at}$*,* $\widetilde{u_s x + at}$*,* $\widetilde{u_s x + v_s\sqrt{D}x}$ *and* $\widetilde{v_s\sqrt{D}x + at}$*, for all* $a \in \mathbf{Z}/\ell\mathbf{Z}$ *and* $s = 1, \ldots, r$ *(the last two are computed independently with* `chain_multadd`*).*

There exists an ***algorithm*** *of above input and precomputed data that*

- *computes a target curve* C'*, with* $\mathrm{Jac}(C') \simeq_{\mathbf{F}_q} (B, \mathcal{M}_0)$ *in* $\mathcal{O}(\ell^2)$ *operations in* $\mathbf{F}$*;*
- *computes the image* $f(x) \in \mathrm{Jac}(C')$ *in* $\mathcal{O}(\ell^2)$ *operations in the field of definition over which the affine theta coordinates of the points* $u_s x + v_s\sqrt{D}x + w_s(a_1, a_2)t$ *are defined.*

Proof. We keep track of the number of operations (that are not constant in ℓ) performed in certain field extensions of $\mathbf{F}_q$.

1. We evaluate the right-hand side of equation (4.18).

   For a given $\mathbf{k} \in K_1(\mathcal{M}^{\star r})$, computing the index $\mathbf{i} \in K_1(\mathcal{L}^{\star r})$ is done in constant time in $\log q$ using the pre-computed data. Same for all elements in the kernel G.

   Computing the right-hand side of (4.18) requires $\ell^{r/2}(r-1)$ multiplications in the field $\mathbf{F}$. There are $\mathcal{O}(\ell^{r/2})$ total multiplications in the field $\mathbf{F}$.

2. We evaluate the right-hand side of equation (4.26).

   We use the precomputed data and therefore, for all $a_1, a_2 \in \mathbf{Z}/\ell\mathbf{Z}$ and for all $s = 1, \ldots, r$, given the scalar $w_s(a_1, a_2) \in \mathbf{Z}/\ell\mathbf{Z}$ we use the look-up tables for the affine points $\widetilde{u_s x + v_s\sqrt{D}x + w_s(a_1, a_2)t}$. In the end, to compute (4.26), there are $\mathcal{O}(\ell^{r/2})$ multiplications in the field of definition of the affine lifts $\widetilde{u_s x + v_s\sqrt{D}x + w_s(a_1, a_2)t}$. The field extension over $\mathbf{F}_q$ is polynomial in ℓ and D.

[9] The extension over $\mathbf{F}_q$ is polynomial in D.

3. We compute the symplectic transformation S.

   We compute the matrix S only once. It requires a constant time in ℓ and $\log q$ as the complexity depends only on level $n = 2$ and r. In practice, this can be speeded up if one finds a faster method for transforming a $4r$-by-$4r$ symplectic matrix with entries in $\mathbf{Z}/4\mathbf{Z}$ into a block-diagonal form (we only need to have a 4-by-4 block that will then correspond to the single copy $(B, \mathcal{M}, \Theta_{\mathcal{M}})$ in the product $(B \times B^{r-1}, \mathcal{M} \star \mathcal{M}^{\star(r-1)}, \Theta_{\mathcal{M}\star\mathcal{M}^{\star(r-1)}}))$. The brute-force method presented in Section 4.7 requires testing $(4)^{4r}$ matrices. The cost is constant in the number of operations over $\mathbf{F}_q$.

4. We apply the transformation formula.

   The main cost is given by computing the RHS of (4.40) as all the other operations are operations with very small integers.

   In the end we do not need but the elements of the form $(b, 0, 0, 0) \in K_1(\mathcal{M}^{\star r})$, where $b \in K_1(\mathcal{M})$, for the final theta structure. For each element $b \in K_1(\mathcal{M})$, it requires $n^4 = \#\mathbf{Z}(n) \cdot \#\mathbf{Z}(n)$ multiplications in the field of definition of the affine theta coordinates. In conclusion, for $x \in A$ and the theta null point of B, it requires n^6 (a constant number in ℓ) operations in $\mathbf{F}_q$.

5. We compute the Rosanhain invariants of the target curve C' via a constant number of operations (in ℓ) in the field of definition. If needed, in order to obtain a model over $\mathbf{F}_q$, we apply Mestre's algorithm [51].

6. We compute the point $f(x) \in \mathrm{Jac}(C')$ in Mumford coordinates by changing the coordinates from theta to Mumford as in [12]. If needed we apply the isomorphism given by the Mestre's algorithm to obtain the image of the point over $\mathbf{F}_q$.

□

Now, we briefly analyze below the costs of computing each step of the precomputed data.

P1 Computing a theta null point of level 2 requires extracting 4 square roots and a constant number in ℓ of multiplications and inversions in the field of definition of λ, μ, ν. Let $\mathbf{F}_{q'}$ be the field of definition of λ, μ, ν. The cost of extracting square roots of a quadratic residue is highly dependent on the field $\mathbf{F}_{q'}$ [75] and could be the most expensive part of this step.

Similarly, computing an affine theta null point $\widetilde{0}_{\mathcal{L}^2}$ requires extracting additional square roots and hence, is of order $\mathcal{O}(\log q')$ operations in $\mathbf{F}_{q'}$.

P2 Computing an affine lift of $t \in G$ for the theta structure $\Theta_{\mathcal{L}}$ out of its Mumford coordinates is done via the method in [12, §5.3] and requires a constant number of operations in ℓ in the field of definition of t (field that we denoted a priori by $\mathbf{F}$).

On the other hand, computing excellent affine lifts for all points in G is quite expensive. We briefly analyse it below. Following 16, in order to obtain excellent affine lifts of **all** kernel elements, we need to compute a sequence of affine lifts $\widetilde{2t}, \ldots, \widetilde{(\ell'+1)t}$, where $\ell = 2\ell' + 1$, via successive chain additions or chain multiplications as in 1.

We consider the number of operations in $\mathbf{F}$ in terms of ℓ. If $\ell' + 1$ is even, there exists $(\ell' + 1)/2$ operations `chain_mult` and $(\ell' + 1)/2 - 1$ operations `chain_add`. Otherwise, $\ell'/2$ operations `chain_mult` and $\ell'/2 + 1)$ operations `chain_add`. In addition, 1 inversion when computing λ_t, $4M + 1E$ per $\widetilde{mt_e}$ with $m = 2, \ldots, \ell'$. The exponentiations are with small exponents as we compute them in a row. Nevertheless, the algorithm requires $\mathcal{O}(\ell)$ operations in $\mathbf{F}$. In the end, to extract an ℓth root which is quite costly [75].

Algorithm 1 Computing $\widetilde{t}_e$ for all $t \in G$

```
Input: $m$, $\widetilde{t}$, $\widetilde{0}_{\mathcal{L}}$
for $m = 2, \dots, (\ell' + 1)$ do
    if $m = 2m'$ then
        $\widetilde{mt} \leftarrow$ chain_mult$(2, \widetilde{m't}, \widetilde{0}_{\mathcal{L}})$
    else
        $\widetilde{mt} \leftarrow (\widetilde{t}, -\widetilde{(m-2)t}, \widetilde{(m-1)t}, \widetilde{0}_{\mathcal{L}})$
    end if
end for
Compute $\lambda_t^{-1}$
for $m = 2 \dots \ell'$ do
    Compute $\lambda_t^{-m^2}$
    Compute excellent $\widetilde{mt}_e \leftarrow \lambda_t^{-m^2} \cdot \widetilde{mt}$
    Compute excellent $\widetilde{(\ell - m)(t)}_e$
end for
```

P3 Computing affine theta coordinates $\widetilde{x}$ and $\widetilde{x+t}'$ is constant in the number of operations over the fields of definition. To compute a suitable affine lift $\widetilde{x+t}$ of $x+t$ requires a `chain_multadd` operation of scalar ℓ and an inversion.

P4 Given that the regulator R_D and x_1 of a solution $x_1 + y_1\sqrt{D}$ to the Pell's equation $x^2 = Dy^2 + 1$ are of $\tilde{\mathcal{O}}(D^{1/2})$ [47], then we can estimate that a numeric approximation of $\log(\beta)$ is also of $\tilde{\mathcal{O}}(D^{1/2})$ and moreover, if $\beta = u + v\sqrt{D}$ then $u \in \tilde{\mathcal{O}}(D^{1/2})$.[10] To compute the first row of F such that $F \cdot F^t = \beta \cdot I_4$ and $\sqrt{D}$ as rational polynomials in π (coefficients in $\mathbf{Q}$) is also constant in ℓ and operations in $\mathbf{F}_q$. We also have that the numerical approximations $\log(\alpha_s) < \log(\beta)$.

P5 Computing the canonical 2-torsion basis from $\widetilde{0}_{\mathcal{L}}$ is fast as it requires some permutations of coordinates. To compute the action of Frobenius π we change from theta to Mumford (again constant time in $\log q$). It is enough to compute the action of π on elements of the 2-torsion basis and is also constant time in ℓ. Computing the action of the endomorphisms $\alpha_1, \dots, \alpha_4$ on the 2-torsion points as degree 3 polynomials in π over $\mathbf{Z}/2\mathbf{Z}$ is again constant.

We do the same for the canonical basis of the 4-torsion basis and the cost is again constant in ℓ.

P6 The cost of computing the action of π on t is also constant in ℓ for the number of operations in $\mathbf{F}$. Computing the actions of $\alpha_1, \dots, \alpha_r$ on t requires evaluating r polynomials with coefficients in $\mathbf{Z}/\ell\mathbf{Z}$ and is also constant.

P7 Computing the least positive integer c_Q representing the action of $\sqrt{D}$ on x is given by evaluating at 1 a degree 3 polynomial with coefficients in $\mathbf{Z}/Q\mathbf{Z}$. For $s = 1, \dots, r$, computing integers u_s, v_s, such that the positive integer $u_s + v_s c_Q$ represents the action of α_s on x, follows from the representation of α_s in K_0 (reducing the rational representation in $\mathbf{Z}/Q\mathbf{Z}$) and is also done in constant number of operations over $\mathbf{F}_q$. The values $u_s + v_s c_Q$ are of size $\tilde{\mathcal{O}}(D^{1/2}c_Q)$.

P8 It requires computing a basis of the D-torsion points in Mumford coordinates. According to [66, §7.6], the cost of a deterministic algorithm is $\tilde{\mathcal{O}}(D^6)$ (without logarithmic factors). To compute the kernel of the $\sqrt{D}$ endomorphism, we consider the action of $\sqrt{D}$ as a rational polynomial in π, reduce its coefficients in $\mathbf{Z}/D\mathbf{Z}$ (if possible) and compute the action of the polynomial on the D-torsion basis. The basis elements killed by $\sqrt{D}$ determine the kernel G_D. Computing excellent

[10] We use $\tilde{\mathcal{O}}(D)$ when we omit logarithmic factors in D.

affine lifts for the elements in G_D is of cost $\mathcal{O}(D^4)$ operations in $\mathbf{F}$, plus an extraction of a Dth root ξ of unity and $\mathcal{O}(D^2)$ multiplications by ξ. In total the cost is of order $\tilde{\mathcal{O}}(D^6)$.

P9 Computing $\widetilde{u_s + v_s\sqrt{D}x}$, $\widetilde{u_s x}$, $\widetilde{v_s\sqrt{D}x}$ via 3`chain_mult` is of cost equal to $\tilde{\mathcal{O}}(D^{1/2}c_Q)$ multiplications in $\mathbf{F}'$.

P10 Computing $\widetilde{x + \sqrt{D}^{-1}t}$ and $\widetilde{u_s x + t}$ via `chain_multadd` is of cost $\tilde{\mathcal{O}}(D^{1/2})$ operations in $\mathbf{F}'$. Computing the affine point $\widetilde{\sqrt{D}x + t} = \mathtt{RM}_D(\widetilde{x + c_t^{-1}t})$ via the (D, D)-isogeny of kernel $G_D = \langle g_1, g_2 \rangle$ is of cost $\mathcal{O}(D^2)$ in the field over which the suitable affine theta coordinates of $z + g_1$, $z + g_2$ and $z + g_1 + g_2$ are defined (recall $z = x + \sqrt{D}^{-1}t$).

Computing the affine theta coordinates of the point $\widetilde{v_s\sqrt{D}x + t}$ via the method `chain_multadd` is of cost $\tilde{\mathcal{O}}(D^{1/2})$ operations in $\mathbf{F}'$.

P11 Given $\widetilde{v_s\sqrt{D}x + t}$ and $\widetilde{u_s x + t}$, computing the look-up table consisting of all affine theta points $\widetilde{u_s x + at}$ and $\widetilde{v_s\sqrt{D}x + at}$, for all $a \in \mathbf{Z}/\ell\mathbf{Z}$ (each of them is computed independently with `chain_multadd`) is of cost $\mathcal{O}(\ell)$ operations in the respective fields of definition. In the end, the number of operations in $\mathbf{F}'$ is constant when computing (4.31).

Following the analysis above we argue that the following theorem is immediate:

Theorem 4.8.2. *Consider the following **input data:***

I1. a finite field of definition $\mathbf{F}_q$, a prime degree ℓ;

I2. a smooth hyperelliptic curve C of genus 2 over $\mathbf{F}_q$.

Let π represent the Frobenius endomorphism. Let $K = \mathbf{Q}(\pi)$ and let the quadratic field $K_0 \subset K$ be of discriminant D. We assume the following conditions with respect to real multiplication on $A = \mathrm{Jac}(C)$:

*H1. $\mathrm{End}(A) \simeq \mathcal{O} \subset K$ is of **maximal real multiplication**, i.e., $\mathcal{O}_0 = \mathcal{O} \cap K_0$ is the ring of integers of K_0 ;*

*H2. the **index of** $[\mathcal{O} \colon \mathbf{Z}[\pi, \overline{\pi}]]$ is **prime** to $2\ell Q$;*

*H3. there **exists a totally positive element** $\beta \in \mathcal{O}_0$ of **norm** ℓ such that $\beta(t) = 0$.*

*There exists an **algorithm** of above input and satisfying the conditions above that*

— computes a target isogenous curve C' in polynomial time in $\log q$ and ℓ.

— computes the image $f(x) \in \mathrm{Jac}(C')$ in polynomial time in $\log q$, ℓ and D.

5 Denominators of Igusa Class Polynomials

5.1 Introduction

In the previous chapter, we focused on computing rational, cyclic isogenies between Jacobians of genus 2 hyperelliptic curves defined over some finite field $\mathbf{F}_q$. Moreover, the abelian varieties have complex multiplication by orders in a quartic field $K = \mathbf{Q}(\pi)$ and admit maximal real multiplication by $\mathcal{O}_0 \subset K_0$ (see Section 4.1). As mentioned in the introduction, one of the applications of computing cyclic isogenies is to prove random self-reducibility in genus 2 [37]. Following this work, the DLP on a given Jacobian with CM by $\mathcal{O}_K$ is efficiently reduced via cyclic isogenies to the DLP on a uniformly random Jacobian with CM by $\mathcal{O}_K$.

Therefore, one of the major parameters from a security point of view is the quartic field K or the Frobenius polynomial χ_π that generate $K/\mathbf{Q}$. If we choose $\mathbf{F}_q$ of large characteristic and the polynomial χ_π such that $N = \chi_\pi(1)$ is divisible by a large prime number, the previous security statement is in alignment with the mainstream cryptographic constraints for choosing a genus 2 curve, i.e., the group of rational points on the Jacobian of the curve (over a finite field of large characteristic) is required to admit a subgroup of large prime order.

Similarly to elliptic curve cryptography, in order to have a secure scheme based on hyperelliptic curves we need to solve one of the two following problems. First, given a curve equation over a finite field, how can we compute efficiently the order of the group of rational points on the Jacobian of the curve? The second question could be seen as the converse to the previous one, namely given a large prime number Q, how can we generate efficiently a hyperelliptic curve over a sufficiently large finite field whose Jacobians has a subgroup of order Q?

An answer to the second question is given by the CM method in genus 2 [73, 80] based on computing and factoring Igusa class polynomials. Given a primitive quartic CM field K, the Igusa class polynomial of index $k \in \{1, 2, 3\}$ is $H_k(X) := \prod_C (X - i_k(C)) \in \mathbf{Q}[X]$, where the product is over the isomorphism classes of complex hyperelliptic curves C, whose Jacobians have CM by the maximal order $\mathcal{O}_K$ and where $i_k(C)$ is the so called kth Igusa invariant of the isomorphism class [74, Def. 2.1.]. When Igusa class polynomials are reduced modulo a prime p, a triple of algebraic numbers i_1, i_2, i_3 that are roots of H_1, H_2 and H_3 respectively, could correspond to hyperelliptic curves over $\mathbf{F}_p$, with CM by the same order $\mathcal{O}_K$, and whose isomorphism class (over $\overline{\mathbf{F}}_p$) is identified with (i_1, i_2, i_3). Similarly to the case of elliptic curves, one method of computing the Igusa polynomials is by estimating their complex roots and finding numerical approximations of the coefficients. Since the polynomials are rational this approach gives rise to a new problem, namely having an accurate bound on the denominators.

The work of Goren and Lauter [24] establishes a connection between the denominators of Igusa class polynomials and certain embeddings of $\mathcal{O}_K$ into the matrix algebra $M_2(\mathbb{B}_{p,\infty})$, where p is a prime number and $\mathbb{B}_{p,\infty}$ is the quaternion algebra over $\mathbf{Q}$ that is ramified only at p and ∞.

Let A be the Jacobian of a hyperelliptic curve C that is defined over a number field k and has CM by $\mathcal{O}_K$, namely $\iota\colon \operatorname{End}_k(A) \to \mathcal{O}_K$ is an isomorphism. Then, if K is primitive, C has bad reduction modulo a prime $p \in \mathbf{Q}$ if and only if there exists a solution to the embedding problem for the prime p, namely there exists a prime ideal $\mathfrak{p}|p$ of $\mathcal{O}_k$ such that $A \pmod{\mathfrak{p}}$ is isomorphic over the field $k(p) = \mathcal{O}_k/\mathfrak{p}$ to a product of supersingular, isogenous elliptic curves $E_1 \times E_2$ with product polarizations [24, Lem. 4.1.1., Thm 4.1.2]. In this case, there exists a ring embedding

$$\iota\colon \mathcal{O}_K \to \operatorname{End}(E_1) \times \operatorname{End}(E_2).$$

and the Rosati involution coming from the product polarization induces complex conjugation on $\mathcal{O}_K$.

Given a prime p for which C has bad reduction, the elements $f \in \operatorname{End}(E_1) \times \operatorname{End}(E_2)$ written as $f = \begin{pmatrix} f_{1,1} & f_{1,2} \\ f_{2,1} & f_{2,2} \end{pmatrix}$, for $f_{i,j} \in \operatorname{Hom}(E_j, E_i)$, are embedded in a subring of $M_2(\mathbb{B}_{p,\infty})$ as explained in [24, p.6],[28, §5.1]. More precisely, consider a supersingular elliptic curve E_1 over $\overline{\mathbf{F}}_p$ whose endomorphism ring is isomorphic to a maximal order $\mathcal{O}$ of $\mathbb{B}_{p,\infty}$. Let $\psi\colon \operatorname{End}(E_1) \to \mathcal{O}$. The set of isomorphism classes of supersingular curves over $\overline{\mathbf{F}}_p$ that are isogenous to E_1 is in bijection to the set of left ideal classes of $\mathcal{O}$. Given ψ and $\phi \in \operatorname{Hom}(E_1, E_2)$, the supersingular curve E_2 is of endomorphism ring $\operatorname{End}(E_2)$ isomorphic to some maximal order $\mathcal{O}' \subset \mathbb{B}_{p,\infty}$. Moreover, an element of $f \in \operatorname{End}(E_1) \times \operatorname{End}(E_2)$ is identified with a square matrix in

$$\mathcal{R}_{E_1,E_2,\phi} := \begin{pmatrix} \mathcal{O} & I \\ I^{-1} & \mathcal{O}' \end{pmatrix},$$

where the ideal $I = \psi(\operatorname{Hom}(E_2, E_1)\phi)$ is of right order $\mathcal{O}'$.

The result of [24, Cor. 5.1.2.] proves that if the prime p divides the denominators of the Igusa class polynomials, then the curve has bad reduction or equivalently, there exists a solution to the embedding problem as above. The reciprocal is not true as it is experimentally proven in [24, §6.2.] for the case of $p = 2$. Following this result, the next natural step is to compute a precise value or a tight bound for the exponents in the prime factorisation of the denominators. First, a new method of counting embeddings was proposed in [28, Prop 6.1.], namely given the curves E_1, E_2, the isomorphism ψ and the homomorphism ϕ, in order to fix an embedding ι it is sufficient to find two elements in $\mathcal{R}_{E_1,E_2,\phi}$ satisfying specific conditions.

Afterwards, by extending the previous work on counting embeddings and their image in $\mathcal{R}_{E_1,E_2,\phi}$ for all possible primitive quartic K, the work of Lauter and Viray [45] and [44] provides an exact formula or a tight bound for all prime powers appearing in the denominators of Igusa class polynomials. The authors propose an alternative to the criterion of finding embeddings of the above form. Instead, in addition to the pair of supersingular elliptic curves (E_1, E_2) and the embedding ι, they look for endomorphisms $x, u \in \operatorname{End}(E_1)$, $z \in \operatorname{End}(E_2)$ and an isogeny $y\colon E_1 \to E_2$ of certain properties [45, Proof Thm. 2.1]. The main result of [45] and [44] computes the valuation of the intersection number at any prime ℓ.

It generalizes the Gross–Zagier formula [27] that computes the factorization of

$$J(d_1, d_2) = \prod_{\substack{[\tau_1],[\tau_2] \\ \mathrm{disc}(\tau_i)=d_i}} \left(j(\tau_1) - j(\tau_2)\right),$$

where d_i are fundamental discriminants of imaginary quadratic fields that are relatively prime to each other and $[\tau_i]$ are elements in the Siegel upper half plane, modulo the action of $\mathbf{SL}_2(\mathbf{Z})$. In the case of [44], the formula is no longer restricted to discriminants of maximal orders or that are prime to each others. In [44, Thm. 5.1.2], the evaluation of $J(d_1, d_2)$ depends on the number of ideals of norm not prime to the conductor of the order the ideal belongs to. The counting problem and its solution is presented in the next section and summarized in Lemma 5.2.1.

5.2 Ideals in Non Maximal Orders

The work in this section was done in collaboration with Kristin Lauter and Bianca Viray. We are interested in the number of ideals of arbitrary norm N that are contained in non maximal orders of a real quadratic field K. Consider $d = f^2 \cdot D$ be the discriminant of such order $\mathcal{O}_d$ of K. We write the order as a $\mathbf{Z}$-module of the form $\mathcal{O}_d := \mathbf{Z} + f\mathbf{Z} \cdot \dfrac{D+\sqrt{D}}{2}$. In order to prove the main result of this section, we use through out the theory of localisations at a prime p. First, we denote by $\mathbf{Z}_{(p)}$ the localization of $\mathbf{Z}$ by p. In a similar manner, the localisation of $\mathcal{O}_d$ at p is denoted by $\mathcal{O}_{d_p}$.

According to [62, p.68], $\mathcal{O}_d = \cap_{\mathfrak{p}} O_{d_p}$, where $\mathfrak{p}|p$ are prime ideals of $\mathcal{O}_d$ that are not 0. Moreover, the invertible ideals of $\mathcal{O}_d$ become principal ideals in any $\mathcal{O}_{d_\mathfrak{p}}$ as any localisation of $\mathcal{O}_d$ is a principal ideal domain. Consider a common prime factor p of both f and N, and let $s = v_p(f)$ and $k = v_p(N)$, where v_p denotes the p-adic valuation of a rational number. Let $f' := f/p^s$ be the factor of f that is not divisible by p. Hence, counting ideals is equivalent to counting all elements $\alpha := a_1 + b_1 \cdot p^s \frac{D+\sqrt{D}}{2}$ in $\mathcal{O}_{d_p}$ whose norm satisfies $v_p(N(\alpha)) = k$ and that are unique up to multiplication by a unit in $\delta \in \mathcal{O}_{d_p}^\times$, i.e. $v_p(\delta) = 0$. Let $k_0 = \lfloor k/2 \rfloor$.

Lemma 5.2.1. *The $\mathcal{O}_{d_p}$-principal ideals of norm p^k satisfy*

— *if $k < 2s$*

— *if k is even, then there are p^{k_0} ideals of the form*

$$(p^{k_0} + bp^s \frac{D+\sqrt{D}}{2})\mathcal{O}_{d_p}, \text{ for } b \in \mathbf{Z}/p^{k_0}\mathbf{Z},$$

— *if k is odd, then there are 0 ideals.*

— *if $k \geq 2s$:*

— *if $p|D$ and $v_p(\frac{D^2-D}{4}) = 1$,*

— *if k is odd, then there are p^s ideals of the form*

$$\left(bp^{k_0+1} + p^{k_0}\frac{D+\sqrt{D}}{2}\right)\mathcal{O}_{d_p}, \text{ for } b \in \mathbf{Z}/p^s\mathbf{Z}.$$

— *if k is even, then there are p^s ideals of the form*

$$\left(p^{k_0} + bp^{k_0}\frac{D+\sqrt{D}}{2}\right)\mathcal{O}_{d_p}, \text{ for } b \in \mathbf{Z}/p^s\mathbf{Z}.$$

— *if* $p|D$ *and* $v_p(\frac{D^2-D}{4}) = 0$ *(*$p=2$*)*

— *if* k *is odd, then there are* p^s *ideals of the form*

$$\left(p^{k_0} + bp^{k_0}\frac{D+\sqrt{D}}{2}\right)\mathcal{O}_{d_p},\ \textit{for } b \in (\mathbf{Z}/p^{s+1}\mathbf{Z})^\times.$$

— *if* k *is even, then there are* p^s *ideals of the form*

$$\left(bp^{k_0+1} + p^{k_0}\frac{D+\sqrt{D}}{2}\right)\mathcal{O}_{d_p},\ \textit{for } b \in \mathbf{Z}/p^{s-1}\mathbf{Z},$$

$$\left(p^{k_0} + bp^{k_0+1}\frac{D+\sqrt{D}}{2}\right)\mathcal{O}_{d_p},\ \textit{for } b \in \mathbf{Z}/p^{s-1}\mathbf{Z}.$$

— *if* $\left(\frac{D}{p}\right) = 1$*. Let* $\alpha_p \in \mathbf{Z}$ *such that* $D \equiv \alpha_p^2 \pmod{p}$*.*
Let $u_0 = -2^{-1}(D+\alpha_p)$ *and* $u_1 = -2^{-1}(D-\alpha_p)$*.*

— *if* k *is odd, then there are* $(k+1-2s)(p^s - p^{s-1})$ *ideals of the form*

$$\left(u_0p^n + bp^{k-n} + p^n\frac{D+\sqrt{D}}{2}\right)\mathcal{O}_{d_p},\ \textit{for } b \in (\mathbf{Z}/p^s\mathbf{Z})^\times \textit{ and } s \le n \le k_0$$

$$\left(u_1p^n + bp^{k-n} + p^n\frac{D+\sqrt{D}}{2}\right)\mathcal{O}_{d_p},\ \textit{for } b \in (\mathbf{Z}/p^s\mathbf{Z})^\times \textit{ and } s \le n \le k_0.$$

— *if* k *is even, then there are* $(k+1-2s)(p^s - p^{s-1})$ *ideals of the form*

$$\left(u_0p^n + bp^{k-n} + p^n\frac{D+\sqrt{D}}{2}\right)\mathcal{O}_{d_p},\ \textit{for } b \in (\mathbf{Z}/p^s\mathbf{Z})^\times \textit{ and } s \le n \le k_0$$

$$\left(u_1p^n + bp^{k-n} + p^n\frac{D+\sqrt{D}}{2}\right)\mathcal{O}_{d_p},\ \textit{for } b \in (\mathbf{Z}/p^s\mathbf{Z})^\times \textit{ and } s \le n < k_0.$$

— *if* $\left(\frac{D}{p}\right) = -1$*.*

— *if* k *is even, then there are* $p^s + p^{s-1}$ *ideals of the form*

$$\left(ap^{k_0+1} + p^{k_0}\frac{D+\sqrt{D}}{2}\right)\mathcal{O}_{d_p},\ \textit{for } a \in \mathbf{Z}/p^{s-1}\mathbf{Z},$$

and

$$\left(p^{k_0} + bp^{k_0}\frac{D+\sqrt{D}}{2}\right)\mathcal{O}_{d_p},\ \textit{for } b \in \mathbf{Z}/p^s\mathbf{Z}.$$

— *if* k *is odd, then there are* 0 *ideals.*

Let $u := \frac{D+\sqrt{D}}{2}$ and $v := \frac{D^2-D}{4}$.

Consider two generators α, β of the same ideal in $\mathcal{O}_{d_p}$. Since $\alpha/\beta = \alpha\beta^c/N(\beta)$, where the norm of β satisfies $v_p(N(\beta)) = k$ and β^c is the real quadratic conjugate of beta, then $\alpha\beta^c$ is an element of the ideal $p^k\mathcal{O}_{d_p}$.

More precisely,

$$\begin{aligned} \alpha\beta^c &= (a_1+b_1p^su)(a_2+b_2p^s\tfrac{D-\sqrt{D}}{2}) \\ &= \big(a_1a_2+a_1b_2p^sD+b_1b_2p^{2s}v\big)+(a_2b_1-a_1b_2)p^su, \end{aligned} \tag{5.1}$$

with:

$$a_1a_2+a_1b_2p^sD+b_1b_2p^{2s}v \in p^k\mathbf{Z}_{(p)} \tag{5.2}$$

and

$$a_2b_1-a_1b_2 \in p^k\mathbf{Z}_{(p)}. \tag{5.3}$$

In order to deduce when the above conditions (5.2),(5.3) are achieved, we compute first $v_p(N_1)$ and $v_p(N_2)$, where N_1, N_2 are the norms of α and β respectively. Immediately, the norm of the element $a_i+b_ip^s\frac{D+\sqrt{D}}{2}$ is

$$N_i = a_i^2+a_ib_ip^sD+b_i^2p^{2s}v. \tag{5.4}$$

Due to the lower bound of the sum, namely $v_p(a+b)\geq \min(v_p(a),v_p(b))$ for any $a,b\in\mathbf{Z}_{(p)}$, we have:

$$k \geq \min\left(v_p(a_i^2+a_ib_ip^sD), v_p(b_i^2p^{2s}v)\right). \tag{5.5}$$

The minimum value on the right hand side of (5.5) yields that either

$$\begin{cases} v_p(a_i^2+a_ib_ip^sD) & =k & < v_p(b_i^2p^{2s}v), \\ v_p(b_i^2p^{2s}v) & =k & < v_p(a_i^2+a_ib_ip^sD), \\ 2v_p(a_i^2+a_ib_ip^sD) & = v_p(b_i^2p^{2s}v) & \leq k \end{cases} \tag{5.6}$$

As the value $v_p(b_i^2p^{2s}v)$ is at least $2s$, we first distinguish between two major cases, namely $k<2s$ and $k\geq 2s$.

5.2.1 Case $k<2s$

In this case, the RHS of (5.5) is equal to $v_p(a_i^2+a_ib_ip^sD)=k$. Again we have a sum of parameters for the valuation function. It implies that either

$$\begin{cases} 2v_p(a_i) & =k & < s+v_p(a_i)+v_p(b_i)+v_p(D), \\ s+v_p(a_i)+v_p(b_i)+v_p(D) & =k & < 2v_p(a_i), \\ s+v_p(a_i)+v_p(b_i)+v_p(D) & =2v_p(a_i) & \leq k \end{cases} \tag{5.7}$$

The last two cases cannot hold as they yield $k/2\geq v_p(a_i)\geq s$ that contradicts $k<2s$. Hence, automatically k is even and if we denote by $k_0:=k/2$, then $v_p(a_i)=k_0$. Automatically, the first condition (5.2) for $\alpha\beta^c\in p^k\mathcal{O}_{d_p}$ is true as the valuation of the first term, namely $v_p(a_1)+v_p(a_2)=2k_0$, is equal to k and is strictly smaller than $v_p(a_1b_2p^sD+b_1b_2p^{2s}v)\geq k_0+s$. So, the valuation at p of the sum is strictly p^k. Let $a_i'=a_i/p^{k_0}$ with $v_p(a_i')=0$. The second requirement (5.3) becomes equivalent to $a_2'b_1-a_1'b_2\in p^{k_0}\mathbf{Z}_{(p)}$ and eventually, to $a_2'b_1\equiv a_1'b_2 \pmod{p^{k_0}}$. Consider the projective space $\mathbf{P}^1(\mathbf{Z}/p^{k_0}\mathbf{Z})$ over the residue class ring $\mathbf{Z}/p^{k_0}\mathbf{Z}$. As a_2', a_1' cannot be zero, the statement of (5.3) is rewritten as equality of projective points

$$(a_1' \colon b_1) = (a_2' \colon b_2) \text{ in } \mathbf{P}^1(\mathbf{Z}/p^{k_0}\mathbf{Z}).$$

Without loss of generality, we can fix $a_1' = a_2' = 1$ and then, the projective points are equal if and only if $b_1 \equiv b_2 \pmod{p^{k_0}}$. This is the necessary and sufficient condition for α and β to be representatives of the same principal ideal in $\mathcal{O}_{d_p}$. For each class modulo p^{k_0}, we take an ideal class representative whose norm has p valuation equal to $2k_0 < 2s$. Since in the case of $a_i + b_i p^s \frac{D+\sqrt{D}}{2}$, the first term is $a_i = a_i' \cdot p^{k_0}$, the principal ideals are of the form

$$\left(p^{k/2} + bp^s \frac{D+\sqrt{D}}{2}\right)\mathcal{O}_{d_p}, \text{ for } b \in \{0, \dots, p^{k/2}-1\}. \tag{5.8}$$

The expression of each ideal representative is unique up to multiplicity by a unit of $\mathcal{O}_{d_p}$.

5.2.2 Case $k \geq 2s$

Let $t := v_p(a_i b_i D + b_i^2 p^s v)$ The relations (5.6) imply

$$\begin{cases} 2s \leq 2v_p(a_i) & = k & < s+t, \\ 2s \leq s+t & = k & < 2v_p(a_i), \\ s+t & = 2v_p(a_i) & \leq k \end{cases} \tag{5.9}$$

In the first two cases, we have $v_p(a_i) \geq s$ for both $i = 1, 2$. Moreover, the valuation t is again bigger or equal than the minimum of the two individual valuations and it yields:

$$\begin{cases} v_p(a_i) + v_p(b_i) + v_p(D) & = t & < s + 2v_p(b_i) + v_p(v), \\ s + 2v_p(b_i) + v_p(v) & = t & < v_p(a_i) + v_p(b_i) + v_p(D), \\ s + 2v_p(b_i) + v_p(v) & = v_p(a_i) + v_p(b_i) + v_p(D) & \leq t \end{cases} \tag{5.10}$$

If we are in the last case of (5.9), namely $t = 2v_p(a_i) - s \leq k - s$, the relations (5.10) yield $v_p(a_i) \geq s$ and hence, $a_i' = a_i/p^s \in \mathbf{Z}_{(p)}$ for both $i = 1, 2$ in all cases of (5.10). From now on, we consider the elements $\alpha_i = a_i' + b_i \frac{D+\sqrt{D}}{2}$ whose norm has p valuation equal to $k' = k - 2s \geq 0$ and we study when $\alpha_1 \alpha_2^c \in p^{k'}\mathcal{O}_{d_p}$ for $k' \geq 0$. More precisely,

$$\begin{aligned} \alpha_1 \alpha_2^c &= (a_1' + b_1 u)(a_2' + b_2 \tfrac{D-\sqrt{D}}{2}) \\ &= (a_1' a_2' + a_1' b_2 D + b_1 b_2 v) + (a_2' b_1 - a_1' b_2) u, \end{aligned} \tag{5.11}$$

with:

$$a_1' a_2' + a_1' b_2 D + b_1 b_2 v \in p^{k'}\mathbf{Z}_{(p)} \tag{5.12}$$

and

$$a_2' b_1 - a_1' b_2 \in p^{k'+s}\mathbf{Z}_{(p)}. \tag{5.13}$$

Next, we distinguish several cases depending on the relation between p and D.

5.2.2.1 Case p Splits in $\mathcal{O}_K$

In this case, D is a square modulo p and $v_p(D) = 0$. For p odd, we make a choice of a root of D and denote it by $\alpha_p := \sqrt{D} \pmod{p}$ for $\alpha_p \in \{1, .., p-1\}$. For a choice of sign $e \in \mathbf{Z}/2\mathbf{Z}$, let $u_e := 2^{-1} \cdot (D + (-1)^e \cdot \alpha_p)$. For $p = 2$, we are in the case of $D \equiv 1 \pmod{4}$ and we take $u = v = 1 \pmod{2}$.

Moreover, if $\alpha_i = a'_i + b_i u_e$, with $i = 1, 2$ for some sign e, generate the same ideal in $\mathcal{O}_{d_p}$ and so,

$$\min(v_p(a'_1), v_p(b_1)) = \min(v_p(a'_2), v_p(b_2)) =: n. \tag{5.14}$$

For fixed e, the real conjugate of α_i is $\alpha_i^c = a'_i + b_i u_{e+1}$. Since $N(\alpha_i) = \alpha_i \cdot \alpha_i^c$ is of p-valuation equal to k', we have $k' \geq 2n$. Consider a sign $e \in \mathbf{Z}/2\mathbf{Z}$ such that

$$v_p(a'_i + b_i u_e) = k' - n \text{ and } v_p(a'_i + b_i u_{e+1}) = n \tag{5.15}$$

for $i = 1, 2$. In the above equation, if $k' = 2n$, let the sign be $e = 1$.

If e is fixed in $\mathbf{Z}/2\mathbf{Z}$ and given the p-valuation of α_i from equation (5.15), we have $a_i \equiv b_i u_e \pmod{p^{k-n}}$ and hence,

$$a'_1 a'_2 \equiv b_1 b_2 u_e^2 \pmod{p^{2k-2n}}$$

In addition, $v_p(b_2) = v_p(b_2 D) \geq n$ and so,

$$a'_1 b_2 D \equiv -b_1 b_2 D u_e \pmod{p^{k-n+n}}.$$

Since $2k - 2n \geq k$ and $\alpha_p^2 = D \pmod{p^k}$, it follows that

$$a'_1 a'_2 + a'_1 b_2 D + b_1 b_2 v \equiv b_1 b_2 (u_e^2 - D u_e + v) \equiv 0 \pmod{p^k}$$

and the condition (5.12) is satisfied.

Consider equation (5.13). It is equivalent to the equality of projective points

$$\left(\frac{a'_1}{p^n} : \frac{b_1}{p^n}\right) = \left(\frac{a'_2}{p^n} : \frac{b_2}{p^n}\right) \in \mathbf{P}^1(\mathbf{Z}/p^{k'+s-2n}\mathbf{Z}).$$

As α_i/p^n has p-valuation equal to $k' - 2n$, we fix an embedding $\varphi_{e,n} \colon \mathbf{P}^1(\mathbf{Z}/p^{k'+s-2n}) \to \mathbf{P}^1(\mathbf{Z}/p^{k'-2n})$ such that

$$\left(\frac{a'_1}{p^n} : \frac{b_1}{p^n}\right) \in \mathbf{P}^1(\mathbf{Z}/p^{k'+s-2n}) \to (-u_e : 1) \in \mathbf{P}^1(\mathbf{Z}/p^{k'-2n})$$

and an embedding $\psi_{e,n} \colon \mathbf{P}^1(\mathbf{Z}/p^{k'+s-2n}) \to \mathbf{P}^1(\mathbf{Z}/p^{k'-2n+1})$ such that

$$\left(\frac{a'_1}{p^n} : \frac{b_1}{p^n}\right) \in \mathbf{P}^1(\mathbf{Z}/p^{k'+s-2n}) \to (-u_e : 1) \in \mathbf{P}^1(\mathbf{Z}/p^{k'-2n+1}).$$

Due to $v_p(\alpha_i/p^n) = k' - 2n$, the point $\left(\frac{a'_i}{p^n} : \frac{b_i}{p^n}\right)$ is not in the preimage of $(u_e : 1) \in \mathbf{P}^1(\mathbf{Z}/p^{k'-2n+1}\mathbf{Z})$. The set of principal ideal classes is in bijection with the set $\varphi_{e,n}^{-1}((u_e : 1)) \setminus \psi_{e,n}^{-1}((u_e : 1))$ of cardinality $p^s - p^{s-1}$.

Hence, for fixed e and n the ideals are of the form:

$$\left(\left(-u_e + bp^{k'-2n}\right)p^n + p^n\frac{D+\sqrt{D}}{2}\right)\mathcal{O}_{d_p},\ \text{where } b \in (\mathbf{Z}/p^s\mathbf{Z})^\times.$$

If k' is even and if $n = k' - n$ the two choices of e are equivalent. Otherwise for each $0 \leq n < k'/2$ we have two choices of e (one for $k' - n$ and, one for n respectively). In conclusion, for a given even number k', if we consider all possible integers n and all signs e corresponding to n, the number of ideals is equal to $(k'+1)(p^s - p^{s-1})$. Similarly, if k' is odd there are $\lfloor k'/2 \rfloor * 2 = (k'+1)(p^s - p^{s-1})$ ideals.

The ideal representatives in terms of $k = k' + 2s$ and $s \leq n < k/2$ are of the form:

$$\left(\left(u_0 + bp^{k-2n}\right)p^n + p^n\frac{D+\sqrt{D}}{2}\right)\mathcal{O}_{d_p}, \left(\left(u_1 + bp^{k-2n}\right)p^n + p^n\frac{D+\sqrt{D}}{2}\right)\mathcal{O}_{d_p},$$

where $b \in (\mathbf{Z}/p^s\mathbf{Z})^\times$, $u_0 = -2^{-1}(D + \alpha_p)$ and $u_1 = -2^{-1}(D + \alpha_p)$ with $\alpha_p = \sqrt{D} \pmod{p}$.

5.2.2.2 Case p is Inert in $\mathcal{O}_K$

In this case D is not a square modulo p and $v_p(D) = 0$. If $k' = 2k'_0 + 1$ then $v_p(a'_i) = v_p(b_i) = n \leq k'_0$ and $a'^2 = b^2u^2 \pmod{p^{k'-2n}}$. This gives no solution as u^2 is not a square modulo p and $k' - 2n$ is odd. If $k = 2k'_0$ then either $v_p(b_i) > v_p(a'_i) = k'_0$ or $v_p(a'_i) > v_p(b'_i) = k'_0$. Hence, it implies that $v_p(a'_1a'_2), v_p(b_1b_2u^2), v_p(b_1a'_2), v_p(a'_1b_2) \geq k'$ and (5.12) is automatically true. Then the value $\alpha_1\alpha_2^c$ is in $p^{k'}\mathcal{O}_{d_p}$ if and only if (5.13) holds, namely $(b_1a'_2 - a'_1b_2)$ is divisible by $p^{k'+s}$ and so,

$$\frac{a'_2}{p^{k'_0}}\frac{b_1}{p^{k'_0}} = \frac{a'_1}{p^{k'_0}}\frac{b_2}{p^{k'_0}} \pmod{p^s}.$$

Then,

$$\left(\frac{a'_1}{p^{k'_0}} : \frac{b_1}{p^{k'_0}}\right) = \left(\frac{a'_2}{p^{k'_0}} : \frac{b_2}{p^{k'_0}}\right)$$

in $\mathbf{P}^1(\mathbf{Z}/p^s\mathbf{Z})$.

Hence, depending whether $v_p(b_i) > v_p(a'_i)$ or $v_p(b_i) < v_p(a'_i) = k'_0$, there are p^s ideals of the form $p^{k'_0+s} + bp^{k'_0+s}u$, with $b \in \mathbf{Z}/p^s\mathbf{Z}$, and there are p^{s-1} ideals of the form $ap^{k'_0+s+1} + p^{k'_0+s}u$, with $a \in \mathbf{Z}/p^{s-1}\mathbf{Z}$.

The ideal representatives in terms of k and s are of the form:

$$\left(p^{k_0} + bp^{k_0}\frac{D+\sqrt{D}}{2}\right)\mathcal{O}_{d_p}, \left(ap^{k_0+1} + p^{k_0}\frac{D+\sqrt{D}}{2}\right)\mathcal{O}_{d_p},$$

for all possible $a \in \mathbf{Z}/p^{s-1}\mathbf{Z}$, $b \in \mathbf{Z}/p^s\mathbf{Z}$.

5.2.2.3 Case p Divides D

Assume that p divides D and consider the valuation $v_p(v)$. If p is odd, the valuation $v_p(D(D-1))$ is $v_p(D) = 1$ as D is free of odd squares. Otherwise if $p = 2$, the discriminant satisfies $D = 0 \pmod 4$ and $D/4$ square free, and equal to 2 or 3 modulo 4. Then the valuation of the ratio v at 2 is $v_2(D/4)$ which can be either 0 or 1.

Hence, if the prime p is odd then the valuation of $v_p(D) = v_p(v) = 1$. Otherwise, for $p = 2$ the valuation is $v_2(D) = v_p(v) + 2$ and we deduce another inequality, $v_p(D) \geq v_p(v)$ for any p dividing D.

We denote by $t' := v_p(a_i'b_iD + b_i^2v)$ and $k_0' := \lfloor k'/2 \rfloor$. As $v_p(a_i') = v_p(a_i) - s \geq 0$ and $t' = t - s$, the relations (5.9) and (5.10) become:

$$\begin{cases} 2v_p(a_i') & = k' & < t', \\ t' & = k' & < 2v_p(a_i'), \\ t' & = 2v_p(a_i') & \leq k' \end{cases} \tag{5.16}$$

and

$$\begin{cases} v_p(a_i') + v_p(b_i) + v_p(D) & = t' & < 2v_p(b_i) + v_p(v), \\ 2v_p(b_i) + v_p(v) & = t' & < v_p(a_i') + v_p(b_i) + v_p(D), \\ 2v_p(b_i) + v_p(v) & = v_p(a_i') + v_p(b_i) + v_p(D) & \leq t' \end{cases} \tag{5.17}$$

First, we prove that the minimum valuation among $a_i'^2$, $a_i'b_iD$ and b_i^2v is never given by $a_i'b_iD$. For that, we take all possible cases for t' and k'.

— Let $t' > 2v_p(a_i') = k'$. Then $2v_p(a_i')$ is the minimum among the terms Then, the relations of (5.17), together with $v_p(D) \geq v_p(v)$, imply

$$2v_p(a_i') < 2v_p(b_i) + v_p(v)$$

independently of p being odd or even.

— Let $t' \leq k'$ and $t' \leq 2v_p(a_i')$. If we consider either the first relation or the last relation of (5.17), then we obtain a contradiction due to:

$$v_p(a_i') \geq t' - v_p(a_i') \geq v_p(b_i) + v_p(D) \geq v_p(b_i) + v_p(v) > v_p(a_i') + v_p(D) > v_p(a_i').$$

So, the minimum valuation must be given by the second equation, namely $2v_p(b_i) + v_p(v) \leq t'$, that implies the following inequality

$$2v_p(a_i') \geq 2v_p(b_i) + v_p(v). \tag{5.18}$$

In conclusion the minimum is given by $2v_p(a_i')$ or $2v_p(b_i) + v_p(v)$. Next, we consider all possible values for $v_p(v)$.

— $v_p(v) = 0$, then $p = 2$ and $v_2(D) = 2$.
If $v_2(a_i) = v_2(b_i) = t$, then $v_2(N(\alpha_i)) = k'$ is equal to $2t + 1$ as $a_i'^2/2^{2t}$ and $b_i^2v/2^{2t}$ are odd and equivalent to 1 modulo 4 and $a_i'b_iD/2^{2t}$ is even. The relation (5.12) is verified with the same argument of having two odd terms, namely $a_1'a_2'/2^{2t}$ and $b_1b_2v/2^2t$, and one even, namely $a_1'b_2D$. Then the value $\alpha_1\alpha_2^c$ is in $p^{k'}\mathcal{O}_{d_2}$ if and only if (5.13) holds, namely $(b_1a_2' - a_1'b_2)$ is divisible

by 2^{2t+1+s} and so,

$$\frac{a_2'}{2^t}\cdot\frac{b_1}{2^t}=\frac{a_1'}{2^t}\cdot\frac{b_2}{2^t}\pmod{2^{s+1}}.$$

Then,

$$(\frac{a_1'}{2^t}:\frac{b_1}{2^t})=(\frac{a_2'}{2^t}:\frac{b_2}{2^t})$$

in $\mathbf{P}^1(\mathbf{Z}/2^{s+1}\mathbf{Z})$.

Hence, as t is equal to $\lfloor k/2\rfloor - s$, after multiplying α_i by p^s, there are $2^{s+1}-2^s=2^s$ principal ideals of the form

$$\left(2^{\lfloor k/2\rfloor}+b\cdot 2^{\lfloor k/2\rfloor}\frac{D+\sqrt{D}}{2}\right)\mathcal{O}_{d_2},\text{ with } b\in(\mathbf{Z}/2^{s+1}\mathbf{Z})^{\times}.$$

Here b is odd as otherwise $v_2(b\cdot 2^{\lfloor k/2\rfloor -s})>v_2(2^{\lfloor k/2\rfloor -s})$.

If $v_2(a_i')<v_2(b_i)$ or $v_2(a_i)>v_2(b_i)$, let $t=\min\{v_2(a_i'),v_2(b_i)\}$. Then $v_2(N(\alpha_i))=k'$ is even and moreover $t=k_0'=k'/2$ as either $a_i'^2/2^{2t}$ or $b_i^2v/2^{2t}$ out of three terms is odd. The relation (5.12) is immediately verified as the valuation of each individual term is at least $2t=k'$. Then the value $\alpha_1\alpha_2^c$ is in $p^{k'}\mathcal{O}_{d_2}$ if and only if (5.13) holds, namely $(b_1a_2'-a_1'b_2)$ is divisible by $2^{k'+s}$ and so,

$$\frac{a_2'}{2^{k_0'}}\cdot\frac{b_1}{2^{k_0'}}=\frac{a_1'}{2^{k_0'}}\cdot\frac{b_2}{2^{k_0'}}\pmod{2^s}.$$

Then,

$$(\frac{a_1'}{2^{k_0'}}:\frac{b_1}{2^{k_0'}})=(\frac{a_2'}{2^{k_0'}}:\frac{b_2}{2^{k_0'}})$$

in $\mathbf{P}^1(\mathbf{Z}/2^s\mathbf{Z})$.

If $v_p(b_i)<v_p(a_i')$, there are 2^{s-1} principal ideals of the form

$$\left(a\cdot 2^{k/2+1}+2^{k/2}\frac{D+\sqrt{D}}{2}\right)\mathcal{O}_{d_2},\text{ with } a\in\mathbf{Z}/2^{s-1}\mathbf{Z}.$$

If $v_p(a_i')<v_p(b_i)$, there are 2^{s-1} principal ideals of the form

$$\left(2^{k/2}+b\cdot 2^{k/2+1}\frac{D+\sqrt{D}}{2}\right)\mathcal{O}_{d_2},\text{ with } b\in\mathbf{Z}/2^{s-1}\mathbf{Z}.$$

— $v_p(v)=1$, then either $v_p(D)=3$ or $v_p(D)=1$. If $k=2k_0+1$ then the minimum is given by $2v_p(b_i)+1$ and hence, $v_p(b_i)=k_0-s<v_p(a_i')$. As $k-(k_0-s)-(k_0+1)=s$, condition (5.13) is equivalent

$$\frac{a_1}{b_1p^{k_0+1}}=\frac{a_2}{b_2p^{k_0+1}}\pmod{p^s}$$

and with a similar argument as before, we obtain

$$\left(ap^{\lfloor k/2\rfloor+1}+p^{\lfloor k/2\rfloor}\frac{D+\sqrt{D}}{2}\right)\mathcal{O}_{d_p},\text{ with } a\in\mathbf{Z}/p^s\mathbf{Z}.$$

If $k = 2k_0$, then the minimum is given by $2v_p(a_i') = k_0' < 2v_p(b_i) + 1$. The ideals are of the form:

$$\left(p^{k/2} + bp^{k/2}\frac{D+\sqrt{D}}{2}\right)\mathcal{O}_{d_p}, \text{ with } b \in \mathbf{Z}/p^s\mathbf{Z}.$$

In both cases we have the same number of ideals, namely p^s. This completes the proof of lemma 5.2.1.

5.3 Table of Results

We summarize the results of this lemma in the following table:

k and s	p and D	Ideals	Number od Ideals
$k < 2s$, $k = 2k_0$	-	$(p^{k_0} + bp^s \frac{D+\sqrt{D}}{2})\mathcal{O}_{d_p}$, for $b \in \mathbf{Z}/p^{k_0}\mathbf{Z}$	p^{k_0}
$k < 2s$, $k = 2k_0 + 1$	-	-	0
$k \geq 2s$, $k = 2k_0$	$p \mid D$ and $v_p(\frac{D^2-D}{4}) = 1$	$\left(p^{k_0} + bp^{k_0} \frac{D+\sqrt{D}}{2}\right)\mathcal{O}_{d_p}$, for $b \in \mathbf{Z}/p^s\mathbf{Z}$	p^s
	$p \mid D$ and $v_p(\frac{D^2-D}{4}) = 0$ $p = 2$	$\left(bp^{k_0+1} + p^{k_0} \frac{D+\sqrt{D}}{2}\right)\mathcal{O}_{d_p}$, $\left(p^{k_0} + bp^{k_0+1} \frac{D+\sqrt{D}}{2}\right)\mathcal{O}_{d_p}$, for $b \in \mathbf{Z}/p^{s-1}\mathbf{Z}$	p^s

	$\left(\frac{D}{p}\right) = 1$	$\left(u_0p^n + bp^{k-n} + p^n \frac{D+\sqrt{D}}{2}\right)\mathcal{O}_{d_p}$,
		for $b \in (\mathbf{Z}/p^s\mathbf{Z})^\times$, $s \leq n \leq k_0$, and
		$\left(u_1p^n + bp^{k-n} + p^n \frac{D+\sqrt{D}}{2}\right)\mathcal{O}_{d_p}$,
		for $b \in (\mathbf{Z}/p^s\mathbf{Z})^\times$, $s \leq n < k_0$
			$(k + 1 - 2s)(p^s - p^{s-1})$

	$\left(\frac{D}{p}\right) = -1$	$\left(ap^{k_0+1} + p^{k_0} \frac{D+\sqrt{D}}{2}\right)\mathcal{O}_{d_p}$, $\left(p^{k_0} + bp^{k_0} \frac{D+\sqrt{D}}{2}\right)\mathcal{O}_{d_p}$, for $a \in \mathbf{Z}/p^{s-1}\mathbf{Z}$, $b \in \mathbf{Z}/p^s\mathbf{Z}$	$p^s + p^{s-1}$
$k \geq 2s$, $k = 2k_0 + 1$	$p \mid D$ and $v_p(\frac{D^2-D}{4}) = 1$	$\left(bp^{k_0+1} + p^{k_0} \frac{D+\sqrt{D}}{2}\right)\mathcal{O}_{d_p}$, for $b \in \mathbf{Z}/p^s\mathbf{Z}$	p^s
	$p \mid D$ and $v_p(\frac{D^2-D}{4}) = 0$ $p = 2$	$\left(p^{k_0} + bp^{k_0} \frac{D+\sqrt{D}}{2}\right)\mathcal{O}_{d_p}$, for $b \in (\mathbf{Z}/p^{s+1}\mathbf{Z})^\times$	p^s
	$\left(\frac{D}{p}\right) = 1$	$\left(u_0p^n + bp^{k-n} + p^n \frac{D+\sqrt{D}}{2}\right)\mathcal{O}_{d_p}$, $\left(u_1p^n + bp^{k-n} + p^n \frac{D+\sqrt{D}}{2}\right)\mathcal{O}_{d_p}$, for $b \in (\mathbf{Z}/p^s\mathbf{Z})^\times$, $s \leq n \leq k_0$	$(k + 1 - 2s)(p^s - p^{s-1})$
	$\left(\frac{D}{p}\right) = -1$	-	0

5.4 Examples

We implemented the ideal representatives in Magma for the purpose of computing the intersection formula in [44] and extending the current Magma packages with a library of computing ideals of arbitrary norm in non-maximal orders.

We consider the first example of [44], namely the quartic field is $K = \mathbf{Q}(-119 + 28\sqrt{17})$ and the prime appearing in the denominators of Igusa polynomials is $\ell = 7$. First, we notice that ℓ is ramified in K and moreover, we need to count ideals of norm 28 and 7 that are not prime to the conductor and that satisfy the conditions specified in [44, Thm 5.1.2.]. There exists only 1 such ideal of norm 7 (and none of norm 28) and the ideal corresponds to solution of multiplicity 2, and hence, the intersection number at prime 7 is equal to 2.

The second example takes a quartic field $K = \mathbf{Q}(-13 + 3\sqrt{13})$ that does not satisfy the assumptions of the Bruinier-Yang formula as $D = 2613$ and is not equivalent to 1 mod 4. For the prime 23, the work of Bruinier-Yang provides an incorrect intersection number at $\ell = 23$. The work of [44] proves that there are indeed four solutions to the Embedding Problem, two of which depend on counting ideals in non-maximal quadratic orders.

Bibliography

[1] L. Adleman. A subexponential algorithm for the discrete logarithm problem with applications to cryptography. In *FOCS*, pages 55–60. IEEE, 1979.

[2] L. Adleman, J. DeMarrais, and M. Huang. A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobians of large genus hyperelliptic curves over finite fields. *ANTS*, pages 28–40, 1994.

[3] L. Adleman, J. DeMarrais, and M. Huang. A subexponential algorithm for discrete logarithms over hyperelliptic curves of large genus over GF(q). *Theor. Comput. Sci.*, 226(1-2):7–18, 1999.

[4] D. V. Bailey, L. Batina, D. J. Bernstein, P. Birkner, J. W. Bos, H.-C. Chen, C.-M. Cheng, G. van Damme, G. de Meulenaer, L. J. Dominguez Perez, J. Fan, T. Güneysu, F. Gurkaynak, T. Kleinjung, T. Lange, N. Mentens, R. Niederhagen, C. Paar, F. Regazzoni, P. Schwabe, L. Uhsadel, A. Van Herrewege, and B.-Y. Yang. Breaking ECC2K-130. Cryptology ePrint Archive, Report 2009/541, 2009. http://eprint.iacr.org/2009/541.

[5] D. Bernstein and T. Lange. Two grumpy giants and a baby. *The Open Book Series*, 1(1):87–111, 2013.

[6] C. Birkenhake and H. Lange. *Complex Abelian Varieties*, volume 302 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2004.

[7] J. Bos, A. Dudeanu, and D. Jetchev. Collision bounds for the additive Pollard rho algorithm for solving discrete logarithms. *J. Mathematical Cryptology*, 8(1):71–92, 2014.

[8] J. W. Bos, M. E. Kaihara, T. Kleinjung, A. K. Lenstra, and P. L. Montgomery. Solving a 112-bit prime elliptic curve discrete logarithm problem on game consoles using sloppy reduction. *International Journal of Applied Cryptography*, 2(3):212–228, 2012.

[9] J. W. Bos, T. Kleinjung, and A. K. Lenstra. On the use of the negation map in the Pollard rho method. In Guillaume Hanrot, François Morain, and Emmanuel Thomé, editors, *Algorithmic Number Theory – ANTS-IX*, volume 6197 of *Lecture Notes in Computer Science*, pages 67–83. Springer, Heidelberg, 2010.

[10] R. P. Brent and J. M. Pollard. Factorization of the eighth Fermat number. *Mathematics of Computation*, 36(154):627–630, 1981.

[11] Certicom. Press release: Certicom announces elliptic curve cryptosystem (ECC) challenge winner. http://www.certicom.com/index.php/2002-press-releases/38-2002-press-releases/340-notre-dame-mathematician-solves-eccp-109-encryption-key-problem-issued-in-1997, 2002.

[12] R. Cosset. *Applications des fonctions theta a la cryptographie sur courbes hyperelliptiques*. PhD thesis, Loria, Nancy, 2011.

[13] R. Cosset and D. Robert. Computing (ℓ, ℓ)-isogenies in polynomial time on Jacobians of genus 2 curves. http://eprint.iacr.org/2011/143, 2011.

[14] C. Diem. An index calculus algorithm for plane curves of small degree. In *International Algorithmic Number Theory Symposium*, pages 543–557. Springer, 2006.

[15] C. Diem. On the discrete logarithm problem in class groups of curves. *Math. Comp.*, 80:443–475, 2011.

[16] C. Dou and M. Hildebrand. Enumeration and random random walks on finite groups. *The Annals of Probability*, 24(2):987–1000, 1996.

[17] R. Dupont. *Moyenne arithmético-géométrique, suites de Borchardt et applications.* PhD thesis, École polytechnique, Palaiseau, 2006.

[18] A. Enge. Computing discrete logarithms in high-genus hyperelliptic Jacobians in provably subexponential time. *Math. Comp.*, 71:729–742, 2002.

[19] P. Flajolet and A. M. Odlyzko. Random mapping statistics. In Jean-Jacques Quisquater and Joos Vandewalle, editors, *Eurocrypt 1989*, volume 434 of *Lecture Notes in Computer Science*, pages 329–354. Springer, Heidelberg, 1990.

[20] S. Galbraith and A. Stolbunov. Improved algorithm for the isogeny problem for ordinary elliptic curves. *Applicable Algebra in Engineering, Communication and Computing*, 24(2):107–131, 2013.

[21] P. Gaudry. An algorithm for solving the discrete log problem on hyperelliptic curves. *EUROCRYPT*, pages 19–34, 2000.

[22] P. Gaudry. Fast genus 2 arithmetic based on theta functions. *Journal of Mathematical Cryptology*, pages 243—-265, 2007.

[23] P. Gaudry, D. Kohel, and B. Smith. Counting points on genus 2 curves with real multiplication. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 504–519. Springer, 2011.

[24] E. Goren and K. Lauter. Class invariants for quartic CM fields. In *Annales de l'institut Fourier*, volume 57, pages 457–480, 2007.

[25] E. Goren and K. Lauter. The distance between superspecial abelian varieties with real multiplication. *Journal of Number Theory*, 129:1562–1578, 2009.

[26] A. S. Greenhalgh. *Random walks on groups with subgroup invariance properties.* PhD thesis, Stanford University, 1989.

[27] B. Gross and D. Zagier. On singular moduli. *J. Reine Angew. Math.*, 355:191–220, 1985.

[28] H. Grundman, J. Johnson-Leung, K. Lauter, A. Salerno, B. Viray, and E. Wittenborn. Igusa class polynomials, embeddings of quartic CM fields, and arithmetic intersection theory. *WIN–Women in Numbers: Research Directions in Number Theory, Fields Institute Communications*, 60:35–60, 2011.

[29] R. Harley. Elliptic curve discrete logarithms project. http://pauillac.inria.fr/~harley/.

[30] B. Harris. Probability distributions related to random mappings. *The Annals of Mathematical Statistics*, 31:1045–1062, 1960.

[31] F. Hess. Computing relations in divisor class groups of algebraic curves over finite fields. *preprint*, 2004.

[32] M. Hildebrand. Random walks supported on random points of $\mathbf{Z}/n\mathbf{Z}$. *Probability Theory and Related Fields*, 100:191–203, 1994.

[33] M. Hildebrand. A survey of results on random random walks on finite groups. *Probability Surveys*, 2:33–63, 2005.

[34] J.-I. Igusa. *Theta Functions*, volume 194 of *Grundlehren der mathematischen Wissenschaf-ten*. Springer, 1972.

[35] S. Ionica and E. Thomé. Isogeny graphs with maximal real multiplication. *Cryptology ePrint Archive*, 2014.

[36] D. Jao, S. D. Miller, and R. Venkatesan. Do all elliptic curves of the same order have the same difficulty of discrete log? In B. Roy, editor, *ASIACRYPT*, volume 3788 of *Lecture Notes in Computer Science*, pages 21–40. Springer, 2005.

[37] D. Jetchev and B. Wesolowski. Random self-reducibility of the discrete logarithm problem in genus two. *preprint*, 2014.

[38] J. H. Kim, R. Montenegro, Y. Peres, and P. Tetali. A birthday paradox for Markov chains, with an optimal bound for collision in the Pollard rho algorithm for discrete logarithm. In Alfred J. van der Poorten and Andreas Stein, editors, *Algorithmic Number Theory – ANTS-VIII*, volume 5011 of *Lecture Notes in Computer Science*, pages 402–415, 2008.

[39] J. H. Kim, R. Montenegro, and P. Tetali. Near optimal bounds for collision in Pollard rho for discrete log. In *FOCS '07: Proceedings of the 48th Annual IEEE Symposium on Foundations of Computer Science*, pages 215–223. IEEE Computer Society, 2007.

[40] Jeong Han Kim, Ravi Montenegro, Yuval Peres, and Prasad Tetali. A birthday paradox for Markov chains, with an optimal bound for collision in the Pollard rho algorithm for discrete logarithm. *The Annals of Applied Probability*, 20(2):495–521, 2010.

[41] Donald E. Knuth. *Seminumerical Algorithms.* The Art of Computer Programming. Addison-Wesley, Reading, Massachusetts, USA, 3rd edition, 1997.

[42] N. Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*, 48(177):203–209, 1987.

[43] S. Lang. *Introduction to Abelian and Algebraic Functions.* Springer-Verlag, second edition, 1982.

[44] K. Lauter and B. Viray. Denominators of Igusa class polynomials. *Publications mathématiques de Besançon*, 137(2):5–29, 2014.

[45] K. Lauter and B. Viray. An arithmetic intersection formula for denominators of Igusa class polynomials. *American Journal of Mathematics*, 137(2):497–533, 2015.

[46] K. Lauter and T. Yang. Computing genus 2 curves from invariants on the Hilbert moduli space. *Journal of Number Theory*, 131(5):936–958, 2011.

[47] H. W. Lenstra Jr. Solving the Pell equation. *Notices of the AMS*, 49(2):182–192, 2002.

[48] D. Lubicz and D. Robert. Computing isogenies between abelian varieties. *Compos. Math.*, 148(5):1483–1515, 2012.

[49] D. Lubicz and D. Robert. A generalisation of Miller's algorithm and applications to pairing computations on abelian varieties. *IACR Cryptology ePrint Archive*, 2013:192, 2013.

[50] D. Lubicz and D. Robert. Arithmetic on abelian and Kummer varieties. *Finite Fields and Their Applications*, 39:130–158, 2016.

[51] J.-F. Mestre. Construction de courbes de genre 2 à partir de leurs modules. In Teo Mora and Carlo Traverso, editors, *Effective Methods in Algebraic Geometry*, volume 94 of *Progress in Mathematics*, pages 313–334. Birkhäuser Boston, 1991.

[52] S. D. Miller and R. Venkatesan. Spectral analysis of Pollard rho collisions. In Florian Hess, Sebastian Pauli, and Michael E. Pohst, editors, *Algorithmic Number Theory – ANTS-VII*, volume 4076 of *Lecture Notes in Computer Science*, pages 573–581, 2006.

[53] S. D. Miller and R. Venkatesan. Non-degeneracy of Pollard rho collisions. *International Mathematics Research Notices*, 1:1–10, 2009.

[54] V. S. Miller. Use of elliptic curves in cryptography. In Hugh C. Williams, editor, *Crypto 1985*, volume 218 of *Lecture Notes in Computer Science*, pages 417–426. Springer, Heidelberg, 1986.

[55] J. S. Milne. Abelian varieties. www.jmilne.org/math/CourseNotes/AV.pdf.

[56] J. S. Milne. Abelian varieties. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 103–150. Springer, New York, 1986.

[57] J. Milnor and D. Husemoller. *Symmetric Bilinear Forms*. Springer-Verlag, 1973.

[58] R. Montenegro and P. Tetali. How long does it take to catch a wild kangaroo? In *STOC '09: Proceedings of the 41st annual ACM symposium on Theory of computing*, pages 553–560. ACM, 2009.

[59] P. L. Montgomery. Speeding the Pollard and elliptic curve methods of factorization. *Mathematics of Computation*, 48(177):243–264, 1987.

[60] D. Mumford. On the equations defining abelian varieties. I. *Inventiones Mathematicae*, 1:287–354, 1966.

[61] D. Mumford. *Abelian varieties*. Published for the Tata Institute of Fundamental Research, Bombay, 1970. Tata Institute of Fundamental Research Studies in Mathematics, No. 5.

[62] J. Neukirch. *Algebraic Number Theory*, volume 322. 1999.

[63] J. M. Pollard. A Monte Carlo method for factorization. *BIT Numerical Mathematics*, 15(3):331–334, 1975.

[64] J. M. Pollard. Monte Carlo methods for index computation (mod p). *Mathematics of Computation*, 32(143):918–924, 1978.

[65] J. M. Pollard. Kangaroos, monopoly and discrete logarithms. *Journal of Cryptology*, 13:437–447, 2000.

[66] D. Robert. *Fonctions thêta et applications à la cryptologie*. PhD thesis, Loria, Nancy, 2010.

[67] M. Rosen. *Abelian Varieties over* **C**. Arithmetic Geometry. Springer-Verlag, 1985.

[68] G. Rosenhain. Abhandlung fiber die Functionen zweier Variabler mit vier Perioden. *Ostwald's Klassiker der Exacten Wissenschaften*, 65, 1895.

[69] J-P. Serre and J. T. Tate. Good reduction of abelian varieties. *Ann. of Math. (2)*, 88:492–517, 1968.

[70] G. Shimura. *Abelian Varieties with Complex Multiplication and Modular Functions*. Princeton University Press, 1997.

[71] G. Shimura and Y. Taniyama. *Complex Multiplication of Abelian Varieties*. The Mathematical Society of Japan, 1961.

[72] V. Shoup. Lower bounds for discrete logarithms and related problems. In Walter Fumy, editor, *Eurocrypt 1997*, volume 1233 of *Lecture Notes in Computer Science*, pages 256–266. Springer, Heidelberg, 1997.

[73] A.-M. Spallek. *Kurven vom Geschlecht 2 und ihre Anwendung in Public-Key-Kryptosystemen*. PhD thesis, Universität Gesamthochschule Essen, 1994.

[74] M. Streng. *Complex Multiplication of Abelian Surfaces*. PhD thesis, Mathematical Institute, Faculty of Science, Leiden University, 2010.

[75] T.-W. Sze. On taking square roots without quadratic nonresidues over finite fields. *Mathematics of Computation*, 80(275):1797–1811, 2011.

[76] J. Tate. Endomorphisms of abelian varieties over finite fields. *Invent. Math.*, 2:134–144, 1966.

[77] E. Teske. On random walks for Pollard's rho method. *Mathematics of Computation*, 70(234):809–825, 2001.

[78] P. C. van Oorschot and M. J. Wiener. Parallel collision search with cryptanalytic applications. *Journal of Cryptology*, 12(1):1–28, 1999.

[79] W. C. Waterhouse and J. S. Milne. Abelian varieties over finite fields. In Donald J. Lewis, editor, *Number Theory Institute*, volume 20 of *Proceedings of Symposia in Pure Mathematics*, pages 54–64. American Mathematical Society, 1969.

[80] A. Weng. Constructing hyperelliptic curves of genus 2 suitable for cryptography. *Mathematics of Computation*, 72(241):435–458, 2003.

Name: Alina Dudeanu

Address: EPFL IC IIF LACAL , Room INJ335, Station 14, 1015 Lausanne, Switzerland

Telephone: +41 78 610 12 44

Email: alina.dudeanu@epfl.ch

CV

Education:

Sept. 2011 – present: EPFL, Switzerland: *PhD Student in Computer Science,* Laboratory for Cryptologic Algorithms (LACAL), under the supervision of Prof. **Arjen Lenstra** and Prof. **Dimitar Jetchev.**

Sept. 2009-July 2011: "UAIC" University of Iasi, Romania, *MSc in Computer Science,* Specialization: Information Security.

Sept. 2006-July 2009: "UAIC" University of Iasi, Romania. *Bachelor of Mathematics,* Specialization: Mathematics and Informatics.

Conferences, Workshops:

Alina Dudeanu, Razvan Oancea, Sorin Iftene **(2010)**: **"An x-Coordinate Point Compression Method for Elliptic Curves over F_p"**. Paper presented by the author at **SYNASC 2010**, held at the West University of Timisoara.

Additional Publications:

2014: Joppe W. Bos, **Alina Dudeanu**, Dimitar Jetchev: **"Collision Bounds for the Additive Pollard Rho Algorithm for Solving Discrete Logarithms"**, Journal of Mathematical Cryptology.

Talks:

*__July 2012__: **"Isogenies between elliptic curves"** at the CryptoBG*2012 summer school on Cryptography and Information Security, Bulgaria.

*__December 2013__: **"Cyclic Isogenies in genus 2"** at the seminar
Arbeitsgemeinschaft in Codierungstheorie und Kryptographie, University of Zurich.

*__May 2014__: **"Cyclic Isogenies in genus 2"** at the Conference
Theoretical and Practical Aspects of the DLP, Ascona, Switzerland.

*__May 2014__: **"Cyclic Isogenies in genus 2"** invited talk at the Institut de Mathématiques de Bordeaux.

*__February 2015__: **"Computing Denominators of Igusa Class Polynomials"** at the seminar Special LACAL@RISC Seminar on Cryptologic Algorithms, CWI, Amsterdam.

Internships:

***(June-September 2010)** Summer internship, School of Computer and Communication Sciences at **EPFL**, Switzerland. **Laboratory for Cryptologic Algorithms (LACAL)**
Supervisors: **Arjen Lenstra, Dimitar Jetchev.** Project: **Pollard rho**.

***(June-September 2014)** Summer internship, **Microsoft Research**,
Redmond, US in the **Cryptography Group.**
Supervisor: **Kristin Lauter**. Project: **Computing Denominators of Igusa Class Polynomials**.

Summer Schools:

2011: ACAGM Summer School in Leuven, on Elliptic Curves, Integer factorization, Groebner bases, codes.

2012: CryptoBG Summer School in Cryptography.

2012: Oberwolfach Seminar on Algorithms for Complex Multiplication over Finite Fields.

Current Projects:

I am finishing my PhD thesis and editing an article, **“Computing Cyclic Isogenies in Genus 2”**, for publication in a journal of Mathematics.

Abilities

Computer Skills:

Programming Languages: C++, C#, Java, Visual Basic, Matlab, Magma, Sage.

Markup Language: Latex.

Platforms: Mac, Windows, Linux.

Foreign Languages:

English (advanced - speaking, writing, reading, listening)

French (intermediate - speaking, writing, reading, listening)

Hobbies:

I enjoy reading, playing chess, dancing, hiking, swimming and traveling.

Referees:

Full Professor **Arjen Lenstra**, Laboratory for Cryptologic Algorithms, EPFL,

contact: arjen.lenstra@epfl.ch

SNSF-funded Professor **Dimitar Petkov Jetchev**, MATHGEOM, Jetchev Group, EPFL,

contact: dimitar.jetchev@epfl.ch