Arithmetic and geometric structures in cryptography

THÈSE N^{O} 8918 (2018)

PRÉSENTÉE LE 30 NOVEMBRE 2018

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

Benjamin Pierre Charles WESOLOWSKI

acceptée sur proposition du jury:

Prof. O. N. A. Svensson, président du jury
Prof. A. Lenstra, Dr R. Granger, directeurs de thèse
Dr P. Gaudry, rapporteur
Dr A. Enge, rapporteur
Prof. Z. Patakfalvi, rapporteur

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE
Suisse
2018

À ma famille

ACKNOWLEDGEMENTS & REMERCIEMENTS

My first and most heartfelt thanks go to Arjen K. Lenstra, a wonderful advisor. You gave me an unhoped-for level of freedom, and constant support along this journey. I am forever grateful for the trust you put in me. I was lucky to get not only one, but two fantastic advisors: many thanks to Robert Granger, for your guidance, and for introducing me to the marvelous world of discrete logarithms.

I am profoundly grateful to Dimitar Jetchev and Kenneth A. Ribet, who guided my first steps in research during my Master's thesis. Dimitar, I am very glad this first experience led to sustained collaboration, and I am looking forward to unravel more of the mysteries of isogeny graphs.

Many, many thanks go to Thorsten Kleinjung. Your patience, generosity and skills (as a mathematician and pastry chef) made it a blessing to work only two doors away from your office.

My sincere thanks go to Ola Svensson, president of the jury for both my candidacy exam and final defense, and to the three jury members Andreas Enge, Pierrick Gaudry and Zsolt Patakfalvi, who read this manuscript in great detail and provided invaluable feedback. *Pierrick, Andreas, je vous adresse mes amitiés sincères, et mes remerciements pour vos précieux conseils et votre accueil à Nancy et à Bordeaux.*

I would like to thank the present and past doctoral or post-doctoral researchers of LACAL for making it such a pleasant laboratory, through coffee breaks, lunches around a movie, research discussions, or afternoon cakes: Maxime Augier, Anja Becker, Alina Dudeanu, Aymeric Genêt, Novak Kaluđerović, Dušan Kostić, Andrea Miele, and Jens Zumbrägel. *Un remerciement spécial revient à ma merveilleuse collègue de bureau Marguerite Delcourt, qui n'autoriserait pas un jour de travail à être ennuyeux.* I am also indebted to a few collaborators across campus, notably Hunter Brooks, Enea Milio and Marius Vuille. *Merci également à Monique, toujours d'une grande aide.*

It is time for these acknowledgements to leave the walls of EPFL. This thesis allowed me to meet wonderful people, notably at conferences, sometimes leading to collaborations and meaningful friendships. *La première de ces rencontres a été celle de Cécile Pierrot, avec qui la collaboration nous a menés jusqu'en Arctique. Merci pour ta précieuse amitié. J'ai une pensée également pour Alexandre Gélin, « demi-frère de thèse », et co-explorateur du Wisconsin. Une mention toute particulière revient à Léo Ducas, qui m'a très tôt accordé sa confiance, en initiant une collaboration des plus stimulantes.* I am deeply grateful to Ronald Cramer, for your trust, and for welcoming me in Amsterdam. Léo, Ronald, I am glad I got the chance to work with you, and proud to be joining your group soon.

Sur une note plus personnelle, je tiens à remercier mes fantastiques amis lyonnais. Adèle, Arnaud, Claire, Johann, Julien, Olivier... je me sens chanceux d'avoir pu rester proche de vous tout en vivant dans un autre pays. Marion, merci pour tout, pour ton amitié, ton soutien, et ton vin de noix.

Finalement, la conclusion de ces remerciements revient à ma famille. À mes parents, dont je suis incroyablement fier. Je vous dois tout évidemment. À ma formidable sœur, Noémie, et à Andréa. Εν τέλει, στον Γιώργο για την συνεχή και αδιάλειπτη υποστήριξη του κάτω από οποιεσδήποτε συνθήκες.

A significant part of this work was supported by the Swiss National Science Foundation under grant number 200021-156420.

RÉSUMÉ

Nous explorons quelques structures algébriques et géométriques, à travers certaines questions posées par la cryptographie moderne. Nous nous attardons sur les logarithmes discrets dans les corps finis de petite caractéristique, la structure des graphes d'isogénies de variétés abéliennes ordinaires, et la géométrie des idéaux dans les corps cyclotomiques.

La difficulté présumée de calculer des logarithmes discrets dans certains groupes est essentielle pour la sécurité de bon nombre de protocoles de communication déployés aujourd'hui. L'un des choix les plus classiques pour le groupe sous-jacent est le groupe multiplicatif d'un corps fini. Mais ce choix commence à montrer son âge, et particulièrement lorsque la caractéristique du corps est petite : de récents algorithmes permettent de calculer des logarithmes efficacement dans ces groupes. Cependant, ces méthodes souffrent de n'être qu'heuristiques : elles semblent toujours fonctionner, mais on ne sait pas le prouver. Dans une première partie, nous proposons d'étudier ces méthodes dans l'espoir d'en gagner une meilleure compréhension, notamment en révélant les structures géométriques en jeu.

Un choix plus moderne est le groupe des points rationnels d'une courbe elliptique définie sur un corps fini. Là, le problème de calculer des logarithmes discrets semble au sommet de sa difficulté. Plus généralement, le groupe des points rationnels d'une variété abélienne (notamment la jacobienne d'une courbe de petit genre) pourrait être approprié. L'un des outils principaux pour l'étude des logarithmes discrets sur de tels objets est la notion d'isogénie : un morphisme d'une variété vers une autre, qui permet, entre autres, de transférer le calcul d'un logarithme. Là où la théorie est déjà bien développée pour les courbes elliptiques, peu est connu sur les structures que forment ces isogénies (les graphes d'isogénies) pour les variétés de dimension supérieure. Dans une deuxième partie, nous étudions la structure de ces graphes d'isogénies pour les variétés abéliennes ordinaires absolument simples, avec quelques conséquences concernant les logarithmes discrets sur les jacobiennes de courbes hyperelliptiques de genre 2, l'objet de prédilection de la cryptographie dite *hyperelliptique*.

La sécurité de bien des protocoles, notamment ceux reposant sur les logarithmes discrets, serait nulle face à un adversaire disposant d'un ordinateur quantique. Cette perspective pousse les cryptologues à étudier des problèmes qui résisteraient à une telle prouesse technologique. L'une des directions majeures est la cryptographie à base de réseaux euclidiens, se reposant sur la difficulé de trouver des vecteurs courts dans un réseau donné. Pour être efficace, il est avantageux de considérer des réseaux munis de plus de structure, tels que les idéaux d'un corps cyclotomique. Dans une troisième partie, nous étudions la géométrie de ces idéaux, et montrons qu'un ordinateur quantique permet d'y trouver efficacement des vecteurs bien plus courts que dans des réseaux génériques.

Mots-clefs : cryptanalyse, problème du logarithme discret, corps fini, variété abélienne, graphe d'isogénies, volcan d'isogénies, réseau idéal, problème du vecteur le plus court, corps cyclotomique, idéal de Stickelberger.

ABSTRACT

We explore a few algebraic and geometric structures, through certain questions posed by modern cryptography. We focus on the cases of discrete logarithms in finite fields of small characteristic, the structure of isogeny graphs of ordinary abelian varieties, and the geometry of ideals in cyclotomic rings.

The presumed difficulty of computing discrete logarithms in certain groups is essential for the security of a number of communication protocols deployed today. One of the most classic choices for the underlying group is the multiplicative group of a finite field. Yet this choice is showing its age, and particularly when the characteristic of the field is small: recent algorithms allow to compute logarithms efficiently in these groups. However, these methods are only heuristic: they seem to always work, yet we do not know how to prove it. In the first part, we propose to study these methods in the hope to get a better understanding, notably by revealing the geometric structures at play.

A more modern choice is the group of rational points of an elliptic curve defined over a finite field. There, the difficulty of the discrete logarithm problem seems at its peak. More generally, the group of rational points of an abelian variety (notably the Jacobian of a curve of small genus) could be appropriate. One of the main tools for studying discrete logarithms on such objects is the notion of isogeny: a morphism from a variety to another one, which allows, among other things, to transfer the computation of a logarithm. Whereas the theory for elliptic curves is already mature, little is known about the structures formed by these isogenies (the isogeny graphs) for varieties of higher dimension. In the second part, we study the structure of isogeny graphs of absolutely simple, ordinary abelian varieties, with a few consequences regarding discrete logarithms on Jacobians of hyperelliptic curves of genus 2, the main object of concern of so-called *hyperelliptic* cryptography.

The security of quite a few protocols, notably those relying on discrete logarithms, would collapse in front of an adversary equipped with a large-scale quantum computer. This perspective motivates cryptographers to study problems that would resist this technological feat. One of the major directions is cryptography based on Euclidean lattices, relying on the difficulty to find short vectors in a given lattice. For efficiency, one benefits from considering lattices endowed with more structure, such as the ideals of a cyclotomic field. In the third part, we study the geometry of these ideals, and show that a quantum computer allows to efficiently find much shorter vectors in these ideals than is currently possible in generic lattices.

Keywords: cryptanalysis, discrete logarithm problem, finite field, abelian variety, isogeny graph, isogeny volcano, ideal lattice, shortest vector problem, cyclotomic field, Stickelberger ideal.

CONTENTS

INTRODUCTION

Delving into the most abstract considerations, mathematicians uncover gems that one would sometimes be surprised to ever see reaching the concrete world. Modern cryptography holds serious responsibility for shining the spotlight on once arcane arithmetic and geometric structures, bringing them into our smartphones or other electronic devices.

A key problem. Classically, cryptography has been concerned with the problem of transforming a message into an unintelligible text, that only the legitimate recipient can decipher. There are convenient methods to achieve this, assuming that the sender and the recipient share a secret: a key (a word, a sequence of symbols, or nowadays a sequence of bits), that metaphorically allows the sender to lock the message (to encrypt) and the recipient to unlock it (to decrypt). This approach suffers a major shortcoming: it aims at communicating a secret message, but assumes that some secret, the key, has already been exchanged. The necessity for prior exchange of a secret had become accepted wisdom when Merkle started to challenge this idea in 1974 (published in 1978 [Mer78]). Two years later, Diffie and Hellman [DH76] achieved this foreseen paradigm shift by formalising the notion of public key cryptosystem, and describing an efficient protocol allowing two parties to exchange a secret key through a public communication channel.

Their protocol is surprisingly simple. Suppose Alice and Bob wish to exchange a common secret key. They first agree on a cyclic group G (written multiplicatively) and a generator g of this group. Alice secretly chooses a random integer a, and sends the group element g^a to Bob via the public communication channel. On his side, Bob also chooses a random integer b, and sends g^b to Alice. Both of them are now able to compute the value

$$(g^a)^b = (g^b)^a,$$

a shared secret, to be used as a key in subsequent communications. An outsider eavesdropping on the public channel knows g, g^a and g^b. Recovering the shared value g^{ab} from that information should be infeasible, and is known as the computational Diffie-Hellman problem (CDH). The security of this key exchange relies essentially on the difficulty of the *discrete logarithm problem* in the group G.

Definition 0.1 (The discrete logarithm problem)**.** Let g be a generator of a finite cyclic group G. The *discrete logarithm problem* in base g is the following: given an element h in G, find an integer n such that $h = g^n$.

This integer n is called a discrete logarithm of h in base g, written $\log_g(h)$, and is unique modulo the order of the group. Diffie and Hellman suggested to choose for group G the multiplicative group of a finite field, as the discrete logarithm problem in

these groups was suspected to be hard. Cryptography had met computational number theory, and this union has since proven itself exceedingly fruitful.

Discrete logarithms in finite fields of small characteristic. The Diffie-Hellman key exchange not only remains to this day one of the most commonly used cryptographic protocols over the Internet, but it also sparked a long series of cryptosystems whose security relies on the difficulty of computing discrete logarithms. The choice of the underlying group is of course critical for the security. Diffie and Hellman first proposed to use the multiplicative group of a field of prime order, i.e., a group $(\mathbf{Z}/p\mathbf{Z})^\times$ where p is a large prime number, and it was quickly suggested that arbitrary finite fields should be equally appropriate.

With this newly found motivation of breaking cryptographic schemes, new algorithms were developed to compute logarithms in such groups. Since the outcome of a discrete logarithm computation can easily be verified, one can effectively benefit from algorithms that have not been rigorously analysed. Not that there was a lack of interest for rigorous algorithms, but the methods employed proved very difficult to analyse, resulting in a long series of increasingly fast heuristic algorithms, with very few provable results. Today, a large gap separates the best known rigorous algorithms from the fastest heuristic ones, and this gap is the largest for fields of fixed characteristic (such as binary fields of order 2^n), for which heuristic quasi-polynomial time methods have recently been discovered.

The first part of this thesis is concerned with these questions of provability and heuristics in small characteristic. In **Chapter 1**, we explore the present situation and review the fastest known rigorous algorithm, analysed by Pomerance in 1987 [Pom87], and the first heuristic quasi-polynomial time algorithm, introduced by Barbulescu *et al.* in 2013 [BGJT14]. A second quasi-polynomial algorithm quickly followed, introduced by Granger *et al.* in 2014 [GKZ18]. More than just an alternative, it has the advantage of being provable for fields admitting a suitable model. In practice, such a model can be found very easily, yet a proof that it always exists seems out of reach. Another approach towards a fully provable algorithm would be to extend the methods of [GKZ18] to other models, yet that would require in the first place a better understanding of these methods. **Chapter 2** is based on the article

[KW18] T. Kleinjung and B. Wesolowski, *A new perspective on the powers of two descent for discrete logarithms in finite fields*, Thirteenth Algorithmic Number Theory Symposium – ANTS-XIII, 2018, proceedings to appear in the Open Book Series, Mathematical Sciences Publishers.

We revisit the algorithm of [GKZ18], and provide much simpler proofs, highlighting the geometric structures at play, and hopefully enlightening our understanding of the quasi-polynomial methods.

Isogeny graphs of ordinary abelian varieties. Facing the rapid progress of algorithms for computing discrete logarithms in the multiplicative group of finite fields, Miller [Mil86a] and Koblitz [Kob87] independently observed that the discrete logarithm problem can very well be instantiated on other groups, and suggested the use of the group of rational points of an elliptic curve over a finite field. More generally, the group of rational points of any abelian variety over a finite field could be appropriate, and this led to *hyperelliptic curve cryptography*, which considers Jacobians of certain algebraic curves.

An isogeny is a morphism between two abelian varieties. As group homomophisms, they can naturally be used to transfer an instance of the discrete logarithm problem from the source abelian variety to the target. Graphs of isogenies are thereby a useful tool in the study of the discrete logarithm problem: these are graphs whose vertices are abelian varieties and edges are isogenies between them. Most notably, isogeny graphs of (ordinary) elliptic curves were used by Galbraith, Hess and Smart in 2002 [GHS02] to heuristically extend the GHS Weil descent attack (which allows to compute discrete logarithms on certain elliptic curves) to a much larger class of elliptic curves. Three years later, Jao, Miller and Venkatesan [JMV05] exploited the structure of these graphs to show (assuming the extended Riemann hypothesis) that the discrete logarithm problem on a given elliptic curve cannot be hard if this curve is isogenous to sufficiently many elliptic curves where the problem is easy: we say that the discrete logarithm problem is *randomly self-reducible* over the isogeny class.

Isogeny graphs of elliptic curves are quite well understood, and have led to a wide variety of applications beyond discrete logarithms. The case of abelian varieties of higher dimension, however, has not been studied as much. Smith [Smi08] used isogenies to tackle the discrete logarithm problem on Jacobians of genus 3 hyperelliptic curves. Two constraints lessened the potential impact of his approach: not only the structure of the isogeny graph was not well understood, but at any rate, very few isogenies were actually computable. In recent years, the toolset for computing isogenies has considerably improved, and it has become worth developing a better understanding of the corresponding graphs.

The second part of this thesis studies the structure of isogeny graphs of absolutely simple, ordinary abelian varieties. We start in **Chapter 3** by studying *horizontal* isogeny graphs. Roughly speaking, an isogeny is horizontal if the source and the target have the same endomorphism ring. The vertices of a horizontal isogeny graph represent isogenous abelian varieties that all have the same endomorphism ring. Chapter 3 is mostly based on the article

[JW18] D. Jetchev and B. Wesolowski, *Horizontal isogeny graphs of ordinary abelian varieties and the discrete logarithm problem*, Acta Arithmetica (2018), in press.

Generalising the results of [JMV05], we prove that horizontal isogeny graphs with isogenies of bounded prime degree rapidly mix random walks: they are expander graphs. Moreover, this property is still true when restricting to the principally polarisable abelian varieties, in which case the isogenies can actually be computed. This proves in particular the "horizontal" random-self reducibility of the discrete logarithm problem for Jacobians of genus two curves (the main object of interest of hyperelliptic curve cryptography). These bounds on the degrees of isogenies yield expander graphs, and in particular, they are connected. But if one is only interested in the connectivity, these bounds are certainly not optimal. In the case of elliptic curves, good explicit bounds can be derived from Bach's work [Bac90], but these are not sufficient in higher dimension. We tackle this issue in **Chapter 4**, which is based on the article

[Wes18b] B. Wesolowski, *Generating subgroups of ray class groups with small prime ideals*, Thirteenth Algorithmic Number Theory Symposium – ANTS-XIII, 2018, proceedings to appear in the Open Book Series, Mathematical Sciences Publishers.

We generalise Bach's bounds to arbitrary subgroups of ray class groups, and derive bounds to obtain connected isogeny graphs of principally polarised abelian varieties of higher dimension.

To go beyond horizontal isogeny graphs, one must investigate how isogenies can change the endomorphism ring. This *vertical* structure of isogeny graphs is the object of **Chapter 5**, based on the article

[BJW17] E. H. Brooks, D. Jetchev, and B. Wesolowski, *Isogeny graphs of ordinary abelian varieties*, Research in Number Theory **3** (2017), no. 1, 28.

There again, the case of elliptic curves is well understood, thanks to Kohel's thesis [Koh96]: fixing a prime number ℓ, graphs of isogenies of degree ℓ (or ℓ-isogenies) form so-called *volcanoes*. These volcanoes are organised in levels, where the top-level (or *crater*, to sustain the geological metaphor) contains elliptic curves with maximal endomorphism ring (locally at ℓ), and the lower the level, the smaller the endomorphism ring. The real part of the endomorphism ring of an elliptic curve is always the ring of integers $\mathbf{Z}$, which is integrally closed (so maximal). The situation is more complicated in higher dimension, as the real part of the endomorphism ring is no longer necessarily maximal. It turns out that this maximality is crucial to obtain "volcano-like" structures: we fully describe isogeny graphs of $\mathfrak{l}$-isogenies (a generalisation of ℓ-isogenies to higher dimensions) for abelian varieties whose real part of the endomorphism ring is maximal. These graphs are volcanoes when certain number-theoretic conditions are met.

The key of this result is a new classification of orders in quadratic extensions, containing the maximal suborder. The lack of a complete classification of arbitrary orders makes it hard to study the full isogeny graph. However, in dimension two, we provide a local description of isogeny graphs of (ℓ, ℓ)-isogenies (an important class of isogenies that preserve principal polarisations), and analyse how such isogenies modify the real part of the endomorphism ring. These results allow us in particular to derive a "going up" algorithm, which finds a path of computable isogenies from an arbitrary abelian surface to one with maximal endomorphism ring.

Ideal lattices in cyclotomic fields. Together with the integer factorisation problem, the discrete logarithm problem is the foundation of the vast majority of today's deployed public key cryptosystems. However, in 1994, Shor [Sho97] discovered a fast algorithm to solve both of these problems on a hypothetical quantum computer. Over two decades later, it is still unclear when, if ever, a quantum computer of sufficient scale will be capable of executing Shor's algorithm. It is nevertheless considered a serious threat, especially in the recent years where research towards the construction of quantum computers has been fuelled by the promise of significant industrial applications. This has led cryptographers to investigate mathematical problems that would resist the charge of an adversary equipped with a quantum computer.

The problem of finding short vectors in a Euclidean vector space of high dimension soon proved to be a serious candidate. The private key would be a "good" basis of a lattice Λ in $\mathbf{R}^n$, consisting in n short vectors, while the public key would be a "bad" basis of the same lattice Λ, consisting in n much longer vectors. The bad, public basis is sufficient to perform simple operations like choosing a random lattice point, or encoding a message as a lattice point $P \in \Lambda$. If one adds a small "error" ε to this lattice point (i.e., shifting it slightly to get a close, non-lattice point), only the secret good basis allows to recover the original P from the noisy $P + \varepsilon$.

The main inconvenience of such plain lattice-based cryptosystems is their heavy memory and bandwidth footprint: the public and secret keys are both an $n \times n$ matrix where the dimension n is in the order of hundreds. This issue can be addressed by using lattices with more structure. An interesting choice are ideals in cyclotomic number fields, seen as lattices via the Minkowski embedding. There is however a risk that this extra structure allows for more efficient methods to solve supposedly hard problems in these lattices. And indeed, a series of results have led to new, fast quantum algorithms to solve certain lattice problems in principal ideals in cyclotomic fields of prime-power conductor. More precisely, following ideas outlined in [CGS14], it was shown how to find a generator of a principal ideal in quantum polynomial time [BS16], and how to transform a generator into a *short* generator by exploiting the geometry of cyclotomic units [CDPR16]. This short generator provides a much shorter lattice vector than what can normally be hoped for in polynomial time, in generic lattices. The third (and last) part of this thesis is mostly based on the article

[CDW17] R. Cramer, L. Ducas, and B. Wesolowski, *Short Stickelberger class relations and application to Ideal-SVP*, Advances in Cryptology – EUROCRYPT 2017 (J. Coron and J. B. Nielsen, eds.), Lecture Notes in Computer Science, vol. 10210, Springer, 2017, pp. 324–348.

More precisely, it is based on an ongoing collaboration with Ronald Cramer and Léo Ducas which aims at extending these results to arbitrary ideals (rather than principal) in arbitrary cyclotomic fields (rather than those of prime-power conductor). The outcome of this collaboration is split into two chapters. First, in **Chapter 6**, we present the method of [CDPR16], and extend upon their results by providing a full analysis of the numerical stability of the algorithm, and generalising it to cyclotomic fields of arbitrary conductor. Second, we show in **Chapter 7** how to extend these results to arbitrary, non-principal ideals. The methods at play, based on the geometry of the Stickelberger ideal, were introduced in the article [CDW17], and we present them in the more general setting of cyclotomic fields of arbitrary conductor.

Bibliographical note. Most chapters of this manuscript are based on published articles, as indicated by a note at the beginning of each concerned chapter. Such chapters are mostly a reproduction (with authorisation) of the corresponding articles, with modifications, sometimes substantial, made in an attempt to form a coherent narrative.

Other contributions. The great freedom I enjoyed as a doctoral candidate allowed me to work on a number of other projects that, mostly for the sake of the narrative, did not find their way in the present manuscript.

The following article shares ties with the second and third parts of this thesis, as it deals with isogeny graphs, and quantum-resistant cryptography:

[GW17] A. Gélin and B. Wesolowski, *Loop-abort faults on supersingular isogeny cryptosystems*, International Workshop on Post-Quantum Cryptography – PQCrypto 2017 (T. Lange and T. Takagi, eds.), Springer, 2017, pp. 93–106.

We show that in a context prone to side-channel attacks, cryptosystems based on isogeny graphs of supersingular elliptic curves [JD11] should be implemented with particular care as they are very susceptible to inexpensive fault attacks.

While the article [GW17] still deals with "algebraic and geometric structures in cryptography", the following articles are much more alien to this manuscript.

Randomness is a critical component of cryptography. Good sources of randomness are often supposed to operate in a concealed environment, generating bits that are meant to be kept secret. However, a number of applications require some form of publicly available randomness that cannot be predicted or manipulated. One would immediately think of national lotteries or sporting event draws, but trustworthy public sources of randomness also appear in more technical, cryptographic settings. Yet the problem of publicly generating randomness with a strong incorruptibility guarantee is a challenging one, as it is hard for someone to flip a coin and convince their peers that the outcome was not rigged. Methods using real-world entropy such as stock market prices [CH10] do not provide any formal security, and classic "commit-then-reveal" protocols do not scale. We address this problem in the article

[LW17] A. K. Lenstra and B. Wesolowski, *Trustworthy public randomness with sloth, unicorn, and trx*, International Journal of Applied Cryptography **3** (2017), no. 4, 330–343.

We describe a way to construct a source of randomness that takes as input random bits sent by any willing participant, and produces an output which any honest participant can verify to be unbiased and unpredictable, even if *everyone else* is controlled by an adversary. Nothing but random bits are requested from the contributers, so participating is very easy (as suggested in [LW17], it could be as simple as publishing a random tweet with some specified hashtag), and the communication complexity scales linearly in the number of contributors.

Other methods have been suggested, which do not provide such strong security guarantees. Notably, the inherent unpredictability of blockchains (in particular the Bitcoin blockchain [Nak09]) has been used to run lotteries, yet this method clearly assumes that a majority of the mining power is held by honest parties. We analyse more precisely how much an adversary with tighter computational and financial constraints could still bias this source of randomness in the following article:

[PW18] C. Pierrot and B. Wesolowski, *Malleability of the blockchain's entropy*, Cryptography and Communications **10** (2018), no. 1, 211–233.

As a tool for the solution we proposed in [LW17], we constructed what we called a *slow-timed hash function* (*sloth*): a function that takes a specified amount of time Δ to evaluate (and extensive parallel power does not allow to go faster, in a way reminiscent of Rivest, Shamir and Wagner's time lock puzzle [RSW96]: an amount Δ of sequential operations are required), but whose result can easily be verified by anyone (in time a small fraction of Δ, or even $\log(\Delta)$). Such functions have since then been formalised and generalised by Boneh *et al.* [BBBF18] as *verifiable delay functions*, and have found a variety of other applications in decentralised systems. Most notably, they can be used to design resource-efficient blockchains, eliminating the need for massively power-consuming mining farms. A few new delay functions are proposed in [BBBF18], reaching an exponential gap between the runtime of the evaluation and the verification (which was not the case for *sloth*). However, none of the practical constructions proposed strictly achieves the security or sequentiality requirements of verifiable delay functions. In the following paper, we propose a new efficient verifiable delay function, based on the

sequentiality of large exponentiation in finite groups of unknown order (such as RSA groups $(\mathbf{Z}/N\mathbf{Z})^\times$ where N is a product of two large primes, or class groups of quadratic imaginary fields):

[Wes18a] B. Wesolowski, *Efficient verifiable delay functions*, IACR Cryptology ePrint Archive, Report 2018/623, 2018, `https://eprint.iacr.org/2018/623`, submitted for publication.

The evaluation requires an amount Δ of sequential group squarings, and the output is a group element, together with a proof of correctness. The proof is short (a single group element), and allows to verify the correctness very fast, in time independent of Δ (essentially two group exponentiations, by exponents of bit-length the bit-security level, usually 128, 192 or 256).

PART I

DISCRETE LOGARITHMS IN FINITE FIELDS OF SMALL CHARACTERISTIC

1

Rigorous and heuristic algorithms

When Diffie and Hellman introduced the discrete logarithm problem in cryptography in 1976, the best known algorithms had complexity essentially the square root of the size of the group. These methods work in arbitrary groups, but interestingly, it was already suspected [MW68, Mil75] that the specific structure of finite fields could be exploited to design better algorithms. The sudden spotlight encouraged research on this path, and the square root complexity was quickly reduced by algorithms built around the *index calculus method*: a method which finds its roots in the early investigations of Kraïtchik [Kra22]. These are notoriously difficult to analyse. However, the result of a logarithm computation is easily verified, so cryptanalysis can profit from efficient algorithms that have not been rigorously evaluated. This has led to a long succession of faster heuristic algorithms, and very few rigorous results. The present chapter reviews this situation, by first recalling the classical generic methods, then specialising to finite fields of small characteristic, presenting the fastest known rigorous and heuristic algorithms to this day.

1.1. Generic algorithms for the discrete logarithm problem

Generic discrete logarithm algorithms assume very little knowledge about the group they are working with. It is only assumed that some algorithms, treated as black boxes, allow to compare, multiply, invert, and sample group elements.

1.1.1. The Pohlig-Hellman method. As a first step for the computation of a logarithm, it can be useful to try and split the problem into several simpler instances. This is the purpose of the Pohlig-Hellman method [PH78], which implies that when the group order and its factorisation are known, the difficulty of the discrete logarithm problem depends essentially on the size of the largest prime factor. These assumptions are usually not an issue in practice, as the groups used in cryptography for the discrete logarithm problem normally have a known prime order, sometimes with a small cofactor, and are thereby easy to factor.

Let G be a cyclic group of finite order n, g a generator, and h an arbitrary element which we want to compute the logarithm of. Suppose that the order of the group is known and given by $n = \prod_p p^{e_p}$. The Pohlig-Hellman method allows to split the logarithm computation in G into multiple logarithm computations in subgroups of G of prime order.

Consider the computation of $x = \log_g(h)$. For each prime factor p of the order n, let $n_p = n/p^{e_p}$, $g_p = g^{n_p}$ and $h_p = h^{n_p}$. Then each h_p belongs to the subgroup G_p of G of order p^{e_p} generated by g_p. Solving the discrete logarithm problem in these subgroups would yield

$$x_p = \log_{g_p}(h_p) \equiv x \mod p^{e_p},$$

from which a straightforward application of the Chinese remainder theorem allows to recover x. We have thereby reduced the problem from a group of order n to groups of prime-power orders p^{e_p}.

Now, the computation of $x_p = \log_{g_p}(h_p)$ can further be reduced to e_p logarithm computations in the subgroup $G^{n/p}$ of order p. To simplify the notation, we now assume that G is itself of prime-power order p^e. The idea is to compute sequentially the coefficients a_j such that

$$x \equiv a_0 + a_1 p + ... + a_{e-1} p^{e-1} \mod p^e.$$

Observe that $h^{p^{e-1}} = g^{xp^{e-1}} = g^{a_0 p^{e-1}}$. Therefore, one can retrieve the first coefficient a_0 as the logarithm of $h^{p^{e-1}}$ in the subgroup of order p generated by $g^{p^{e-1}}$. Now, assuming that the coefficients $a_0, \ldots, a_j$ are known, we have

$$\left(hg^{-\sum_{i=0}^{j} a_i p^i}\right)^{p^{e-j-2}} = g^{a_{j+1} p^{e-1}},$$

and one can compute a_{j+1} as the logarithm of the left-hand side element in the same subgroup of order p generated by $g^{p^{e-1}}$.

In conclusion, to compute a logarithm in a finite cyclic group G whose order factors as $n = \prod_p p^{e_p}$, it is sufficient to compute for each prime factor p, a number e_p of logarithms in the subgroup $G^{n/p}$ of order p.

1.1.2. Square root algorithms. In a generic finite cyclic group G, logarithms can be computed in $O(\sqrt{|G|})$ group operations. The simplest method to do so is certainly Shanks' baby-step giant-step algorithm. Let g be a generator and h be an element which we want to compute the discrete logarithm $x = \log_g(h)$ of. Let m be a parameter between 1 and $|G|$ to be tuned later. One can write $x = qm + r$ with $0 \leq r < m$ and $0 \leq q < |G|/m$. Of course, x is not known (yet), so r and q cannot be found by a Euclidean division. The idea is to proceed the other way around: find r and q such that $h = g^{qm+r}$, and deduce x. Equivalently, we are looking for q and r such that

$$(g^m)^q = hg^{-r}. \tag{1.1}$$

There are only m possible values for the right-hand side. We start by precomputing them in the following list (the *baby steps*):

$$B = \{(hg^{-r}, r) \mid 0 \leq r < m\},$$

at the cost of about m group operations. This list is stored as a hash map keyed by the first element of each pair. If it contains a pair $(1, r')$ it can be concluded that $x = r'$. Otherwise, for $q = 1, 2, \ldots, \lfloor |G|/m \rfloor$ in succession, the element $(g^m)^q$ is computed (the *giant steps*, corresponding to the left-hand side of Equation (1.1)) and looked up in the hash table. When a match is found, we get a pair $(hg^{-r}, r) \in B$ such that $hg^{-r} = (g^m)^q$, which implies $x = qm + r$. This method requires at most about $m + |G|/m$ group operations, which is minimised at $m = \lceil \sqrt{|G|} \rceil$, and results in a total of at most about $2\sqrt{|G|}$ group operations. Note that it has the great disadvantage of requiring storage of about $\sqrt{|G|}$ group elements.

Less memory and more scalability. The baby-step giant-step method is only the simplest of a variety of algorithms requiring $O(\sqrt{|G|})$ group operations. An important variant is Pollard's Rho algorithm [Pol78], which requires the storage of only $O(1)$ elements, whereas the baby-step giant-step requires $O(\sqrt{|G|})$. For practical purposes it is also crucial to be able to distribute the computation on any number of parallel processors. This can be achieved by variations of Pollard's Rho algorithm using distinguished points in the group, as described in [VOW99].

1.2. Index calculus methods

While black box groups are a powerful model for the design and analysis of discrete logarithm algorithms, it does not allow to exploit the particularities of a given group. Multiplicative groups of finite fields enjoy much more structure than generic groups, which can be exploited to design faster algorithms.

1.2.1. Index calculus algorithms. Modern methods to compute logarithms in the multiplicative group of finite fields are all variants of the index calculus method, and achieve much better performance than generic methods: they have subexponential complexities. Algorithms of this family are characterised by three phases: the relation collection phase, the linear algebra phase, and the individual logarithm phase. They work as follows.

Relation collection phase: This phase consists in collecting a large number of multiplicative relations between elements of a small subset of the group G, the *factor base*. Typically, the factor base would be a set of small prime numbers, or of irreducible polynomials of small degree, depending on the context. Let $\mathfrak{F}$ denote this factor base. We want to collect relations of the form

$$\prod_{f\in\mathfrak{F}} f^{m_f} = g^r,$$

where g is the generator, for various integers m_f and r. Each such relation implies the following linear relation between the logarithms of the factor base elements:

$$\sum_{f\in\mathfrak{F}} m_f \log_g(f) \equiv r \mod |G|.$$

The relation collection phase is over when enough relations have been collected, resulting in a linear system with a unique solution.

Linear algebra phase: This step consists in solving the full-rank linear system built in the previous phase, thus revealing the values of $\log_g(f)$ for all the elements f in the factor base.

Individual logarithm phase: This last phase consists in decomposing an arbitrary element h into a product of elements of the factor base, and thereby deduce its logarithm as a linear combination of known logarithms.

1.2.2. Small, medium, and large characteristic. With the development of these new algorithms, a trichotomy of finite field emerged, according to which variant of the index calculus method performs best: those of small, medium, or large characteristic. This classification (as well as the associated complexities) is expressed using the notation

$$L_q(\alpha, c) = e^{(c+o(1))(\log q)^\alpha (\log\log q)^{1-\alpha}},$$

where $\alpha \in [0,1]$ and $c > 0$, and $o(1)$ tends to zero as q tends to infinity. We also write $L_q(\alpha) = L_q(\alpha, O(1))$, and the subscript q is often omitted when there is no ambiguity.

Consider a family of finite fields of characteristic p and order $q = p^n$, where $p = L_q(\alpha)$ and q tends to infinity. We talk about small characteristic if $\alpha \leq 1/3$, medium characteristic if $\alpha \in [1/3, 2/3]$ and large characteristic if $\alpha \geq 2/3$ (leaving an ambiguity at the boundary cases $\alpha = 1/3$ and $\alpha = 2/3$). We also talk about fixed characteristic if p is constant and only n varies. Matching the intuition, fields of prime order are naturally of large characteristic, while binary fields (of order 2^n) are of fixed (and therefore small) characteristic.

1.3. A rigorous discrete logarithm algorithm in small characteristic

The first subexponential time index calculus algorithm for finite fields was proposed by Adleman [Adl79] in the late seventies. It was designed for fields of prime cardinality, and was soon adapted by Hellman and Reyneri [HR82] to finite fields of small characteristic. In its original form, this algorithm is heuristic, but Pomerance [Pom87] proposed a rigorous variant which remains to this day the fastest known provable algorithm for finite fields of small characteristic, with a complexity of $L(1/2)$. This variant and its analysis are presented below.

A first thing to note when designing an algorithm specialised to finite fields is that we are essentially free to choose how to represent the field, as long as it is in the form of a vector space over the prime subfield. Indeed, it is easy to find an isomorphism between two such representations of the same field [Len91]. Consider a finite field $\mathbf{F}_{q^\ell}$, and we can assume it is represented as the quotient $\mathbf{F}_q[x]/(I)$ where I is some irreducible polynomial of degree ℓ. Any element of the finite field is represented by its unique representative in $\mathbf{F}_q[x]$ of degree smaller than ℓ in this quotient structure (the *principal representative*). We are given a polynomial g representing a generator of the multiplicative group $\mathbf{F}_{q^\ell}^\times$, and a polynomial h representing an element of which we want to compute the logarithm. Pomerance's algorithm follows the stereotypical index calculus structure: a relation collection phase, a linear algebra phase, and an individual logarithm phase.

1.3.1. The relation collection phase. Any polynomial of $\mathbf{F}_q[x]$ factors in a unique way into a product of monic, irreducible polynomials, multiplied by a scalar (an element of $\mathbf{F}_q$). In this context, a natural choice for the factor base is the set of scalars and monic irreducible polynomials of small degree — say, bounded by a parameter d to be tuned later. Notice that the scalars can be dealt with separately since $g^{(q^\ell-1)/(q-1)}$ is a generator of $\mathbf{F}_q^\times$, and this subgroup is small enough to apply the generic methods from Section 1.1. Therefore we assume that we already know the logarithms of elements of $\mathbf{F}_q^\times$. The factor base is then defined as

$$\mathfrak{F} = \{f \in \mathbf{F}_q[x] \mid f \text{ is monic, irreducible, and of degree at most } d\}.$$

The idea behind the relation collection phase is then quite simple. Given an integer r generated uniformly at random in $[1, q^\ell - 1]$, the element g^r is uniformly distributed in $\mathbf{F}_{q^\ell}^\times$. The polynomial representing it is said to be d-smooth if it splits as a product of irreducible polynomials of degrees at most d. This smoothness condition is easy to check, as polynomials can be factored in polynomial time (see for instance the survey [VZGP01]). When it is indeed d-smooth, we get a decomposition of the form $g^r \equiv \alpha \prod_{f\in\mathfrak{F}} f^{e_f} \mod I$ with $\alpha \in \mathbf{F}_q^\times$, leading to the linear relation

$$\sum_{f\in\mathfrak{F}} e_f \log_g(f) \equiv r - \log_g(\alpha) \mod (q^\ell - 1). \tag{1.2}$$

A standard heuristic approach at this point would be to say that repeating this process $O(|\mathfrak{F}|)$ times should yield a full rank linear system with overwhelming probability, concluding the relation collection phase. Instead, to eliminate heuristics, Pomerance introduced the following lemma.

Lemma 1.1 ([Pom87, Lemma 4.1])**.** *Let V be a vector space of finite dimension n over a field k. Let S be a finite set of vectors in V and let $b_1, \dots, b_n$ be a basis of V. Let $m = \lfloor 2 \log_2 n \rfloor + 3$. Let $v_1, \dots, v_{mn}, w_1, \dots, w_{mn}$ be independently and uniformly distributed elements of S. Then, the linear subspace spanned by*

$$\{v_1, \dots, v_{mn}\} \cup \{b_j + w_{(j-1)m+i} \mid i = 1, \dots, m, \text{ and } j = 1, \dots, n\}$$

is the whole space V with probability at least $1 - 1/(2n)$.

This lemma provides a method to generate the set of relations with a rigorous, probabilistic guarantee of success. The vector space V is the space of all possible linear relations between elements of the factor base, or formally, tuples of the form $(e_f)_{f \in \mathfrak{F}}$. The set S is the set of tuples representing the decomposition of the d-smooth non-zero polynomials of degree less than ℓ. The basis $b_1, \dots, b_n$ consists of the canonical vectors $\mathbf{1}_f$, with value 1 at $f \in \mathfrak{F}$, and 0 everywhere else.

Remark 1.2. Of course, the coefficients of our linear relations live in $\mathbf{Z}/(q^\ell - 1)\mathbf{Z}$, which is not a field. However, a straightforward application of the Chinese remainder theorem implies that Lemma 1.1 almost holds when k is replaced by the ring $\mathbf{Z}/(q^\ell - 1)\mathbf{Z}$, and V is a free module of rank n. Instead of $1 - 1/(2n)$, the final probability becomes $(1 - 1/(2n))^{\omega(q^\ell - 1)}$, where $\omega(q^\ell - 1)$ is the number of distinct prime divisors of $q^\ell - 1$. Notice that the multiplicity of these prime divisors does not cause trouble: for any prime number s and positive integer m, given a generating set of vectors in $(\mathbf{Z}/s\mathbf{Z})^n$, any lift to $(\mathbf{Z}/s^m\mathbf{Z})^n$ is also a generating set.

Remark 1.3. One might wonder why instead, we do not apply the Pohlig-Hellman method from the start and present the algorithm in a prime order subgroup of $\mathbf{F}_{q^\ell}^\times$. That would save us the trouble of doing linear algebra in modules. The reason, again, is provability. Knowing the number of smooth polynomials of degree smaller than ℓ, it is easy to derive the smoothness probability of a uniformly random element of $\mathbf{F}_{q^\ell}^\times$. That probability is not as easy to compute for subgroups.

We have already seen how to collect random vectors playing the role of the vectors v_i: they correspond to the left-hand side of Relation (1.2). For the vectors of the form $b_j + w_{(j-1)m+i}$, we need to collect a new kind of relation. Fix a factor base element $b \in \mathfrak{F}$, and generate a random integer r from $[1, q^\ell - 1]$, until the principal representative of bg^r is d-smooth. The decomposition $bg^r \equiv \alpha \prod_{f \in \mathfrak{F}} f^{e_f} \mod I$ yields the relation

$$\log_g(b) - \sum_{f \in \mathfrak{F}} e_f \log_g(f) \equiv \log_g(\alpha) - r \mod (q^\ell - 1). \tag{1.3}$$

The left-hand side corresponds to vectors of the wanted form: a basis vector, plus a uniformly random vector from the set S.

This proves that with $n = |\mathfrak{F}|$ and $m = \lfloor 2 \log_2 n \rfloor + 3$, the relation collection phase succeeds with overwhelming probability after collecting mn relations of the form (1.2), and m relations of the form (1.3) for each $b \in \mathfrak{F}$.

1.3.2. The linear algebra phase. The relation collection phase returns a full rank linear system (with overwhelming probability), which can then be solved with Wiedemann's algorithm [Wie86]. Since $q^\ell - 1$ is not a prime number in general, one must first factor it and use the Chinese remainder theorem as well as some Hensel lifting argument in order to properly use Wiedemann's algorithm. This seems to require a fast, rigorous factoring algorithm; such an algorithm is indeed presented in [Pom87]. There is however a more elementary approach. One can first try their best to factor $q^\ell - 1$. The resulting decomposition consists in prime numbers and possibly a few composite numbers that seem hard to factor. It is possible to apply Wiedemann's algorithm modulo these composite numbers. The only error that can occur is that the algorithm tries to invert a non-invertible element. This would reveal a non-trivial factor of the modulus, and Wiedemann's algorithm could be applied again with the newly discovered factors. This may happen at most as many times as the number of distinct prime factors of $q^\ell - 1$, which is less than $\ell \log_2(q)$. Although it should actually happen much less often, this rough upper bound will not affect the complexity analysis below.

1.3.3. Individual logarithm phase. After the linear algebra phase, the logarithms of all the elements of the factor base are known, and we now wish to represent $\log_g(h)$ as a linear combination of them. This can be done in a way similar to the collection of relations. Simply generate a random integer r from $[1, q^\ell - 1]$ until the principal representative of hg^r is d-smooth. We get a decomposition $hg^r \equiv \alpha \prod_{f \in \mathfrak{F}} f^{e_f} \mod I$, which implies

$$\log_g(h) \equiv \log_g(\alpha) + \sum_{f \in \mathfrak{F}} e_f \log_g(f) - r \mod (q^\ell - 1).$$

As all the logarithms of the right-hand side are known, this concludes the final stage of the algorithm.

1.3.4. Analysis. In the first phase, we need to collect $O(|\mathfrak{F}| \log |\mathfrak{F}|)$ relations. Since a uniformly random polynomial of degree smaller than ℓ is d-smooth with probability $P = (\ell/d)^{-\ell/d + o(1)}$ (see [PGF98, Theorem 1]), each relation requires an expected $1/P$ number of trials. Since the factor base contains at most q^d elements the total expected cost of the first phase is at most

$$(\ell/d)^{\ell/d + o(1)} q^d \leq q^{(\ell/d \log_q(\ell/d) + d)(1 + o(1))}.$$

Choosing $d = \left\lceil \sqrt{\ell \log_q \ell / 2} \right\rceil$ leads to the complexity $L(1/2, \sqrt{2})$. Since Wiedemann's algorithm has quadratic cost in the dimension of the matrix (which is sparse, since each relation involves at most ℓ elements of the factor base), the linear algebra phase has the same complexity. Finally, the last phase has a negligible cost compared to the first, as it is equivalent to the generation of a single relation. Therefore Pomerance's algorithm has a provable expected complexity $L(1/2, \sqrt{2})$.

1.4. The descent is sufficient

Pomerance's algorithm relies on one crucial ingredient: a method to rewrite any element f of the group as a product of elements of the factor base (up to considering g and the scalars $\mathbf{F}_q^\times$ as part of the factor base). This process of rewriting an arbitrary element in terms of the factor base is called the *descent*. Pomerance's approach actually implies that given a rigorous descent algorithm, one can automatically devise a full rigorous index calculus algorithm, with a running time essentially determined by the size of the factor base and the complexity of the descent. This idea that the descent is sufficient

has been reworked in [EG02], then in [Die11] and [GKZ18]. The latest iterations enjoy a very neat analysis, which we present in a more abstract setting (by considering an arbitrary finite cyclic group) in the following theorem.

Theorem 1.4. *Consider a finite cyclic group G of order n, and two elements $g \in G$ and $h \in \langle g \rangle$. Assume we are given a factor base $\mathfrak{F} = \{f_1, \dots, f_m\} \subset G$, for some integer m, and an algorithm* Descent *that on input $f \in G$ outputs a sequence $(e_j)_{j=1}^m$ such that $f = \prod_{j=1}^m f_j^{e_j}$. Then, there is a probabilistic algorithm (Algorithm 1.1) that computes discrete logarithms in G at the expected cost of $O(m \log\log n)$ calls to the descent procedure* Descent*, and an additional $O(m^3 \log\log n)$ operations in $\mathbf{Z}/n\mathbf{Z}$.*

Algorithm 1.1 A full discrete logarithm algorithm from a descent algorithm.

Require: A finite cyclic group G of order n, two elements $g \in G$ and $h \in \langle g \rangle$.
We assume there is a descent algorithm for G: we are given a factor base $\mathfrak{F} = \{f_1, \dots, f_m\} \subset G$, and an algorithm Descent that on input $f \in G$ outputs a sequence $(e_j)_{j=1}^m$ such that $f = \prod_{j=1}^m f_j^{e_j}$.
Ensure: An integer x such that $g^x = h$.

```
repeat
    {Construct a matrix R = (r_{i,j}) ∈ (Z/nZ)^{(m+1)×m} and two column vectors α, β ∈ (Z/nZ)^{(m+1)} as follows}
    for i = 1, 2, ..., m + 1 do
        Choose α_i, β_i ∈ Z/nZ uniformly and independently at random;
        (r_{i,j})_{j=1}^m ← Descent(g^{α_i} h^{β_i});
    end for
    Compute a row echelon form R' of R with invertible row transformations;
    Apply these transformations to α and β, resulting in α' and β';
until gcd(β'_{m+1}, n) = 1
return −α'_{m+1}/β'_{m+1} mod n.
```

Remark 1.5. Algorithm 1.1 does not follow the traditional structure of an index calculus algorithm as it does not have distinguished relation collection and individual logarithm phases. It directly constructs relations involving the target $h \in \langle g \rangle$. This allows for a simpler, more straightforward analysis of the algorithm.

Proof. Note that for each row $(r_{i,j})_{j=1}^m$ of the matrix R, we have

$$g^{\alpha_i} h^{\beta_i} = \prod_{j=1}^m f_j^{r_{i,j}}.$$

Adding the fact that all the entries of the last row of the row echelon form R' vanish, we deduce that we have $g^{\alpha'_{m+1}} h^{\beta'_{m+1}} = 1$ at the end of each execution of the main loop. Therefore, if β'_{m+1} is invertible modulo n, then $g^{-\alpha'_{m+1}/\beta'_{m+1} \bmod n} = h$. This proves the correctness of the algorithm.

Concerning the running time, observe that the costly operations of the main loop are the $m+1$ calls to the algorithm Descent, and the computation of the row echelon form of R (which can be performed by a modification of the Gaussian elimination algorithm, with a cost of $O(m^3)$ operations in $\mathbf{Z}/n\mathbf{Z}$). It only remains to estimate the number of times the main loop must be repeated. The key observation there is that β'_{m+1} is uniformly distributed in $\mathbf{Z}/n\mathbf{Z}$ — assuming that the randomness used to generate α

and β is independent from all the random choices potentially made by DESCENT. Indeed, for each i, α_i and β_i are uniform and independent, so β_i is independent from $g^{\alpha_i}h^{\beta_i}$, and thereby also from the row $(r_{i,j})_{j=1}^{m}$. Then, β is also independent from the (invertible) transformation matrix U resulting in the row echelon form, and therefore $\beta' = U\beta$ is uniformly distributed over $(\mathbf{Z}/n\mathbf{Z})^{(m+1)}$, since β is. We deduce that the main loop needs to be executed an expected number of times $n/\varphi(n)$, where φ is Euler's totient function. We get the final cost from the estimate $n/\varphi(n) = O(\log\log n)$, found in [RS62]. □

1.5. A heuristic quasi-polynomial time algorithm

With a complexity of $L(1/2)$, Pomerance's variant of the Hellman-Reyneri algorithm remains the fastest rigorous algorithm to solve the discrete logarithm problem in finite fields of small characteristic. However, heuristic approaches have led to much more efficient algorithms. In fact, faster heuristic algorithms were already known at the time of Pomerance's work: Coppersmith proposed a heuristic algorithm [Cop84] of complexity $L(1/3)$ as early as 1984. Numerous improvements followed, notably including the function field sieve [AH99], yet the complexities remained in $L(1/3)$ for decades. That is until 2013, when it was reduced to a heuristic $L(1/4 + o(1))$ by Joux [Jou13], quickly followed by a heuristic quasi-polynomial time algorithm [BGJT14] for fields of fixed characteristic, of expected running time $b^{O(\log b)}$, where b is the bit-size of the cardinality of the finite field.

This section reviews the ideas of [BGJT14], which set the current bar for the heuristic complexity of the discrete logarithm problem in finite fields of small characteristic. Instead of presenting the exact same algorithm as described in [BGJT14], we focus on the descent procedure, which is sufficient to deduce a full discrete logarithm algorithm thanks to Theorem 1.4. This approach has two advantages. First, it simplifies the presentation, allowing to focus on the core ideas leading to the quasi-polynomial complexity. Second, it allows to effectively reduce the number of heuristics, by obviating the need for [BGJT14, Heuristic 8]. A practitioner may not appreciate this approach as much: the algorithm built from Theorem 1.4 performs multiple descents, while [BGJT14] requires only one (for the individual logarithm phase), and computes the logarithms of the factor base in polynomial time. An orthogonal approach is taken in [Pie16], which focusses on computing as fast as possible the logarithms of factor base elements.

1.5.1. Constructing smooth polynomials. To generate relations between polynomials of the factor base, Hellman-Reyneri, as well as most of its successors for decades, generates "easy" relations between random (or random looking) polynomials of a rather large degree until, by chance, these polynomials split into sufficiently small irreducibles. This paradigm led to algorithms of complexity $L(1/3)$, first reached in [Cop84]. To break this complexity barrier, a new approach was necessary. Instead of relying on the (very low) probability of random polynomials of large degree to be smooth, one could construct large degree polynomials in a way that ensures their smoothness. This idea first appeared in [GGMZ13], yet that algorithm was still in $L(1/3)$.

Consider a finite field $\mathbf{F}_q$. The key to the construction of smooth, large degree polynomials is the identity

$$x^q - x = \prod_{\alpha\in\mathbf{F}_q} (x - \alpha).$$

It leads to a whole family of identities, as any polynomial or rational fraction can be substituted for x. Given two non-zero polynomials F and G with coefficients in the

algebraic closure of $\mathbf{F}_q$, substituting F/G for x leads to the identity

$$F(x)^q G(x) - F(x)G(x)^q = G(x) \prod_{\alpha \in \mathbf{F}_q} (F(x) - \alpha G(x)).$$

Although $F^q G - F G^q$ has a rather large degree, it is guaranteed to split into polynomials of degrees at most $d = \max(\deg F, \deg G)$. To construct a relation involving this polynomial, observe that $F^q G - F G^q = F^{(q)}(x^q)G(x) - F(x)G^{(q)}(x^q)$, where $F^{(q)}$ and $G^{(q)}$ are respectively F and G with coefficients raised to the power q. Now, suppose we want to compute logarithms in a field $\mathbf{F}_{q^\ell}$ represented as $\mathbf{F}_q[x]/(I)$, for some irreducible polynomial I. Let h be the reduction of x^q modulo I. We get a relation of the form

$$F^{(q)}(h(x))G(x) - F(x)G^{(q)}(h(x)) \equiv G(x) \prod_{\alpha \in \mathbf{F}_q} (F(x) - \alpha G(x)) \mod I. \tag{1.4}$$

The polynomial on the right-hand side is d-smooth. The left-hand side does not seem particularly smooth, but observe that it has degree at most $d(\deg h + 1)$. When h has a small degree, this polynomial has good chances to also be d-smooth. Luckily, it is easy to construct a representation of $\mathbf{F}_{q^\ell}$ with this property, following an idea that dates back to [Cop84]: generate random small degree polynomials $h \in \mathbf{F}_q[x]$ until $x^q - h$ has an irreducible factor I of degree ℓ. Then, $\mathbf{F}_{q^\ell} \cong \mathbf{F}_q[x]/(I)$, and $x^q \equiv h \mod I$.

With such a field representation, it is not hard to see how to construct a large number of relations of the form (1.4) between low degree polynomials, defined over a small extension of $\mathbf{F}_q$ (pick at random such polynomials F and G, and keep the relations for which the left-hand side is smooth). And this indeed leads to a (heuristic) polynomial time algorithm for computing the logarithms of elements represented by small degree polynomials. However, we are mostly interested here in constructing a descent algorithm, whose input is usually a polynomial of large degree. The key innovation of [BGJT14] is to use relations of the form (1.4) involving the input polynomial and polynomials of half the degree, resulting in a "degree halving" procedure. This procedure can then be used recursively until all the polynomials involved have a very small degree.

1.5.2. A special field representation. Before exploring in more details the degree halving and the descent, we need to settle on an appropriate field representation, which allows to construct interesting relations of the form (1.4). We consider the discrete logarithm problem over a finite field k, and we first require this field to be of a particular form. We will see later, in Section 1.5.4, how to extend the algorithm to the general case.

Definition 1.6 (Sparse medium subfield representation)**.** Suppose that

(1) the field k has a subfield of q^2 elements for some prime power q, i.e., k is isomorphic to $\mathbf{F}_{q^{2\ell}}$ with $\ell \geq 1$, and
(2) there exist two polynomials h_0 and h_1 over $\mathbf{F}_{q^2}$ of small degree, such that $h_1 x^q - h_0$ has a degree ℓ irreducible factor $I(x)$.

Then, the quotient $\mathbf{F}_{q^2}[x]/(I)$ is a *sparse medium subfield representation* of k.

Here comes already the first obstacle to a rigorous algorithm. We wish that any field of the form $\mathbf{F}_{q^{2\ell}}$ with $\ell \leq q + 2$ has a sparse medium subfield representation. And this is indeed believable, as such representations are very easy to find in practice, yet there is no proof to this day that they always exist.

Heuristic 1.7. *Any field of the form $\mathbf{F}_{q^{2\ell}}$ with $\ell \leq q + 2$ has a sparse medium subfield representation (where these q and ℓ implicitly play the same role as in Definition 1.6), with h_0 and h_1 of degrees at most* 2.

To get an algorithm of heuristic quasi-polynomial time complexity, this bound of 2 on the degrees of h_0 and h_1 could harmlessly be replaced by any other constant. Given such a representation for $\mathbf{F}_{q^{2\ell}}$, we adopt the model $\mathbf{F}_{q^{2\ell}} = \mathbf{F}_{q^2}[x]/(I)$.

1.5.3. The descent. The descent consists in recursively applying a degree halving procedure on the polynomials of $\mathbf{F}_{q^2}[x]$ (representing elements of $\mathbf{F}_{q^{2\ell}}$), until all the polynomials involved are linear. This degree halving is the essential building block, and its properties are made precise in the following Proposition 1.8.

Proposition 1.8 (Degree halving)**.** *Let $k = \mathbf{F}_{q^{2\ell}}$ be a finite field with a sparse medium subfield representation. Under the heuristic assumption made precise in Heuristic 1.9 below, there exists an algorithm with complexity polynomial in q and ℓ which solves the following task. Given an element of k represented by a polynomial $f \in \mathbf{F}_{q^2}[x]$ with $2 \leq \deg f \leq \ell - 1$, the algorithm returns an expression of $\log f$ as a linear combination of $\log h_1$ and at most $O(\ell q^2)$ logarithms $\log f_i$ with $\deg f_i \leq \lceil \deg(f)/2 \rceil$.*

It allows us to define the factor base as

$$\mathfrak{F} = \{f \in \mathbf{F}_{q^2}[x] \mid \deg(f) \leq 1, f \neq 0\} \cup \{h_1\}.$$

The descent to $\mathfrak{F}$ goes as follows. Let f be a polynomial in $\mathbf{F}_{q^2}[x]$ of degree at most $\ell - 1$. Applying the algorithm of Proposition 1.8 to f yields a relation of the form

$$\log(f) = e_0 \log(h_1) + \sum_i e_i \log(f_i),$$

where the sum has at most $O(q^2\ell)$ terms, and the polynomials f_i have degrees at most $\lceil \deg(f)/2 \rceil$. By recursively applying that algorithm to the polynomials f_i, one builds a tree rooted at f, where the children of any node are the resulting f_i-values, and the leaves are linear polynomials over $\mathbf{F}_{q^2}$. The logarithm of each of the nodes of the tree can then be computed as a linear combination of its children and $\log h_1$. Therefore $\log(f)$ can be expressed as a linear combination of logarithms of the factor base: the descent is complete.

The arity of the tree is $O(q^2\ell)$, and its depth is $O(\log \ell)$. Therefore it has $(q^2\ell)^{O(\log \ell)}$ nodes, and since any polynomial in q and ℓ is absorbed in the O in the exponent, we obtain a running time bounded by $\max(q, \ell)^{O(\log \ell)}$ for the descent.

Proof of Proposition 1.8. Let $f \in \mathbf{F}_{q^2}[x]$ be a polynomial of degree at most $\ell - 1$. As discussed in Section 1.5.1, for any polynomials F and G, we get a relation of the form (1.4), which with the congruence $x^q \equiv h_0/h_1 \mod I$ becomes

$$F^{(q)}\left(\frac{h_0}{h_1}\right) G(x) - F(x) G^{(q)}\left(\frac{h_0}{h_1}\right) \equiv G(x) \prod_{\alpha \in \mathbf{F}_q} (F(x) - \alpha G(x)) \mod I. \tag{1.5}$$

The left-hand side is a rational function, whose denominator is a power of h_1. We would like this multiplicative relation to involve f, and polynomials of degrees at most $\lceil \deg(f)/2 \rceil$. As a first try, we could simply let $F = f$ and $G = 1$. The numerator of the left-hand side is of degree at most $2\deg(f)$, and assuming it behaves as a random polynomial of this size, it has a constant probability of being $\lceil \deg(f)/2 \rceil$-smooth. The right-hand side is the product of the polynomials $f - \alpha$ for all α in $\mathbf{F}_q$. The good news is that it involves f. The bad news is that it involves a lot of other polynomials of the same degree (instead of half the degree). The trick is to generate a lot more of these relations, and then use some linear algebra to eliminate all the factors $f - \alpha$, for $\alpha \neq 0$.

We cannot get more of these relations if we insist on keeping these α-values in $\mathbf{F}_q$. However, we can generate a plethora of relations involving the linear polynomials $f - \alpha$

for α in $\mathbf{F}_{q^2}$. Consider any four coefficients $a, b, c, d \in \mathbf{F}_{q^2}$, and substitute F for $af + b$ and G for $cf + d$ in Relation (1.5). The right-hand side becomes

$$(cf + d) \prod_{\alpha \in \mathbf{F}_q} ((af + b) - \alpha(cf + d)),$$

which factors as a product of polynomials $f - \alpha$ for α in $\mathbf{F}_{q^2}$, up to a scalar in $\mathbf{F}_{q^2}$. It induces a vector $v = (v_\alpha)_{\alpha \in \mathbf{F}_{q^2}}$ where v_α is the valuation of this expression at $x - \alpha$. The left-hand side reads

$$\left(a^q f^{(q)}\left(\frac{h_0}{h_1}\right) + b^q\right)(cf + d) - (af + b)\left(c^q f^{(q)}\left(\frac{h_0}{h_1}\right) + d^q\right),$$

and its numerator has degree at most $3\deg(f)$. Whenever it is $\lceil \deg(f)/2 \rceil$-smooth, we say that a, b, c, d yield a relation, and we add the vector v as a new row of a large matrix $H(f)$. Once sufficiently many relations have been found, the matrix $H(f)$ should have full-rank, so some simple linear algebra allows to eliminate all the factors $f - \alpha$ for $\alpha \neq 0$, resulting in a relation between f and a $\lceil \deg(f)/2 \rceil$-smooth polynomial (and h_1, which systematically appears in the denominator of the left-hand side), with at most $O(q^2 \deg(f))$ irreducible factors. This describes the degree-halving procedure.

A question remains: is there a good reason to believe that choosing a, b, c and d in $\mathbf{F}_{q^2}$ leads to sufficiently many relations to construct a full rank matrix $H(f)$? It is important to note that a lot of these relations are trivial, or redundant. Consider these coefficients as a matrix

$$m = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

It is easy to see that when m is not invertible, the resulting relation is trivial: both sides are zero. It is also clear that the relations we get from m and from γm are the same for any $\gamma \in \mathbf{F}_{q^2}$. Therefore the interesting relations arise from invertible matrices up to a scalar, in other words, from $\mathrm{PGL}_2(\mathbf{F}_{q^2})$. Now, considering the usual action of PGL_2 on the projective line $\mathbf{P}^1$, it appears that the right-hand side can be rewritten as

$$(cf + d) \prod_{\alpha \in \mathbf{F}_q} ((af + b) - \alpha(cf + d)) = \prod_{(\alpha:\beta) \in m^{-1}\mathbf{P}^1(\mathbf{F}_q)} (\beta f - \alpha),$$

for some appropriate choice of representatives for the points $(\alpha : \beta)$ of $\mathbf{P}^1(\mathbf{F}_{q^2})$. Under this form, it becomes clear that two matrices m and $\tilde{m}$ in PGL_2 give the same relation if and only if $m^{-1}\mathbf{P}^1(\mathbf{F}_q) = \tilde{m}^{-1}\mathbf{P}^1(\mathbf{F}_q)$, meaning that $\tilde{m}m^{-1} \in \mathrm{PGL}_2(\mathbf{F}_q)$. Therefore we should restrict to a single matrix for each coset of

$$\mathrm{PGL}_2(\mathbf{F}_q) \backslash \mathrm{PGL}_2(\mathbf{F}_{q^2}).$$

As a result, we get only $q^3 + q$ potential relations. Recall that we only get a useful relation when the numerator of the left-hand side is $\lceil \deg(f)/2 \rceil$-smooth. Assuming this numerator behaves like a random polynomial of degree at most $3\deg(f)$, we should still get a total of $\Theta(q^3)$ relations. Considering that $H(f)$ has q^2 columns, it seems like $\Theta(q^3)$ rows is plenty enough to ensure $H(f)$ has full rank. As often with questions involving smoothness of "random looking" polynomials, and ranks of "random looking" matrices, a rigorous answer seems out of reach.

Heuristic 1.9. *For any polynomial f, the matrix $H(f)$ obtained after processing all the $q^3 + q$ cosets of $\mathrm{PGL}_2(\mathbf{F}_q) \backslash \mathrm{PGL}_2(\mathbf{F}_{q^2})$ has full rank q^2.*

Under this heuristic assumption, the degree halving procedure succeeds in polynomial time, which concludes the proof of Proposition 1.8. □

Remark 1.10. The authors of [BGJT14] justify this Heuristic 1.9 by showing that the matrix $\mathcal{H}$ obtained from the q^3+q cosets of $\mathrm{PGL}_2(\mathbf{F}_q)\backslash\mathrm{PGL}_2(\mathbf{F}_{q^2})$, without restriction on the smoothness of the left-hand sides, has full rank q^2. A random submatrix $H(f)$ containing $\Theta(q^3)$ rows (assuming we are lucky enough with questions of smoothness), should have full rank with overwhelming probability.

1.5.4. Heuristic quasi-polynomial complexity. Consider the discrete logarithm problem in $\mathbf{F}_{p^m}$, where p is the characteristic of the field, and suppose $p = L_{p^m}(\alpha)$, for some α in the range $[0,1]$. If $\mathbf{F}_{p^m}$ is not itself of a suitable form, one can construct an extension that has a sparse medium subfield representation as follows. Let ℓ be m if m is odd, and $m/2$ if m is even. Then, let $q = p^{\lceil \log_p \ell \rceil}$, and work in $\mathbf{F}_{q^{2\ell}}$, which is an extension of $\mathbf{F}_{p^m}$. This field $\mathbf{F}_{q^{2\ell}}$ is of the appropriate form, and satisfies $\ell = p^{\log_p(\ell)} \leq q$ so we can assume it has a sparse medium subfield representation. As discussed in Section 1.5.3, the descent in $\mathbf{F}_{q^{2\ell}}$ (and therefore the discrete logarithm algorithm, thanks to Theorem 1.4) has complexity

$$\max(q,\ell)^{O(\log \ell)} = q^{O(\log m)} = \max(p,m)^{O(\log m)}.$$

Since $m = L_{p^m}(0)$, the complexity becomes

$$L_{p^m}(\alpha)^{O(\log\log p^m)}.$$

If $\alpha = 0$, meaning that p is polynomial in the bit-length of the cardinality of the field, then the complexity is of the form $e^{O((\log\log p^m)^2)}$, which is a quasi-polynomial quantity in the bit length $\log p^m$ of the size of the field. In particular, the discrete logarithm problem in $\mathbf{F}_{2^m}$ can be solved in time $e^{O((\log m)^2)}$. Also, observe that $L_{p^m}(\alpha)^{O(\log\log p^m)}$ is smaller than $L_{p^m}(\alpha')$ for any $\alpha' > \alpha$. Therefore, for any $\alpha < 1/3$, the algorithm is faster than any previously known algorithm.

2

The powers of 2 descent method

Abstract. This chapter is based on a joint work with Thorsten Kleinjung, presented at ANTS-XIII, Thirteenth Algorithmic Number Theory Symposium, as

[KW18] T. Kleinjung and B. Wesolowski, *A new perspective on the powers of two descent for discrete logarithms in finite fields*, Thirteenth Algorithmic Number Theory Symposium – ANTS-XIII, 2018, proceedings to appear in the Open Book Series, Mathematical Sciences Publishers.

Original abstract. A new proof is given for the correctness of the powers of 2 descent method for computing discrete logarithms. The result is slightly stronger than the original work, but more importantly we provide a unified geometric argument, eliminating the need to analyse all possible subgroups of $\mathrm{PGL}_2(\mathbf{F}_q)$. Our approach sheds new light on the role of PGL_2, in the hope to eventually lead to a complete proof that discrete logarithms can be computed in quasi-polynomial time in finite fields of fixed characteristic.

2.1. Towards a provable quasi-polynomial time algorithm

The discrete logarithm problem in finite fields of small characteristic finds itself in an uncomfortable situation: a large gap separates what is provably feasible (an algorithm of complexity $L(1/2)$) and what seems to be feasible (a heuristic algorithm of quasi-polynomial complexity). Soon after the first heuristic quasi-polynomial algorithm was introduced, a second one was proposed in [GKZ18] with the promise to get a bit closer to a provable algorithm. The authors of [GKZ18] provide a rigorous analysis under the sole assumption that the field admits a suitable representation. This chapter explores this algorithm through a new proof of the following theorem.

Theorem 2.1. *Given a prime power q, a positive integer d, coprime polynomials h_0 and h_1 in $\mathbf{F}_{q^d}[x]$ of degree at most 2, and an irreducible degree ℓ factor I of $h_1x^q - h_0$, the discrete logarithm problem in $\mathbf{F}_{q^{d\ell}} \cong \mathbf{F}_{q^d}[x]/(I)$ can be solved in expected time $q^{\log_2 \ell + O(d)}$.*

The integers q, d and ℓ, and the polynomials h_0, h_1 and I are defined as in the above theorem for the rest of the chapter. It was originally proven in [GKZ18] when $q > 61$, q is not a power of 4, and $d \geq 18$. Even though we eliminate these technical conditions, the main contribution is the new approach to the proof — more geometric, and, hopefully, more insightful. The obstacle separating Theorem 2.1 from a fully provable algorithm for the discrete logarithm problem is the question of the existence of a good field representation: polynomials h_0, h_1 and I for a small d. A direction towards a fully provable

algorithm would be to find analogues of this theorem for other field representations, but this may require in the first place a good understanding of why Theorem 2.1 is true.

That result rests on two ideas. The first was discussed in Section 1.4: to build a full, rigorous index calculus algorithm, it is sufficient to design a rigorous *descent* algorithm — an algorithm which rewrites an arbitrary element of the group as a product of elements of the factor base. The second observation, new in [GKZ18], is that to build a descent algorithm, it is sufficient to design a *degree 2 elimination* algorithm — an algorithm which rewrites an irreducible polynomial in $\mathbf{F}_{q^d}[x]$ of degree $2m$ as an equivalent product of irreducible polynomials of degrees dividing m. This degree 2 elimination is the true core of the result, and there resides the main difficulty. We present it in more detail in Section 2.1.1, before describing precisely how it leads, thanks to the above ideas, to a full index calculus algorithm in Section 2.1.2. The rest of the chapter is dedicated to the rigorous analysis of the degree 2 elimination algorithm.

2.1.1. Degree 2 elimination. Proposition 2.3 below essentially states that elements of $\mathbf{F}_{q^{d\ell}}$ represented by a *good* irreducible polynomial in $\mathbf{F}_{q^d}[x]$ of degree $2m$ can be rewritten as a product of *good* irreducible polynomials of degrees dividing m. This process, the degree 2 elimination, was first introduced for $m = 1$ in [GGMZ13] and generalised in [GKZ18].

Definition 2.2 (Traps and good polynomials)**.** An element $\tau \in \overline{\mathbf{F}}_q$ for which $[\mathbf{F}_{q^d}(\tau) : \mathbf{F}_{q^d}]$ is an even number $2m$ and $h_1(\tau) \neq 0$ is called

(1) a *degenerate trap root* if $\frac{h_0}{h_1}(\tau) \in \mathbf{F}_{q^{dm}}$,
(2) a *trap root of level* 0 if it is a root of $h_1 x^q - h_0$, or
(3) a *trap root of level dm* if it is a root of $h_1 x^{q^{dm+1}} - h_0$.

Analogously, a polynomial in $\overline{\mathbf{F}}_q[x]$ that has a trap root is called a *trap*. A polynomial is *good* if it is not a trap.

Proposition 2.3 (Degree 2 elimination)**.** *Given an extension $k/\mathbf{F}_{q^d}$ of degree m such that $dm \geq 23$, and a good irreducible quadratic polynomial $Q \in k[x]$, there is an algorithm which finds a list of good linear polynomials $(L_0, \ldots, L_n)$ in $k[x]$ such that $n \leq q+1$ and*

$$Q \equiv h_1 L_0^{-1} \cdot \prod_{i=1}^{n} L_i \mod I,$$

and that runs in expected polynomial time in q, d and m.

The main contribution of this chapter is a new proof of Proposition 2.3, which hopefully provides a better understanding of the degree 2 elimination method, the underlying geometry, and the role of traps. The action of PGL_2 on the polynomial $x^q - x$ became a crucial ingredient in the recent progress on the discrete logarithm problem for fields of small characteristic, since [Jou13] (and implicitly in [GGMZ13]). While the proof in [GKZ18] resorted to an intricate case by case analysis enumerating all possible subgroups of $\mathrm{PGL}_2(\mathbf{F}_q)$, we provide a unified geometric argument, shedding new light on the role of PGL_2.

Overview of the algorithm. Let Q be as in Proposition 2.3. The key observation allowing degree 2 elimination is that a polynomial of the form $\alpha x^{q+1} + \beta x^q + \gamma x + \delta$ has a high chance to split completely over its field of definition. Furthermore, we have the congruence

$$\alpha x^{q+1} + \beta x^q + \gamma x + \delta \equiv h_1^{-1}(\alpha x h_0 + \beta h_0 + \gamma x h_1 + \delta h_1) \mod I, \tag{2.1}$$

and the numerator of the right-hand side has degree at most 3. Consider the $\overline{\mathbf{F}}_q$-vector space V spanned by x^{q+1}, x^q, x and 1 in $\overline{\mathbf{F}}_q[x]$, and the linear subspace

$$V_Q = \{\alpha x^{q+1} + \beta x^q + \gamma x + \delta \in V \mid \alpha x h_0 + \beta h_0 + \gamma x h_1 + \delta h_1 \equiv 0 \mod Q\}. \tag{2.2}$$

As long as Q is a good irreducible polynomial, V_Q is of dimension two. The algorithm simply consists in sampling uniformly at random elements $f \in V_Q(k)$ (or equivalently in its projectivisation $\mathbf{P}^1_Q(k)$) until f splits completely over k into good linear polynomials $(L_1, \dots, L_{\deg f})$. Since $f \in V_Q$, the polynomial Q divides the numerator of the right-hand side of (2.1), and the quotient is a polynomial L_0 of degree at most 1. The algorithm returns $(L_0, \dots, L_{\deg f})$. This procedure is summarised in Algorithm 2.1.

Algorithm 2.1 Degree 2 elimination

Require: An extension $k/\mathbf{F}_{q^d}$ of degree m such that $dm \geq 23$, and a good irreducible quadratic polynomial $Q \in k[x]$.
Ensure: A list of good linear polynomials $(L_0, \dots, L_n)$ in $k[x]$ such that $n \leq q+1$ and $Q \equiv h_1 L_0^{-1} \cdot \prod_{i=1}^n L_i \mod I$.
1: Let $V(k)$ be the k-vector space spanned by x^{q+1}, x^q, x, and 1 in $k[x]$;
2: Let $V_Q(k) \subset V(k)$ be the linear subspace defined in Equation (2.2);
3: **repeat**
4: Choose $f = \alpha x^{q+1} + \beta x^q + \gamma x + \delta$ uniformly at random in $V_Q(k)$;
5: Let $\prod_{i=1}^m L_i$ be the factorisation of f into irreducible polynomials of $k[x]$;
6: **until** $(L_1, \dots, L_m)$ is a list of good linear polynomials in $k[x]$;
7: $L_0 \leftarrow (\alpha x h_0 + \beta h_0 + \gamma x h_1 + \delta h_1)/Q$;
8: **return** $(L_0, \dots, L_m)$.

To prove that the algorithm terminates in expected polynomial time, we need to show that a random polynomial in $V_Q(k)$ has good chances to split into good linear polynomials over k. We prove this by constructing a morphism $C \to \mathbf{P}^1_Q$ where C is an absolutely irreducible curve defined over k, such that the image of any k-rational point of C is a polynomial that splits completely over k. This construction is the object of Section 2.4. The absolute irreducibility implies that C has a lot of k-rational points, allowing us to deduce that a lot of polynomials in $\mathbf{P}^1_Q(k)$ split over k. This is done in Section 2.5.

2.1.2. The zigzag descent. We explain in this section how the degree 2 elimination (Proposition 2.3) allows to construct a full discrete logarithm algorithm, resulting in Theorem 2.1. From Theorem 1.4, it is sufficient to construct a descent algorithm. Consider the factor base

$$\mathfrak{F} = \{f \in \mathbf{F}_{q^d}[x] \mid \deg f \leq 1, f \neq 0\} \cup \{h_1\}.$$

The following proposition extends the degree 2 elimination to a full descent algorithm from any polynomial down to the factor base.

Proposition 2.4. *Suppose $d \geq 23$. Given a polynomial $F \in \mathbf{F}_{q^d}[x]$, there is an algorithm that finds integers $(e_f)_{f \in \mathfrak{F}}$ such that*

$$F \equiv \prod_{f \in \mathfrak{F}} f^{e_f} \mod I,$$

and that runs in expected time $q^{\log_2 \ell + O(d)}$.

Proof. This is essentially the *zigzag* descent presented in [GKZ18]. First, one finds a good irreducible polynomial $G \in \mathbf{F}_{q^d}[x]$ of degree 2^e such that $F \equiv G \mod I$ (this can be done for $e = \lceil \log_2(4\ell + 1) \rceil$, see [Wan97, Theorem 5.1] and [GKZ18, Lemma 2]). Over the extension $\mathbf{F}_{q^{d2^{e-1}}}$, the polynomial G splits into 2^{e-1} good irreducible quadratic polynomials, all conjugate under $\mathrm{Gal}(\mathbf{F}_{q^{d2^{e-1}}}/\mathbf{F}_{q^d})$. Let Q be one of them, and apply the algorithm of Proposition 2.3 to rewrite Q in terms of linear polynomials $(L_0, \ldots, L_n)$ in $\mathbf{F}_{q^{d2^{e-1}}}[x]$ and h_1. For any index i, let $\tilde{L}_i$ be the product of all the conjugates of L_i in the extension $\mathbf{F}_{q^{d2^{e-1}}}/\mathbf{F}_{q^d}$. Then,

$$F \equiv h_1^{2^{e-1}} \tilde{L}_0^{-1} \cdot \prod_{i=1}^{n} \tilde{L}_i \mod I,$$

and each $\tilde{L}_i$ factors into good irreducible polynomials of degree a power of 2 at most 2^{e-1}. The descent proceeds by iteratively applying this method to each $\tilde{L}_i$ until all the factors are in the factor base $\mathfrak{F}$. □

Proof of Theorem 2.1. Proposition 2.4 above, together with Theorem 1.4, imply Theorem 2.1 for any $d \geq 23$. To remove this constraint on d, suppose that $d \leq 22$, and let $d' \leq 44$ be the smallest multiple of d larger than 22. Let I' be an irreducible factor of I in $\mathbf{F}_{q^{d'}}[x]$. The discrete logarithm problem can be solved in expected time

$$q^{\log_2(\deg I') + O(d')} = q^{\log_2 \ell + O(1)}$$

in the field $\mathbf{F}_{q^{d'}}[x]/(I')$, and therefore also in the subfield $\mathbf{F}_{q^d}[x]/(I)$. □

2.2. The action of PGL_2 on $x^q - x$

As already mentioned, the crucial reason why degree 2 elimination works is that a polynomial of the form $\alpha x^{q+1} + \beta x^q + \gamma x + \delta$ has a high chance to split completely over its field of definition. This fact is closely related to the action of 2×2 matrices on such polynomials.

Definition 2.5. We denote by $\star$ the action of invertible 2×2 matrices on univariate polynomials defined as follows:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \star f(x) = (cx + d)^{\deg f} f\left(\frac{ax + b}{cx + d}\right).$$

Consider the $\overline{\mathbf{F}}_q$-vector subspace V spanned by x^{q+1}, x^q, x, and 1 in $\overline{\mathbf{F}}_q[x]$. The above action induces an action of the group PGL_2 on the projective space $\mathbf{P}(V)$, which we also write $\star$. Parameterizing the polynomials in $\mathbf{P}(V)$ as $\alpha x^{q+1} + \beta x^q + \gamma x + \delta$, let S be the quadratic surface in $\mathbf{P}(V)$ defined by the equation $\alpha\delta = \beta\gamma$. This surface is the image of the morphism

$$\psi : \mathbf{P}^1 \times \mathbf{P}^1 \longrightarrow \mathbf{P}(V) : (a, b) \longmapsto (x - a)(x - b)^q.$$

Note that to avoid heavy notation, everything is written affinely, but we naturally have $\psi(\infty, b) = (x - b)^q$, $\psi(a, \infty) = x - a$ and $\psi(\infty, \infty) = 1$. More generally, we say that $f(x) \in V$ has a root of degree n at infinity if f is of degree $q + 1 - n$. Now, the following lemma shows that apart from the surface S, the polynomials in $\mathbf{P}(V)$ form exactly one orbit for PGL_2.

Lemma 2.6. *We have* $\mathbf{P}(V) \setminus S = \mathrm{PGL}_2 \star (x^q - x)$.

Proof. First notice that both S and $\mathbf{P}(V) \setminus S$ are closed under the action of PGL_2. In particular, $\mathrm{PGL}_2 \star (x^q - x) \subseteq \mathbf{P}(V) \setminus S$. Let $f(x) \in \mathbf{P}(V) \setminus S$. Suppose by contradiction that $f(x)$ has a double root $r \in \mathbf{P}^1$, and let $g \in \mathrm{PGL}_2$ be a linear transformation sending 0 to r. The polynomial $g \star f(x)$ has a double root at 0, so has no constant or linear term, and must be of the form $\alpha x^{q+1} + \beta x^q$, so it is in S, a contradiction. Therefore $f(x)$ has $q+1$ distinct roots. Let $g \in \mathrm{PGL}_2$ send 0, 1 and ∞ to three of these roots. Then, $g \star f(x)$ has a root at 0 and at ∞ so is of the form $\beta x^q + \gamma x$, and since it also has a root at 1, it can only be $x^q - x$. □

This result implies that most polynomials in $\mathbf{P}(V)$ are of the form $g \star (x^q - x)$, and thus split completely over the field of definition of the matrix g.

2.3. The role of traps

Consider a finite field extension $k/\mathbf{F}_{q^d}$ of degree m. Let Q be an irreducible quadratic polynomial in $k[x]$ coprime to h_1. Let a_1 and a_2 be the roots of Q in $\overline{\mathbf{F}}_q$. The degree 2 elimination aims at expressing Q modulo $h_1 x^q - h_0$ as a product of linear polynomials. To do so, we study a variety $\mathbf{P}^1_Q \subset \mathbf{P}(V)$ parameterizing polynomials that can possibly lead to an elimination of Q (i.e., such that Q divides the right-hand side of (2.1)). In this section, we define $\mathbf{P}^1_Q$ and show how the notions of traps and good polynomials determine how it intersects the surface S from Lemma 2.6.

Recall that V is the $\overline{\mathbf{F}}_q$-vector subspace spanned by x^{q+1}, x^q, x, and 1 in $\overline{\mathbf{F}}_q[x]$. Consider the linear map

$$\varphi : V \longrightarrow \overline{\mathbf{F}}_q[x][h_1^{-1}] : \begin{cases} 1 & \longmapsto 1, \\ x & \longmapsto x, \\ x^q & \longmapsto h_0/h_1, \\ x^{q+1} & \longmapsto x h_0/h_1. \end{cases} \tag{2.3}$$

We want $\mathbf{P}^1_Q$ to parameterise the polynomials $f \in V$ such that $\varphi(f)$ is divisible by Q. For any $P \in \overline{\mathbf{F}}_q[x]$ coprime with h_1, write $\varphi_P = \pi_P \circ \varphi$ where $\pi_P : \overline{\mathbf{F}}_q[x][h_1^{-1}] \to \overline{\mathbf{F}}_q[x]/P$ is the canonical projection. We can now define $\mathbf{P}^1_Q$ as

$$\mathbf{P}^1_Q = \mathbf{P}(\ker \varphi_Q). \tag{2.4}$$

The variety $\mathbf{P}^1_Q$ is the intersection of the two planes $\mathbf{P}(\ker \varphi_{x-a_1})$ and $\mathbf{P}(\ker \varphi_{x-a_2})$.

Lemma 2.7. *If Q is not a degenerate trap, then $|(\mathbf{P}^1_Q \cap S)(\overline{\mathbf{F}}_q)| = 2$, and these two points are of the form $\psi(a_1, b_1)$ and $\psi(a_2, b_2)$, with $a_1 \neq a_2$ and $b_1 \neq b_2$.*

Proof. For $a \in \{a_1, a_2\}$, we have

$$\mathbf{P}(\ker \varphi_{x-a}) \cap S = \psi\left(\{a\} \times \mathbf{P}^1\right) \cup \psi\left(\mathbf{P}^1 \times \left\{\frac{h_0}{h_1}(a)^{1/q}\right\}\right).$$

Since the polynomial Q is irreducible, we have $a_1 \neq a_2$. Furthermore, assuming that Q is not a degenerate trap, we have $\frac{h_0}{h_1}(a_1) \notin k$, and thereby $\frac{h_0}{h_1}(a_1) \neq \frac{h_0}{h_1}(a_2)$. Therefore the intersection $\mathbf{P}^1_Q \cap S$ is equal to

$$\mathbf{P}(\ker \varphi_{x-a_1}) \cap \mathbf{P}(\ker \varphi_{x-a_2}) \cap S = \left\{\psi\left(a_1, \frac{h_0}{h_1}(a_2)^{1/q}\right), \psi\left(a_2, \frac{h_0}{h_1}(a_1)^{1/q}\right)\right\}.$$

□

In particular, when Q is not a degenerate trap, $\mathbf{P}^1_Q$ is exactly the line passing through the two points $s_1 = \psi(a_1, b_1)$ and $s_2 = \psi(a_2, b_2)$. We get a k-isomorphism $\mathbf{P}^1 \to \mathbf{P}^1_Q : \alpha \mapsto s_1 - \alpha s_2$. For this reason the two points s_1 and s_2 play a central role in the rest of the analysis, and the following proposition shows that they behave nicely when Q is a good polynomial.

Proposition 2.8. *Suppose Q is a good polynomial. Then, $(\mathbf{P}^1_Q \cap S)(\overline{\mathbf{F}}_q) = \{s_1, s_2\}$, where $s_1 = (x - a_1)(x - b_1)^q$, and $s_2 = (x - a_2)(x - b_2)^q$, and the roots a_1, a_2, b_1 and b_2 are all distinct.*

Proof. From Lemma 2.7, we can write $(\mathbf{P}^1_Q \cap S)(\overline{\mathbf{F}}_q) = \{s_1, s_2\}$ with $a_1 \neq a_2$ and $b_1 \neq b_2$. If $a_1 = b_2$ or $a_2 = b_1$, then Q divides $x^q h_1 - h_0$, a trap of level 0. Now, suppose $a_1 = b_1$ (the case $a_2 = b_2$ is similar). Since a_1 and a_2 are the two roots of Q, and Q divides $(x - a_1)(h_0 - a_1^q h_1)$, then a_2 is a root of $h_0 - a_1^q h_1$. We get that $h_0(a_2) = a_1^q h_1(a_2)$, so a_2 is a root of $h_1 x^{q^{dm+1}} - h_0$, a trap of level dm. □

2.4. Irreducible covers of $\mathbf{P}^1_Q$

In this section we suppose that Q is a good polynomial, and we consider the polynomials $s_1 = (x - a_1)(x - b_1)^q$ and $s_2 = (x - a_2)(x - b_2)^q$ as defined in Proposition 2.8, where a_1, a_2, b_1 and b_2 are all distinct. Consider the variety $\mathbf{P}^1_Q$ from (2.4).

Recall that our goal is to prove that a significant proportion of the polynomials of $\mathbf{P}^1_Q(k)$ splits completely over k. As mentioned in Section 2.1.1, our method consists in constructing a morphism $C \to \mathbf{P}^1_Q$ where C is an absolutely irreducible curve defined over k, such that the image of any k-rational point of C is a polynomial that splits completely over k. The absolute irreducibility is crucial as it implies that C has a lot of k-rational points. The idea is to consider the algebraic set

$$C = \{(u, r_1, r_2, r_3) \mid \text{the } r_i\text{-values are three distinct roots of } u\} \subset \mathbf{P}^1_Q \times \mathbf{P}^1 \times \mathbf{P}^1 \times \mathbf{P}^1,$$

and the canonical projection $C \to \mathbf{P}^1_Q$.

Proposition 2.9. *If $(u, r_1, r_2, r_3) \in C(k)$, then u splits completely over k.*

Proof. Suppose that (u, r_1, r_2, r_3) is a k-rational point of C. From Lemma 2.6, we get $u = g \star (x^q - x)$ where g is the matrix $g \in \mathrm{PGL}_2(k)$ sending the three points r_1, r_2 and r_3 to 0, 1 and ∞. In particular, the set of roots of u is $g^{-1}(\mathbf{P}^1(\mathbf{F}_q))$, a subset of $\mathbf{P}^1(k)$. □

In the rest of this section, we prove that C is absolutely irreducible (Proposition 2.14). The strategy is the following. Instead of considering C directly, which encodes three roots for each polynomial of $\mathbf{P}^1_Q$, we start with the variety

$$X = \{(u, r) \mid u(r) = 0\} \subset \mathbf{P}^1_Q \times \mathbf{P}^1,$$

where each point encodes a single root. We can then "add" roots by considering fibre products. Recall that given two covers $\nu : Z \to Y$ and $\mu : Z' \to Y$, the geometric points of the fibre product $Z \times_Y Z'$ are pairs (z, z') such that $\nu(z) = \mu(z')$. In particular, the fibre product over the projection $X \to \mathbf{P}^1_Q$ is

$$\begin{aligned} X \times_{\mathbf{P}^1_Q} X &= \{((u_1, r_1), (u_2, r_2)) \mid u_1(r_1) = 0, u_2(r_2) = 0, u_1 = u_2\} \\ &\cong \{(u, r_1, r_2) \mid u(r_1) = 0, u(r_2) = 0\}. \end{aligned}$$

This product $X \times_{\mathbf{P}^1_Q} X$ contains a trivial component, the diagonal, corresponding to triples (u, r, r). The rest is referred to as the non-trivial part, and we prove that it is

an absolutely irreducible curve (Corollary 2.11). Iterating this construction, the fibre product $(X \times_{\mathbf{P}^1_Q} X) \times_X (X \times_{\mathbf{P}^1_Q} X)$ (over the projection $X \times_{\mathbf{P}^1_Q} X \to X$ to the first component) encodes quadruples (u, r_1, r_2, r_3). Therefore the curve C naturally embeds into the non-trivial part of this product. We prove that this non-trivial part is itself an absolutely irreducible curve (Lemma 2.13).

Instead of the projection $X \to \mathbf{P}^1_Q$, we work with an isomorphic cover θ. It is easy to see that the canonical projection $X \to \mathbf{P}^1$ is an isomorphism, with inverse $r \mapsto (s_2(r)s_1 - s_1(r)s_2, r)$. Through the isomorphisms $X \cong \mathbf{P}^1$ and $\mathbf{P}^1_Q \cong \mathbf{P}^1$, this projection is isomorphic to the cover θ in the following commutative diagram (where, again, the morphisms are written affinely for convenience):

$$\begin{array}{ccccc}
 & & (u,r) & \longmapsto & u \\
(u,r) & & X & \longrightarrow & \mathbf{P}^1_Q \qquad\qquad s_1 - \alpha s_2 \\
\big\downarrow & & \big\downarrow \wr & & \big\downarrow \wr \qquad\qquad \big\downarrow \\
r & & \mathbf{P}^1 & \xrightarrow{\theta} & \mathbf{P}^1 \qquad\qquad \alpha \\
 & & r & \longmapsto & s_1(r)/s_2(r).
\end{array}$$

For convenience, consider θ as a cover $X_1 \to X_0$ where $X_0 = X_1 = \mathbf{P}^1$. As a first step, we study the induced fibre product $X_1 \times_{X_0} X_1$. It contains the diagonal Δ_1, isomorphic to X_1. We wish to show that $Y_2 = X_1 \times_{X_0} X_1 \setminus \Delta_1$ is absolutely irreducible. The second step consists in showing that $X_2 \times_{X_1} X_2 \setminus \Delta_2$ is also absolutely irreducible, where X_2 is a desingularisation of Y_2 and Δ_2 is the diagonal. The following lemma provides a general method used in both steps.

Lemma 2.10. *Let Y and Z be two absolutely irreducible, smooth, complete curves over k, and consider a cover $\eta : Z \to Y$. If there exists a point $a \in Z$ such that η is not ramified at a and $\#(\eta^{-1}(\eta(a))) = 2$, then $Z \times_Y Z \setminus \Delta$ is absolutely irreducible, where Δ is the diagonal component.*

Proof. By contradiction, suppose that $Z \times_Y Z \setminus \Delta$ is not absolutely irreducible, and can be decomposed as two components $A \cup B$. Let $\mathrm{pr} : Z \times_Y Z \to Z$ be the projection on the first factor. Since $Z \times_Y Z$ is complete, both A and B are complete, so we have $\mathrm{pr}(A) = \mathrm{pr}(B) = \mathrm{pr}(\Delta) = Z$. Observe that $\mathrm{pr}^{-1}(a)$ consists of $\#(\eta^{-1}(\eta(a))) = 2$ points, so one of them must belong to two of the components A, B and Δ. That point must therefore be singular in $Z \times_Y Z$, contradicting the fact that η is not ramified at a (recall that a point $(z_1, z_2) \in Z \times_Y Z$ is singular if and only if η is ramified at both z_1 and z_2). □

Corollary 2.11. *The curve $Y_2 = X_1 \times_{X_0} X_1 \setminus \Delta_1$ is absolutely irreducible.*

Proof. First observe that θ is ramified only at b_1 and b_2 (as can be verified from the explicit formula $\theta(r) = s_1(r)/s_2(r)$). In particular, it is not ramified at a_1. Since $\#(\theta^{-1}(\theta(a_1))) = \#\{a_1, b_1\} = 2$, we apply Lemma 2.10. □

Lemma 2.12. *The desingularisation morphism $\nu : X_2 \to Y_2$ is a bijection between the geometric points.*

Proof. It is sufficient to prove that for any singular point P on Y_2, and $\varphi : \tilde{Y}_2 \to Y_2$ the blowing-up at P, the preimage $\varphi^{-1}(P)$ consists of a single smooth point. Up to

a linear transformation of $X_1 = \mathbf{P}^1$, we can assume that s_1 and s_2 are of the form $s_1(x) = (x-1)x^q$ and $s_2(x) = x - a$, for some $a \neq 0, 1$. The intersection A of the curve Y_2 with the affine patch $\mathbf{A}^2 \subset \mathbf{P}^1 \times \mathbf{P}^1$ can then be defined by the polynomial

$$f(x,y) = \frac{s_1(x)s_2(y) - s_1(y)s_2(x)}{x-y} = \frac{x^q(x-1)(y-a) - y^q(y-1)(x-a)}{x-y}.$$

It remains to blow up A at the singularity $(0,0)$ (which corresponds to (b_1, b_1) through the linear transformation), and check the required properties. This is easily done following [Har77, Example 4.9.1], and we include details for the benefit of the reader. Let $\psi : Z \to \mathbf{A}^2$ be the blowing-up of $\mathbf{A}^2$ at $(0,0)$. The inverse image of A in Z is defined in $\mathbf{A}^2 \times \mathbf{P}^1$ by the equations $f(x,y) = 0$ and $ty = xu$ (where t and u parameterize the factor $\mathbf{P}^1$). It consists of two irreducible components: the blowing-up $\tilde{A}$ of A at $(0,0)$ and the exceptional curve $\psi^{-1}(0,0)$. Suppose $t \neq 0$, so we can set $t = 1$ and use u as an affine parameter (since f is symmetric, the case $u \neq 0$ is similar). We have the affine equations $f(x,y) = 0$ and $y = xu$, and substituting we get $f(x, xu) = 0$, which factors as

$$f(x,xu) = x^{q-1}\frac{(x-1)(xu-a) - u^q(xu-1)(x-a)}{1-u}.$$

The blowing-up $\tilde{A}$ is defined on $t = 1$ by the equations $g(x,u) = f(x,xu)/x^{q-1} = 0$ and $y = xu$. It meets the exceptional line only at the point $u = 1$, which is non-singular. □

The projection $X_1 \times_{X_0} X_1 \to X_1$ on the first component induces another cover $\theta_2 : X_2 \to X_1$, through which we build the fibre product $X_2 \times_{X_1} X_2$. As above, it contains a diagonal component Δ_2 isomorphic to X_2.

Lemma 2.13. *The curve $Y_3 = X_2 \times_{X_1} X_2 \setminus \Delta_2$ is absolutely irreducible.*

Proof. Let $\nu : X_2 \to Y_2$ be the bijective morphism from Lemma 2.12. Since θ is only ramified at b_1 and b_2, the cover θ_2 is ramified at most at the points $\nu^{-1}(b_i, b_i)$ and $\nu^{-1}(a_i, b_i)$ (for $i \in \{1,2\}$). In particular, it is not ramified at $\nu^{-1}(b_1, a_1)$. Since $\#(\theta_2^{-1}(\theta_2(\nu^{-1}(b_1,a_1)))) = \#\{\nu^{-1}(b_1,a_1), \nu^{-1}(b_1,b_1)\} = 2$, we apply Lemma 2.10. □

Proposition 2.14. *The curve C is absolutely irreducible.*

Proof. Let $\nu : X_2 \to Y_2$ be the morphism from Lemma 2.12. It is an isomorphism away from the singularities of Y_2, so

$$C \longrightarrow Y_3 : (u, r_1, r_2, r_3) \longmapsto (\nu^{-1}(r_1, r_2), \nu^{-1}(r_1, r_3))$$

is a morphism. It is an embedding, and the result follows from Lemma 2.13. □

2.5. Counting split polynomials in $\mathbf{P}^1_Q$

Recall that we wish to prove Proposition 2.3 by showing that $\mathbf{P}^1_Q(k)$ contains a lot of polynomials that split into good polynomials over k. The results of Section 2.4 allow us to prove in Theorem 2.15 that a lot of polynomials in $\mathbf{P}^1_Q(k)$ do split. We then show in Proposition 2.16 that all these polynomials are coprime, which implies that bad polynomials cannot appear too often.

Theorem 2.15. *Let $k/\mathbf{F}_{q^d}$ be a field extension of degree m, and Q be a good irreducible quadratic polynomial in $k[x]$ coprime to h_1. If $dm \geq 23$, there are at least $\#k/2q^3$ polynomials in $\mathbf{P}^1_Q$ that split completely over the field k.*

Proof. Let $\Theta : Y_3 \to \mathbf{P}^1_Q$ be the cover resulting from the composition of the successive covers of Section 2.4. Let $S_3 = \Theta^{-1}(\mathbf{P}^1_Q \cap S)$. The embedding $C \to Y_3$ from Proposition 2.14 has image $Y_3 \setminus S_3$. The morphism

$$\mu : Y_3 \to \mathbf{P}^1 \times \mathbf{P}^1 \times \mathbf{P}^1 : (\nu^{-1}(r_1, r_2), \nu^{-1}(r_1, r_3)) \mapsto (r_1, r_2, r_3)$$

restricts to an embedding of $Y_3 \setminus S_3$. Let A be the intersection of $\mu(Y_3)$ with the affine patch $\mathbf{A}^3$. The curve A is a component of the (reducible) curve defined by the equations $\theta(r_1) = \theta(r_2)$ and $\theta(r_1) = \theta(r_3)$. Therefore A is of degree at most $4(q+1)^2$. If B is the closure of A in $\mathbf{P}^3$, then [Bac96, Th. 3.1] shows that

$$|\#B(k) - \#k - 1| \leq 16(q+1)^4\sqrt{\#k}.$$

Since Y_3 is complete, $\mu(Y_3)$ is closed, so all the points of $B \setminus A$ are at infinity, and there are at most $\deg(B) \leq 4(q+1)^2$ of them. Also, at most $2(q^3 - q)$ points of B are in $\mu(S_3)$ (because $\#S = 2$ and Θ is of degree $q^3 - q$). Therefore

$$\#C(k) = \#(Y_3 \setminus S_3)(k) \geq \#k + 1 - 16(q+1)^4\sqrt{\#k} - 4(q+1)^2 - 2(q^3 - q).$$

Since $q \geq 2$ and $dm \geq 23$, we get $\#C(k) \geq \#k/2$. From Proposition 2.9, and the fact that the map Θ is $q^3 - q$ to one, we get that at least $\#k/2q^3$ polynomials in $\mathbf{P}^1_Q$ split completely over k. □

Let φ be the morphism defined in (2.3) on page 27.

Proposition 2.16. *Suppose Q is a good polynomial. For any two distinct polynomials f and g in $\mathbf{P}^1_Q(\overline{\mathbf{F}}_q)$, we have* $\gcd(f, g) = 1$ *and* $\gcd(h_1\varphi(f), h_1\varphi(g)) = Q$.

Proof. Let s_1 and s_2 be as in Proposition 2.8. They have no common root. Since f and g are distinct, all the polynomials of $\mathbf{P}^1_Q$ are of the form $\alpha f + \beta g$ for $(\alpha : \beta) \in \mathbf{P}^1$. Then, if r is a root of f and g, it is a root of all the polynomials of $\mathbf{P}^1_Q$. In particular, it is a root of both s_1 and s_2, a contradiction. This shows that $\gcd(f, g) = 1$.

Similarly, if a polynomial h divides $h_1\varphi(f)$ and $h_1\varphi(g)$, it must also divide both $h_1\varphi(s_1) = (x - a_1)(h_0 - b_1^q h_1)$ and $h_1\varphi(s_2) = (x - a_2)(h_0 - b_2^q h_1)$. Since $h_0 - b_1^q h_1$ and $h_0 - b_2^q h_1$ are coprime, h must divide Q. □

Proof of Proposition 2.3 (degree 2 elimination). As discussed in Section 2.1.1, it is sufficient to prove that a uniformly random element of $\mathbf{P}^1_Q(k)$ has a good probability to lead to an elimination into good polynomials. A polynomial $f \in \mathbf{P}^1_Q(k)$ leads to an elimination into good polynomials if f splits completely over k into good linear polynomials, and $\varphi(f)$ is itself a good polynomial.

Let A be the set of polynomials of $\mathbf{P}^1_Q(k)$ that split completely over k. From Theorem 2.15, A contains at least $q^{dm-3}/2$ elements. Trap roots τ occurring in A or $\varphi(A)$ must be roots of $h_1 x^q - h_0$, or of $h_1 x^{q^{dn+1}} - h_0$ for $n \mid m/2$, or satisfy $\frac{h_0}{h_1}(\tau) \in \mathbf{F}_{q^{dm/2}}$. There are at most $q^{\frac{dm}{2}+3}$ such trap roots. From Proposition 2.16, any trap root can only occur once in A and in $\varphi(A)$. So there are at most $2q^{\frac{dm}{2}+3}$ polynomials in A for which trap roots appear. Therefore the number of elements in A leading to a good reduction is at least

$$\frac{1}{2}q^{dm-3} - 2q^{\frac{dm}{2}+3} \geq \frac{1}{2}\left(q^{dm-3} - 4q^{dm-8}\right) \geq \frac{1}{4}q^{dm-3},$$

using $dm \geq 23$. Since $\mathbf{P}^1_Q(k)$ contains $q^{dm} + 1$ elements, the probability of a random element to lead to a good elimination is $1/O(q^3)$. □

PART II

ISOGENY GRAPHS OF ORDINARY ABELIAN VARIETIES

3

Horizontal isogeny graphs

Abstract. This chapter is based on a joint work with Dimitar Jetchev, to appear in the journal Acta Arithmetica as

[JW18] D. Jetchev and B. Wesolowski, *Horizontal isogeny graphs of ordinary abelian varieties and the discrete logarithm problem*, Acta Arithmetica (2018), in press.

It is the natural continuation of my master's thesis [Wes14] (supervised by Dimitar Jetchev and Kenneth A. Ribet), which dealt with the simpler case where the abelian varieties have dimension two, with maximal endomorphism ring whose real part has a trivial narrow class group.

Original abstract. Fix an ordinary abelian variety defined over a finite field. The ideal class group of its endomorphism ring acts freely on the set of isogenous varieties with same endomorphism ring, by complex multiplication. Any subgroup of the class group, and generating set thereof, induces an isogeny graph on the orbit of the variety for this subgroup. We compute (under the extended Riemann hypothesis) some bounds on the norms of prime ideals generating the subgroup, such that the associated graph has good expansion properties.

We use these graphs, together with a recent algorithm of Dudeanu, Jetchev, Robert and Vuille for computing explicit isogenies in genus 2, to prove random self-reducibility of the discrete logarithm problem within the subclasses of principally polarisable ordinary abelian surfaces with fixed endomorphism ring. In addition, we remove the heuristics in the complexity analysis of an algorithm of Galbraith for explicitly computing isogenies between two elliptic curves in the same isogeny class, and extend it to a more general setting including genus 2.

Since the seminal work of Miller [Mil86a] and Koblitz [Kob87], elliptic curves have become a central tool to the design of cryptographic protocols. Their popularity is largely due to the fact that the discrete logarithm problem on elliptic curves has resisted decades of cryptanalysis. The generic algorithms presented in Section 1.1 do apply, and other methods successfully attacked certain classes of elliptic curves, but very little has been discovered beyond that. More generally, if $\mathscr{A}$ is an abelian variety defined over a finite field k, one could consider the discrete logarithm problem in the group of rational points $\mathscr{A}(k)$.

Definition 3.1 (Abelian variety)**.** An *abelian variety* over a field k is a connected, projective algebraic group over k. In other words, a connected, projective algebraic

variety endowed with a group structure, such that the multiplication and inversion are regular maps.

An elliptic curve is an abelian variety of dimension one. Choosing $\mathscr{A}$ to be the Jacobian of a hyperelliptic curve of genus g leads to what is commonly referred to as *hyperelliptic curve cryptography*, and elliptic curve cryptography falls under this umbrella as the case $g = 1$. Interestingly, the index calculus method has led to efficient algorithms for curves of high genus. However, the case $g = 2$ remains unaffected, and has in fact been shown to be a promising alternative to elliptic curves, allowing very efficient arithmetic [Gau07, BCHL16] (and thereby, efficient protocols). Much like elliptic curves, little is known about the hardness of the corresponding version of the discrete logarithm problem beyond the generic methods.

Definition 3.2 (Isogeny)**.** An *isogeny* is a morphism of abelian varieties (a regular map that is also a group homomorphism) that is surjective and has finite kernel. By convention, the trivial map (sending each point to zero) is also an isogeny.

Two abelian varieties are said to be *isogenous* if there exists a non-zero isogeny between them. The set of all abelian varieties (up to isomorphism) isogenous to $\mathscr{A}$ is called the *isogeny class* of $\mathscr{A}$. Note that in this thesis, given a finite field k, all varieties and morphisms are considered over the algebraic closure $\overline{k}$, and when we say that an abelian variety $\mathscr{A}$ is defined over k, we always mean that we have implicitly chosen a model of $\mathscr{A}$ over k, which endows $\mathscr{A}$ with an action of the k-Frobenius. An isogeny $\varphi : \mathscr{A} \to \mathscr{B}$ is said to be defined over k if it arises via base change from an isogeny of the implicitly chosen models; this is equivalent to commuting with the k-Frobenius.

If $\mathscr{A}$ is an abelian variety over a finite field k, and $\mathscr{B}$ is an isogenous abelian variety, then the discrete logarithm problem on the group of k-rational points $\mathscr{A}(k)$ may be transferred to a problem on $\mathscr{B}(k)$, assuming that one has an efficiently computable isogeny $\mathscr{A} \to \mathscr{B}$. There is thus a natural cryptographic interest in understanding the structure of *graphs* of isogenies between abelian varieties. These are graphs whose vertices are isomorphism classes of abelian varieties and whose edges are equivalence classes of isogenies belonging to some particular family, two isogenies being equivalent if they share a kernel. Isogeny graphs of elliptic curves are well-understood, and have found a profusion of applications in cryptography and algorithmic number theory. There is great interest in generalising these results to higher dimensions, which is the object of the next three chapters.

In this first chapter on isogeny graphs, we focus on so-called *horizontal* isogenies, and the problem of transferring discrete logarithm instances will serve as a guiding thread. We investigate the structure of horizontal isogeny graphs and prove that they rapidly mix random walks (assuming the extended Riemann hypothesis, henceforth ERH). This leads to a random self-reducibility theorem: the discrete logarithm problem on a given abelian variety reduces to the same problem on a uniformly random abelian variety in the isogeny graph. The case of ordinary elliptic curves was treated by Jao, Miller and Venkatesan [JMV05, JMV09], and we generalise it to higher dimensions.

These properties of horizontal isogeny graphs also allow us to tackle the isogeny path problem: given two abelian varieties in the isogeny graph, find a path between them (allowing, for instance, to transfer the discrete logarithm problem from one to the other). Galbraith provides in [Gal99] a heuristic algorithm for this problem on ordinary

elliptic curves. We construct a rigorous variant (assuming ERH), generalised to higher dimensions, using again rapid mixing properties.

3.1. Isogenies, endomorphism rings, and complex multiplication

In this section, we review important notions for our study of isogeny graphs. We start with properties of isogenies and endomorphisms, and the structure of endomorphism rings. These notions allow to build a relation between some isogeny graphs and class groups of certain orders in number fields, or subgroups thereof.

3.1.1. Isogeny graphs. Recall that an isogeny is a morphism of abelian varieties that is surjective and has finite kernel. The *degree* of a non-zero isogeny $\varphi : \mathscr{A} \to \mathscr{B}$ defined over a field k is the degree of the induced injection of function fields $\varphi^* : \overline{k}(\mathscr{B}) \to \overline{k}(\mathscr{A})$, and the isogeny is *separable* if this field extension is separable. For separable isogenies, the degree coincides with the size of the kernel. By convention, a zero isogeny has degree 0. An *endomorphism* is an isogeny from an abelian variety to itself. A simple family of endomorphisms are the multiplication-by-m maps: for any integer m, we denote by $[m]$ the endomorphism that sends any geometric point $P \in \mathscr{A}(\overline{k})$ to mP. The endomorphism $[m]$ has degree $m^{2\dim(\mathscr{A})}$, and its kernel is the group $\mathscr{A}[m]$ of m-torsion points.

We need two important facts about isogenies. First, any isogeny $\varphi : \mathscr{A} \to \mathscr{B}$ has a *dual* isogeny[1] $\hat{\varphi} : \mathscr{B} \to \mathscr{A}$ such that $\hat{\varphi} \circ \varphi$ is the multiplication by $\deg(\varphi)$ on $\mathscr{A}$. This makes the relation "there is an isogeny from $\mathscr{A}$ to $\mathscr{B}$" an equivalence relation on isomorphism classes of abelian varieties, and the equivalence classes are called isogeny classes. Note that this notion of dual is well-behaved in the case of elliptic curves, where φ and $\hat{\varphi}$ have the same degree, and $\hat{\hat{\varphi}} = \varphi$, but in general, $\hat{\varphi}$ has degree $\deg(\varphi)^{2\dim(\mathscr{A})-1}$. Second, any finite subgroup κ of $\mathscr{A}$ determines a unique separable isogeny (up to an isomorphism of the target) of kernel κ, which is simply the projection $\mathscr{A} \to \mathscr{A}/\kappa$.

The vertices of an isogeny graph are usually isomorphism classes of abelian varieties in a given isogeny class. Sometimes we only consider a subset of the isogeny class. For instance, we might restrict to varieties with a specified endomorphism ring. An edge between two vertices in an isogeny graph represents an isogeny between the corresponding abelian varieties. We do not usually consider every possible isogeny in a single graph (as there are infinitely many of them between any two isogenous abelian varieties), but restrict to certain families. For instance, we might consider an isogeny graph containing all isogenies of a given prime degree ℓ (we call this an ℓ-isogeny graph), or all isogenies of prime degree smaller than a given bound. Therefore, restricting to a family of isogenies, the graphs can be oriented: if there is an isogeny from $\mathscr{A}$ to $\mathscr{B}$ in this family, there is not necessarily an isogeny from $\mathscr{B}$ to $\mathscr{A}$ in that same family. Finally, there is a natural way to add a multiplicity to each edge. For any two vertices represented by the abelian varieties $\mathscr{A}$ and $\mathscr{B}$, the multiplicity of the edge $\mathscr{A} \to \mathscr{B}$ is the number of subgroups κ of $\mathscr{A}$ such that $\mathscr{A}/\kappa \cong \mathscr{B}$ and the isogeny $\mathscr{A} \to \mathscr{A}/\kappa$ is in the family of interest.

The choice of a subset of the isogeny class for the vertices, and of a family of isogenies for the edges, is usually motivated by two aspects: structure, and computability. Structure, because we want the graphs to be either enlightening (can we read interesting information about the varieties from the structure of the graph?) or convenient (can we easily move around that graph, take random walks or solve path problems?). Computability, because we usually want to navigate (algorithmically) in these graphs,

[1] This "dual" should not be confused with the isogeny between the dual varieties $\varphi^\vee : \mathscr{B}^\vee \to \mathscr{A}^\vee$.

which requires to compute isogenies corresponding to the edges. Computing isogenies can be a very difficult problem, the solution of which usually requires more structure than just an abstract abelian variety. As a result, we often need to restrict to principally polarisable (or even polarised) abelian varieties, and isogenies of small degree. This is not an issue for elliptic curves, which are all principally polarised, and isogenies can be computed with Vélu's formulas [Vél71] in polynomial time in the degree. The similar problem in dimension 2 (or higher) is more challenging since, unlike elliptic curves, abelian surfaces are not *a priori* principally polarised, yet computing isogenies with the algorithm of Dudeanu, Jetchev, Robert and Vuille [DJRV16, Dud16] requires a principal polarisation.

3.1.2. Endomorphism rings of ordinary abelian varieties. Two endomorphisms of an abelian variety can be added (point-wise) or multiplied (by composing them), thus endowing the set of endomorphisms with a ring structure. Given an abelian variety $\mathscr{A}$ defined over a field k, we write $\mathrm{End}_k(\mathscr{A})$ for the ring of endomorphisms defined over k. Unless otherwise specified, we are working over the algebraic closure, with the endomorphism ring $\mathrm{End}(\mathscr{A}) = \mathrm{End}_{\overline{k}}(\mathscr{A})$. Endomorphism rings play a central role in the structure of isogeny graphs.

Our study of isogeny graphs is focused on the case of absolutely simple, ordinary abelian varieties over a finite field. An abelian variety is absolutely simple if it is not isogenous to a product of abelian varieties of lower dimension. It is ordinary if its p-rank is equal to its dimension (where p is the characteristic of the finite field). Note that in this ordinary case, for any finite field $\mathbf{F}_q$, we have $\mathrm{End}(\mathscr{A}) = \mathrm{End}_{\overline{\mathbf{F}}_q}(\mathscr{A}) = \mathrm{End}_{\mathbf{F}_q}(\mathscr{A})$ (see [Wat69, Theorem 7.2.]).

An order in a number field is a full rank $\mathbf{Z}$-lattice which is also a subring. Let $\mathscr{A}$ be an absolutely simple, ordinary abelian variety of dimension g over a finite field $\mathbf{F}_q$. Its endomorphism ring $\mathrm{End}(\mathscr{A})$ is an order in a CM-field K, i.e., in a totally imaginary quadratic extension K of a totally real number field K^+ (CM stands for *complex multiplication*). This CM-field is the *endomorphism algebra* of $\mathscr{A}$, which can be constructed as the tensor product $K = \mathrm{End}(\mathscr{A}) \otimes_{\mathbf{Z}} \mathbf{Q}$. The degree of an endomorphism of $\mathscr{A}$ coincides with its algebraic norm in the field K. The maximal real subfield K^+ is of degree g over $\mathbf{Q}$. If $\varphi : \mathscr{A} \to \mathscr{B}$ is an isogeny, we can construct an embedding

$$\begin{aligned} \iota_\varphi : \mathrm{End}(\mathscr{B}) &\longrightarrow K = \mathrm{End}(\mathscr{A}) \otimes_{\mathbf{Z}} \mathbf{Q} \\ \alpha &\longmapsto (\hat{\varphi} \circ \alpha \circ \varphi) \otimes \deg(\varphi)^{-1}. \end{aligned}$$

An immediate consequence is that for any abelian variety $\mathscr{B}$ isogenous to $\mathscr{A}$, we have $\mathrm{End}(\mathscr{B}) \otimes_{\mathbf{Z}} \mathbf{Q} \cong K$. In fact, this embedding does not depend on a choice of φ. Therefore, fixing (arbitrarily) the abelian variety $\mathscr{A}$ as a "reference" in the isogeny class, we simply denote by $\iota_{\mathscr{B}}$ the embedding of $\mathrm{End}(\mathscr{B})$ in the CM-field K, and $\mathcal{O}(\mathscr{B})$ is the image of this embedding — an order in K. Note that we will often abuse notation and refer to the order $\mathcal{O}(\mathscr{B})$ as the endomorphism ring of $\mathscr{B}$.

Even though isogenies preserve the endomorphism algebra K, they can change the endomorphism ring (as an order in K). In this chapter and the next, we study horizontal isogenies, which preserve the endomorphism ring, and in Chapter 5, we study vertical isogenies, which change the endomorphism ring.

The Frobenius endomorphism π of $\mathscr{A}$ generates the field $K = \mathbf{Q}(\pi)$. The *Frobenius polynomial* is the characteristic polynomial of π, and Tate's isogeny theorem [Tat66] implies that two abelian varieties defined over $\mathbf{F}_q$ are isogenous if and only if they have the same Frobenius polynomial. This element π is an algebraic integer with the property

that for any complex embedding $\imath : \mathbf{Q}(\pi) \to \mathbf{C}$, we have $|\imath(\pi)| = q^{1/2}$. Elements with this property are called *q-Weil numbers*. Any q-Weil number π uniquely determines an isogeny class of simple abelian varieties over $\mathbf{F}_q$ with Frobenius π, and two q-Weil numbers define the same isogeny class if and only if they are conjugate over $\mathbf{Q}$ (see [Tat71, Théorème 1]).

3.1.3. Action of class groups on abelian varieties. Consider an absolutely simple, ordinary abelian variety $\mathscr{A}$ with endomorphism algebra K. There is a natural action of the class group of the endomorphism ring of $\mathscr{A}$ on the set of isogenous abelian varieties (up to isomorphism) with same endomorphism ring. This action has classically been studied for abelian varieties defined over the field $\mathbf{C}$ of complex numbers (as done by Taniyama and Shimura [ST61], and presented in the upcoming Section 3.2), and the theory over finite fields can be deduced by canonical lifting. However, the action can be constructed directly over any field, and modern tools make is quite simple (notably quotients by finite group schemes in positive characteristic, unavailable to Taniyama and Shimura). The following construction seems to have first appeared in the work of Waterhouse [Wat69] as a way to study isogenies over finite fields, where the powerful machinery of complex lattices is not readily available. Note that the presentation below is a bit simpler, since we focus on the ordinary case: the endomorphism ring is commutative, so all ideals are "kernel ideals" in the language of Waterhouse.

Definition 3.3 ($\mathfrak{a}$-torsion)**.** For any ideal $\mathfrak{a}$ in the endomorphism ring of $\mathscr{A}$, the $\mathfrak{a}$-torsion of $\mathscr{A}$ is the finite subgroup $\mathscr{A}[\mathfrak{a}] = \cap_{\alpha\in\mathfrak{a}} \ker(\alpha)$.

Like any finite subgroup of $\mathscr{A}$, the $\mathfrak{a}$-torsion is the kernel of a unique separable isogeny: the projection

$$\varphi_{\mathfrak{a}} : \mathscr{A} \longrightarrow \mathscr{A}/\mathscr{A}[\mathfrak{a}].$$

This isogeny is the *$\mathfrak{a}$-multiplication* of $\mathscr{A}$, and its target $\mathscr{A}/\mathscr{A}[\mathfrak{a}]$ is the *$\mathfrak{a}$-transform* of $\mathscr{A}$ (up to isomorphism). We denote this $\mathfrak{a}$-transform by $\mathscr{A}^{\mathfrak{a}}$. Suppose that $\mathscr{A}$ is defined over a finite field k. Then, $\mathscr{A}[\mathfrak{a}]$ is also defined over k (using the fact that the k-Frobenius commutes with all the endomorphisms in $\mathfrak{a}$), hence so are the variety $\mathscr{A}^{\mathfrak{a}}$ and the isogeny $\varphi_{\mathfrak{a}}$. Another notable property is that the degree of $\varphi_{\mathfrak{a}}$ coincides with the norm of $\mathfrak{a}$ (this can be deduced from the previously mentioned fact that the degree of an endomorphism coincides with its algebraic norm).

Lemma 3.4. *For any invertible ideal $\mathfrak{a}$ in the endomorphism ring of $\mathscr{A}$, we have that $\mathscr{A} \cong \mathscr{A}^{\mathfrak{a}}$ if and only if $\mathfrak{a}$ is principal.*

Proof. If $\mathfrak{a}$ is generated by an endomorphism α, then $\mathscr{A}[\mathfrak{a}] = \ker(\alpha)$, and the first isomorphism theorem implies that $\mathscr{A} \cong \mathscr{A}^{\mathfrak{a}}$. Now, suppose that there is an isomorphism $\eta : \mathscr{A}^{\mathfrak{a}} \to \mathscr{A}$. Then, $\alpha = \eta \circ \varphi_{\mathfrak{a}}$ is an endomorphism of $\mathscr{A}$. Since $\ker\alpha = \mathscr{A}[\mathfrak{a}]$, any endomorphism in $\mathfrak{a}$ factors through α, so $\mathfrak{a} \subseteq (\alpha)$. Since these ideals have the same norm (they correspond to isogenies of same degree), they must be equal, so $\mathfrak{a}$ is principal. □

Lemma 3.5. *For any invertible ideal $\mathfrak{a}$ in the endomorphism ring of $\mathscr{A}$, we have $\mathcal{O}(\mathscr{A}) = \mathcal{O}(\mathscr{A}^{\mathfrak{a}})$. In other words, the $\mathfrak{a}$-multiplication is a horizontal isogeny.*

Proof. It is sufficient to prove that for any ideal $\mathfrak{a}$, the order $\mathcal{O}(\mathscr{A}^{\mathfrak{a}})$ contains the order $\mathcal{O}(\mathscr{A})$. For any endomorphism α of $\mathscr{A}$, it is easy to check that $\mathscr{A}[\mathfrak{a}] \subseteq \ker(\varphi_{\mathfrak{a}} \circ \alpha)$, so there is an endomorphism α' of $\mathscr{A}^{\mathfrak{a}}$ such that $\varphi_{\mathfrak{a}} \circ \alpha = \alpha' \circ \varphi_{\mathfrak{a}}$. Then,

$$\imath_{\mathscr{A}^{\mathfrak{a}}}(\alpha') = (\hat{\varphi}_{\mathfrak{a}} \circ \alpha' \circ \varphi_{\mathfrak{a}}) \otimes \deg(\varphi_{\mathfrak{a}})^{-1} = (\hat{\varphi}_{\mathfrak{a}} \circ \varphi_{\mathfrak{a}} \circ \alpha) \otimes \deg(\varphi_{\mathfrak{a}})^{-1} = \alpha \otimes 1 = \imath_{\mathscr{A}}(\alpha),$$

which proves that $\imath_{\mathscr{A}}(\alpha) \in \mathcal{O}(\mathscr{A}^{\mathfrak{a}})$, so $\mathcal{O}(\mathscr{A}) \subseteq \mathcal{O}(\mathscr{A}^{\mathfrak{a}})$. □

Therefore, the notion of $\mathfrak{a}$-transform defines an action of invertible ideals of $\mathcal{O}(\mathscr{A})$ on the set of isomorphism classes of abelian varieties isogenous to $\mathscr{A}$ and with same endomorphism ring. This action has an identity ($\mathscr{A}^{\mathcal{O}(\mathscr{A})} = \mathscr{A}$) and is compatible ($\mathscr{A}^{\mathfrak{ab}} \cong (\mathscr{A}^{\mathfrak{a}})^{\mathfrak{b}}$ for any two ideals $\mathfrak{a}$ and $\mathfrak{b}$).

The class group $\mathrm{Cl}(\mathcal{O})$ of an order $\mathcal{O}$ is the quotient $\mathscr{I}(\mathcal{O})/P(\mathcal{O})$, where $\mathscr{I}(\mathcal{O})$ is the group of fractional ideals of $\mathcal{O}$, and $P(\mathcal{O})$ the subgroup generated by principal ideals. Therefore, Lemma 3.4 implies that the action of ideals induces a *free* action of the class group $\mathrm{Cl}(\mathcal{O}(\mathscr{A}))$ on the set of isomorphism classes of abelian varieties isogenous to $\mathscr{A}$ and with same endomorphism ring.

3.1.4. Horizontal isogeny graphs as Cayley graphs. Let π be a q-Weil number, and let $K = \mathbf{Q}(\pi)$ be the corresponding CM-field, with K^+ its maximal real subfield. Fix an order $\mathcal{O}$ in K, and let $\mathcal{V}_{\pi,\mathcal{O}}$ be the set of all $\mathbf{F}_q$-isomorphism classes of abelian varieties defined over $\mathbf{F}_q$ with endomorphism ring $\mathcal{O}$ in the isogeny class characterised by π. We have shown in Section 3.1.3 that the class group $\mathrm{Cl}(\mathcal{O})$ acts freely on $\mathcal{V}_{\pi,\mathcal{O}}$. One can choose any reference variety $\mathscr{A}$ in $\mathcal{V}_{\pi,\mathcal{O}}$ and any subgroup H in $\mathrm{Cl}(\mathcal{O})$, and consider the orbit $H(\mathscr{A})$.

The action of the class group induces an equivalence of categories between the category of objects $H(\mathscr{A})$ and morphisms the isogenies between them, and the category whose objects are the ideal classes in the subgroup H, and the sets of morphisms from $a \in H$ to $b \in H$ are the ideals of $\mathcal{O}$ in the class $a^{-1}b$. Restricting the morphisms to a finite set of generators, the latter category can be seen as a Cayley (multi)graph.

Definition 3.6 (Cayley graph)**.** Let G be a finite group and S a generating subset of G, with $S = S^{-1}$. The *Cayley graph* $\mathrm{Cay}(G, S)$ is the finite $|S|$-regular undirected graph with set of vertices G, and an edge between g and sg for any $g \in G$ and $s \in S$.

Remark 3.7. The edges of $\mathrm{Cay}(G, S)$ can have multiplicities if S is a multiset. If $\mathcal{S}$ is a set of labels and $f : \mathcal{S} \to S$ is a surjection, then f naturally induces a Cayley multigraph for the set of generators S whose edges are labelled by elements of $\mathcal{S}$.

Let $\mathcal{S}$ be a set of ideals of $\mathcal{O}$, and S its image in $\mathrm{Cl}(\mathcal{O})$, with $f : \mathcal{S} \to S$ the induced surjection. Let $\mathrm{Cay}(H, S \cap H)$ be the induced labelled multigraph. Let T be the set of all isogenies between elements of $H(\mathscr{A})$ corresponding to the ideals of $\mathcal{S}$. We build the graph $\mathscr{G}_{\mathcal{S}}$ with set of vertices $H(\mathscr{A})$ by adding an edge between the vertices $\mathscr{B}$ and $\mathscr{C}$ for any isogeny $\mathscr{B} \to \mathscr{C}$ in T. Then, the equivalence of categories induces an isomorphism between the graphs $\mathscr{G}_{\mathcal{S}}$ and $\mathrm{Cay}(H, S \cap H)$. The choice of a subgroup H and a generating set $\mathcal{S}$ usually accounts for constraints on the computability of certain isogenies. One might for instance want to consider only isogenies between principally polarisable abelian varieties, as in Example 3.15 below.

3.1.5. Class groups of orders. As reviewed in Section 3.1.3, class groups of orders in number fields are tightly connected to isogeny graphs. In this section, we recall some useful results on class groups.

Let K be a number field. Then, $\mathscr{I}(K)$ denotes the group of fractional ideals of $\mathcal{O}_K$. Fix a modulus $\mathfrak{m}$ of K (i.e., a formal product of primes in K, finite or infinite). The finite part is an ideal $\mathfrak{m}_0$ in $\mathcal{O}_K$, and the infinite part is a subset $\mathfrak{m}_\infty$ of the real embeddings of K. Let $\mathscr{I}_{\mathfrak{m}}(K)$ be the subgroup generated by ideals coprime to $\mathfrak{m}_0$. Let $P^{\mathfrak{m}}_{K,1}$ be the subgroup of $\mathscr{I}_{\mathfrak{m}}(K)$ generated by principal ideals of the form $\alpha\mathcal{O}_K$ where $\mathrm{ord}_{\mathfrak{p}}(\alpha - 1) \geq \mathrm{ord}_{\mathfrak{p}}(\mathfrak{m}_0)$ for all primes $\mathfrak{p}$ dividing $\mathfrak{m}_0$, and $\imath(\alpha) > 0$ for all $\imath \in \mathfrak{m}_\infty$. The *ray class group* of K modulo $\mathfrak{m}$ is the quotient group

$$\mathrm{Cl}_{\mathfrak{m}}(K) = \mathscr{I}_{\mathfrak{m}}(K)/P^{\mathfrak{m}}_{K,1}.$$

For any ideal $\mathfrak{a}$ such that $(\mathfrak{a}, \mathfrak{m}_0) = 1$, let $[\mathfrak{a}]_\mathfrak{m}$ denote its class in $\mathrm{Cl}_\mathfrak{m}(K)$. The *narrow ray class group* modulo the ideal $\mathfrak{m}_0$ is $\mathrm{Cl}_\mathfrak{m}(K)$ when $\mathfrak{m}_\infty$ contains all the real embeddings.

Example 3.8. The subgroup $P_{K,1}^{\mathcal{O}_K}$ is generated by all the principal ideals, so $\mathrm{Cl}_{\mathcal{O}_K}(K)$ is the usual ideal class group $\mathrm{Cl}(K)$. Also, the narrow ray class group modulo $\mathcal{O}_K$ is exactly the narrow class group $\mathrm{Cl}^+(K)$.

Let $\mathcal{O}$ be an order in K. The *conductor* of $\mathcal{O}$, defined as

$$\mathfrak{f} = \{x \in K \mid x\mathcal{O}_K \subset \mathcal{O}\},$$

is an invariant of the order. It is the largest subset of K that is simultaneously an ideal in $\mathcal{O}$ and in the maximal order $\mathcal{O}_K$. Any ideal coprime to the conductor $\mathfrak{f}$ is invertible in $\mathcal{O}$. Recall that the class group of $\mathcal{O}$ is the quotient $\mathrm{Cl}(\mathcal{O}) = \mathscr{I}(\mathcal{O})/P(\mathcal{O})$, where $\mathscr{I}(\mathcal{O})$ is the group of fractional ideals of $\mathcal{O}$, and $P(\mathcal{O})$ the subgroup generated by principal ideals. This class group can also be expressed as a quotient of $\mathscr{I}_\mathfrak{f}(K)$, as follows. Let $P_{K,\mathcal{O}}^\mathfrak{f}$ be the subgroup of $\mathscr{I}_\mathfrak{f}(K)$ generated by principal ideals $\alpha\mathcal{O}_K$ where $\alpha \in \mathcal{O}$ and $\alpha\mathcal{O} + \mathfrak{f} = \mathcal{O}$. From [LD15, Theorem 3.8] and [LD15, Theorem 3.11], the map sending any integral ideal $\mathfrak{a}$ of $\mathcal{O}_K$ to the ideal $\mathfrak{a} \cap \mathcal{O}$ of $\mathcal{O}$ extends to a surjection $\mathscr{I}_\mathfrak{f}(K) \to \mathrm{Cl}(\mathcal{O})$ with kernel $P_{K,\mathcal{O}}^\mathfrak{f}$. Therefore, it induces an isomorphism

$$\mathrm{Cl}(\mathcal{O}) \cong \mathscr{I}_\mathfrak{f}(K)/P_{K,\mathcal{O}}^\mathfrak{f}.$$

From [LD15, Theorem 4.2], there is a unique abelian extension $H(\mathcal{O})$ of K, the *ring class field* of $\mathcal{O}$, such that all primes of K ramified in $H(\mathcal{O})$ divide $\mathfrak{f}$, and the kernel of the Artin map

$$\varphi_{H(\mathcal{O})/K}^\mathfrak{f} : \mathscr{I}_\mathfrak{f}(K) \to \mathrm{Gal}(H(\mathcal{O})/K)$$

is $P_{K,\mathcal{O}}^\mathfrak{f}$. This map then induces an isomorphism $\mathrm{Cl}(\mathcal{O}) \cong \mathrm{Gal}(H(\mathcal{O})/K)$. Similarly, there is a unique abelian extension $H^+(\mathcal{O})$, the *narrow ring class field* of $\mathcal{O}$, ramified only at primes dividing $\mathfrak{f}$ and at infinite primes, such that $\mathrm{Gal}(H^+(\mathcal{O})/K)$ is isomorphic to the narrow class group $\mathrm{Cl}^+(\mathcal{O})$, through the Artin map.

3.2. Complex abelian varieties with complex multiplication

A key tool for studying isogeny graphs is the theory of complex multiplication (henceforth, CM theory). The main reference for this section is [ST61]. Let $\mathscr{A}_\mathbf{C} = \mathbf{C}^g/\Lambda$ be an abelian variety of dimension g over $\mathbf{C}$, where Λ is a lattice, and suppose its endomorphism algebra is a CM-field K (we say that $\mathscr{A}_\mathbf{C}$ has complex multiplication by K) and let K^+ be the real subfield of K of degree g.

3.2.1. CM-types. The field K has $2g$ embeddings in $\mathbf{C}$ which we denote $\varphi_1, \ldots, \varphi_{2g}$. An endomorphism of $\mathscr{A}_\mathbf{C}$ yields an endomorphism of $\mathbf{C}^g$ and of Λ. We get an analytic representation $\rho_a \colon \mathrm{End}(\mathscr{A}_\mathbf{C}) \to \mathrm{End}_\mathbf{C}(\mathbf{C}^g)$ and a rational representation $\rho_r \colon \mathrm{End}(\mathscr{A}_\mathbf{C}) \to \mathrm{End}_\mathbf{Z}(\Lambda)$. We have $\rho_r \otimes \mathbf{C} \sim \rho_a \oplus \overline{\rho}_a$ and at the same time, $\rho_r \otimes \mathbf{C} \sim \varphi_1 \oplus \cdots \oplus \varphi_{2g}$. It follows that, up to some reindexing, $\rho_a = \varphi_1 \oplus \cdots \oplus \varphi_g$ where $\varphi_1, \ldots, \varphi_g$ are not pairwise conjugate. We call $(K; \{\varphi_1, \ldots, \varphi_g\})$ the CM-type of $\mathscr{A}_\mathbf{C}$. The abelian variety $\mathscr{A}_\mathbf{C}$ is simple if and only if its CM-type is *primitive*, which means that $(K; \{\varphi_1, \ldots, \varphi_g\})$ is not a lift of a CM-type on a CM-subfield of K (see [ST61, Section 8.2]).

Remark 3.9. If $g = 2$, the abelian surface $\mathscr{A}_\mathbf{C}$ is simple if and only if the field K is a primitive CM-field, i.e., K does not have any proper CM-subfield. This follows from [Str10, Lemma I.3.4].

Fix a CM-type $\Phi = \{\varphi_1, \dots, \varphi_g\}$ for K. Any abelian variety over $\mathbf{C}$ of CM-type $(K;\Phi)$ is isomorphic to $\mathbf{C}^g/\Phi(\mathfrak{m})$ for some full-rank lattice $\mathfrak{m}$ in K, where the embedding $\Phi\colon K \to \mathbf{C}^g$ is given by $x \mapsto (\varphi_1(x), \dots, \varphi_g(x))$. Let $\mathcal{O}$ be the order of K isomorphic to the endomorphism ring of the variety. Then, the lattice $\mathfrak{m}$ is an $\mathcal{O}$-submodule of K, and $\mathcal{O}$ coincides with the order $\mathcal{O}(\mathfrak{m})$ associated to the lattice,

$$\mathcal{O}(\mathfrak{m}) = \{\alpha \in K \mid \alpha\mathfrak{m} \subset \mathfrak{m}\}.$$

Given an invertible ideal $\mathfrak{a}$ in $\mathcal{O}$, the variety $\mathbf{C}^g/\Phi(\mathfrak{a}^{-1}\mathfrak{m})$ is isogenous to $\mathbf{C}^g/\Phi(\mathfrak{m})$. This construction actually coincides with the action of ideals presented in Section 3.1.3: the abelian variety $\mathbf{C}^g/\Phi(\mathfrak{a}^{-1}\mathfrak{m})$ is the $\mathfrak{a}$-transform of $\mathbf{C}^g/\Phi(\mathfrak{m})$. Again, it induces a free action of the ideal class group $\mathrm{Cl}(\mathcal{O})$ on the set of isomorphism classes of abelian varieties of CM-type $(K;\Phi)$ with endomorphism ring $\mathcal{O}$.

When the order $\mathcal{O}$ is a Gorenstein ring, any lattice $\mathfrak{m}$ with $\mathcal{O}(\mathfrak{m}) = \mathcal{O}$ is an invertible fractional ideal of $\mathcal{O}$ (see for instance [JT15, Theorem 4.3]), which implies that this free action of $\mathrm{Cl}(\mathcal{O})$ is also transitive.

Definition 3.10 (Gorenstein ring)**.** A commutative Noetherian local ring R is *Gorenstein* if it has finite injective dimension as an R-module. A commutative Noetherian ring is *Gorenstein* if each localisation at a prime ideal is a Gorenstein local ring.

3.2.2. Polarisations and the Shimura class group. A polarisation on an abelian variety X over a field k is an ample line bundle $\mathcal{L}_X$ on X. Associated to such $\mathcal{L}_X$ is the polarisation isogeny $\varphi_{\mathcal{L}_X}\colon X \to X^\vee$, where $X^\vee$ is the dual of X. A principal polarisation is an ample line bundle of degree one (equivalently, the polarisation isogeny is an isomorphism).

Example 3.11. If $\mathscr{A}_{\mathbf{C}}$ is a simple abelian surface, $\mathscr{A}_{\mathbf{C}}$ is principally polarisable if and only if it is the Jacobian of a smooth genus 2 curve (see [DM02, Theorem 4.1]).

In the remainder of this paragraph, we shall restrict to abelian varieties which are simple, or equivalently, to primitive CM-types $(K;\Phi)$. If $X = \mathscr{A}_{\mathbf{C}}$, a simple complex abelian variety with endomorphism ring an order $\mathcal{O}$ in K, the theory of Taniyama and Shimura [ST61, Section 14] which we now briefly recall provides an explicit description of the polarisations on X in terms of the arithmetic of K. Indeed, by the theory of complex multiplication, there exists a full-rank lattice $\mathfrak{m}$ in K such that $X(\mathbf{C}) \cong \mathbf{C}^g/\Phi(\mathfrak{m})$. The dual abelian variety of $\mathbf{C}^g/\Phi(\mathfrak{m})$ is $\mathbf{C}^g/\Phi(\mathfrak{m}^*)$ where

$$\mathfrak{m}^* = \{\beta \in K\colon \mathrm{Tr}_{K/\mathbf{Q}}(\beta\overline{\mathfrak{m}}) \subset \mathbf{Z}\}.$$

Given a polarisation $\mathcal{L}$ on $\mathbf{C}^g/\Phi(\mathfrak{m})$ the corresponding polarisation isogeny is the isogeny $\varphi_{\mathcal{L}}\colon \mathbf{C}^g/\Phi(\mathfrak{m}) \to \mathbf{C}^g/\Phi(\mathfrak{m}^*)$ given by $x \mapsto \rho_a(\xi)x$ for some purely imaginary element $\xi \in K$ that satisfies $\Phi(\xi) \in (i\mathbf{R}_{>0})^g$. The polarisation is also described by the Riemann form $E(x,y) = \mathrm{Tr}_{K/\mathbf{Q}}(\xi\overline{x}y)$. The polarisation is principal if and only if $\varphi_{\mathcal{L}}(\Phi(\mathfrak{m})) = \Phi(\mathfrak{m}^*)$, i.e., if and only if $\xi\mathfrak{m} = \mathfrak{m}^*$. Thus, the CM-type $(K;\Phi)$ being fixed, a principally polarised abelian variety $(\mathscr{A}_{\mathbf{C}}, \mathcal{L})$ is determined by the associated pair $(\mathfrak{m}, \xi)$, which satisfies $\xi\mathfrak{m} = \mathfrak{m}^*$. The *Shimura class group* of $\mathcal{O}$, acts on such pairs. It is defined as

$$\mathfrak{C}(\mathcal{O}) = \{(\mathfrak{a}, \alpha) \mid \mathfrak{a} \in \mathscr{I}(\mathcal{O}) \text{ and } \mathfrak{a}\overline{\mathfrak{a}} = \alpha\mathcal{O}, \alpha \in K^+ \text{ totally positive}\}/\sim$$

with componentwise multiplication, where two pairs $(\mathfrak{a}, \alpha)$ and $(\mathfrak{b}, \beta)$ are equivalent for the relation $\sim$ if there exists an element $u \in K^\times$ such that $\mathfrak{b} = u\mathfrak{a}$ and $\beta = u\overline{u}\alpha$. For any $(\mathfrak{a}, \alpha) \in \mathfrak{C}(\mathcal{O})$ (up to equivalence), the pair $(\mathfrak{a}^{-1}\mathfrak{m}, \alpha\xi)$ corresponds to a principally polarised abelian variety isogenous to $\mathscr{A}_{\mathbf{C}}$ and with same endomorphism ring $\mathcal{O}$ (and this action of $\mathfrak{C}(\mathcal{O})$ is well defined on isomorphism classes). This action of $\mathfrak{C}(\mathcal{O})$ is in fact

free on the set of isomorphism classes of principally polarised abelian varieties isogenous to $\mathscr{A}_{\mathbf{C}}$ with same endomorphism ring [ST61, Section 17]. The structure of $\mathfrak{C}(\mathcal{O})$ and its relation to $\mathrm{Cl}(\mathcal{O})$ is described by the exact sequence

$$1 \longrightarrow \mathrm{TP}(\mathcal{O})/N_{K/K^+}(\mathcal{O}^\times) \xrightarrow{u\mapsto(\mathcal{O},u)} \mathfrak{C}(\mathcal{O}) \xrightarrow{(\mathfrak{a},\alpha)\mapsto\mathfrak{a}} \mathrm{Cl}(\mathcal{O}) \xrightarrow{N_{K/K^+}} \mathrm{Cl}^+(\mathcal{O}^+), \tag{3.1}$$

where $\mathcal{O}^+ = \mathcal{O} \cap K^+$, $\mathrm{TP}(\mathcal{O})$ is its multiplicative subgroup of totally positive units, and $\mathrm{Cl}^+(\mathcal{O}^+)$ its narrow class group, and N_{K/K^+} is the norm from K to K^+. The image of the projection $\mathfrak{C}(\mathcal{O}) \to \mathrm{Cl}(\mathcal{O})$, denoted $\mathscr{P}(\mathcal{O})$, is a subgroup of $\mathrm{Cl}(\mathcal{O})$ that acts freely on the set of principally *polarisable* abelian varieties isogenous to $\mathscr{A}_{\mathbf{C}}$ with endomorphism ring $\mathcal{O}$. Notice the crucial distinction between polarised and polarisable. The amount of information lost with the polarisation is encoded in the group

$$U(\mathcal{O}) = \mathrm{TP}(\mathcal{O})/N_{K/K^+}(\mathcal{O}^\times).$$

Indeed, given a principally polarisable $\mathscr{A}_{\mathbf{C}}$, the set of isomorphism classes of principal polarisations on $\mathscr{A}_{\mathbf{C}}$ is a torsor for the group $U(\mathcal{O})$. The following lemma recalls some well-known facts about $U(\mathcal{O})$. It is originally part of the article [BJW17], which is the object of Chapter 5, but is relocated here as it is already useful in the present chapter.

Lemma 3.12. *The group $U(\mathcal{O})$ is an $\mathbf{F}_2$-vector space of dimension d, where $d \leq g-1$. If $\mathcal{O} \subset \mathcal{O}'$ and $\mathcal{O} \cap K^+ = \mathcal{O}' \cap K^+$, then the natural map $U(\mathcal{O}) \to U(\mathcal{O}')$ is surjective.*

Proof. We have the following hierarchy, the last containment following because for any element $\beta \in \mathcal{O} \cap K^+$ one has $\beta^2 = N_{K/K^+}(\beta)$:

$$(\mathcal{O} \cap K^+)^\times \supseteq \mathrm{TP}(\mathcal{O}) \supseteq N_{K/K^+}(\mathcal{O}^\times) \supseteq \left((\mathcal{O} \cap K^+)^\times\right)^2. \tag{3.2}$$

By Dirichlet's unit theorem (and its extension to non-maximal orders), the group of units $(\mathcal{O} \cap K^+)^\times$ is of the form $\{\pm 1\} \times A$, where A is a free abelian group of rank $g-1$, so the quotient $(\mathcal{O} \cap K^+)^\times/(\mathcal{O} \cap K^+)^{\times 2}$ is an $\mathbf{F}_2$-vector space of dimension at most g. Since -1 is never a totally positive unit, the first claim follows. The second sentence of the lemma is clear. □

Remark 3.13. The inequalities in the chain (3.2) are in general difficult to control. For example, if $g = 2$, the total index in (3.2) is 4. The factor $\{\pm 1\}$ accounts for a factor 2 of this index, and so exactly one of the other three containments must be non-trivial; for each containment, one has examples where it is non-strict. In any case, we get that for orders in quartic CM-fields, $U(\mathcal{O})$ is either trivial, in which case $\mathfrak{C}(\mathcal{O})$ and $\mathscr{P}(\mathcal{O})$ are isomorphic and no information is lost with the polarisation, or it is of order two, in which case the abelian surfaces encoded in $\mathscr{P}(\mathcal{O})$ each have two possible polarisations.

From the exactness of Sequence 3.1, the subgroup $\mathscr{P}(\mathcal{O})$ is also the kernel of N_{K/K^+}. The following lemma extends the result of [BGL11, Theorem 3.1] to higher dimensions, and non-maximal orders.

Lemma 3.14. *Let K be a CM-field and K^+ its maximal real subfield. Let $\mathcal{O}$ be an order in K of conductor $\mathfrak{f}$, and $\mathcal{O}^+ = \mathcal{O} \cap K^+$. The image of $\mathrm{Cl}(\mathcal{O})$ through the norm map $N_{K/K^+} : \mathrm{Cl}(\mathcal{O}) \to \mathrm{Cl}^+(\mathcal{O}^+)$ is of index at most 2 in $\mathrm{Cl}^+(\mathcal{O}^+)$. If there is a prime in K^+ that ramifies in K and does not divide $\mathfrak{f}$, the norm map N_{K/K^+} is surjective.*

Proof. We use the elements of class field theory recalled in Section 3.1.5. Let $H = H(\mathcal{O})$ and $H^+ = H^+(\mathcal{O}^+)$. The compositum KH^+ is a subfield of H, so we have a natural surjection $\mathrm{Gal}(H/K) \to \mathrm{Gal}(KH^+/K)$. From Galois theory, $\mathrm{Gal}(KH^+/K)$

is isomorphic to $\mathrm{Gal}(H^+/(K\cap H^+))$, which in turn is isomorphic to the quotient $\mathrm{Gal}(H^+/K^+)/\mathrm{Gal}((K\cap H^+)/K^+)$. Let $N=\mathrm{Gal}((K\cap H^+)/K^+)$. Then,

$$\begin{aligned}\psi : \mathrm{Gal}(H/K) &\longrightarrow \mathrm{Gal}(H^+/K^+)/N\\ \sigma &\longmapsto \sigma\mid_{H^+} \mod N\end{aligned}$$

is the composition of these canonical maps, and is therefore a surjection. Through the Artin map, the norm N_{K/K^+} commutes with ψ. We conclude that the image of $\mathrm{Cl}(\mathcal{O})$ through N_{K/K^+} is a subgroup of $\mathrm{Cl}^+(\mathcal{O}^+)$ of index at most $|N|\leq 2$. If there is a prime in K^+ that ramifies in K and does not divide $\mathfrak{f}$, then $K\cap H^+=K^+$, so $|N|=1$ and the map N_{K/K^+} is surjective. □

In particular, this lemma implies that the index $[\mathrm{Cl}(\mathcal{O}):\mathscr{P}(\mathcal{O})]$ is either the narrow class number $h^+_{\mathcal{O}^+}=|\mathrm{Cl}^+(\mathcal{O}^+)|$, or $h^+_{\mathcal{O}^+}/2$. It is exactly $h^+_{\mathcal{O}^+}$ whenever there is a prime in the field K^+ that ramifies in K and does not divide $\mathfrak{f}$. As observed in [BGL11, Theorem 3.1], there exists such a prime when $\mathcal{O}$ is the maximal order in a primitive quartic CM-field.

3.2.3. Canonical lifting. Recall that our objects of primary interest are varieties defined over a finite field $\mathbf{F}_q$. The theory of canonical lifting of Serre and Tate [ST68] allows us to lift an ordinary abelian variety $\mathscr{A}/\mathbf{F}_q$ to an abelian variety $\tilde{\mathscr{A}}$ over $W(\mathbf{F}_q)$, the ring of Witt vectors of $\mathbf{F}_q$ in such a way that all endomorphisms of $\mathscr{A}$ lift to endomorphisms of $\tilde{\mathscr{A}}$, and $\mathscr{A}\mapsto\tilde{\mathscr{A}}$ is functorial. To obtain lifts from abelian varieties over $\mathbf{F}_q$ to abelian varieties over $\mathbf{C}$, we fix an embedding $\imath\colon W(\overline{\mathbf{F}}_q)\hookrightarrow\mathbf{C}$ and let $\mathscr{A}_{\mathbf{C}}$ be the complex abelian variety $\tilde{\mathscr{A}}\otimes_\imath\mathbf{C}$. If $T(\mathscr{A})=H_1(\mathscr{A}_{\mathbf{C}},\mathbf{Z})$ then $T(\mathscr{A})$ is a free $\mathbf{Z}$-module of rank $2\cdot\dim(\mathscr{A})$. The correspondence $\mathscr{A}\mapsto T(\mathscr{A})$ is functorial and any isogeny $\varphi\colon\mathscr{A}\to\mathscr{B}$ over $\overline{\mathbf{F}}_q$ gives rise to a short exact sequence

$$0\longrightarrow T(\mathscr{A})\xrightarrow{T(\varphi)}T(\mathscr{B})\longrightarrow\ker(\varphi)\longrightarrow 0.$$

A theorem of Deligne [Del69, Theorem 7] says that if π is the Frobenius endomorphism of $\mathscr{A}$ over $\mathbf{F}_q$ then the functor $\mathscr{A}\mapsto(T(\mathscr{A}),T(\pi))$ is an equivalence of categories between the category of ordinary abelian varieties over $\mathbf{F}_q$ and the category of free $\mathbf{Z}$-modules T endowed with an endomorphism F satisfying

(1) F is semi-simple, with eigenvalues of complex absolute value $\sqrt{q}$,
(2) at least half the roots in $\overline{\mathbf{Q}}_p$ of the characteristic polynomial of F are p-adic units, and
(3) there is an endomorphism V of T such that $FV=q$.

As discussed in [Del69, Section 8], any such (T,F) that is the image of a variety $\mathscr{A}$ through this functor determines the complex abelian variety $\mathscr{A}_{\mathbf{C}}$ up to isomorphism as $\mathscr{A}_{\mathbf{C}}\cong(T\otimes\mathbf{R})/T$ (with a complex structure on $T\otimes\mathbf{R}$ such that F is $\mathbf{C}$-linear; the existence and uniqueness of the appropriate complex structure is established by a theorem of Serre [Del69, Section 8]). This means that up to isomorphism, we can write $\mathscr{A}_{\mathbf{C}}=\mathbf{C}^g/\Lambda$, for a lattice Λ in $\mathbf{C}^g$ and since lifting preserves the endomorphism ring $\mathcal{O}=\mathrm{End}(\mathscr{A})$, we even have $\mathscr{A}_{\mathbf{C}}=\mathbf{C}^g/\Phi(\mathfrak{m})$ for some full-rank lattice $\mathfrak{m}$ in K with order $\mathcal{O}(\mathfrak{m})=\mathcal{O}$, where, as above, the map $\Phi\colon K\to\mathbf{C}^g$ is the CM-type of $\mathscr{A}_{\mathbf{C}}$. From the canonical identification between $\Phi(\mathfrak{m})$ and $H_1(\mathscr{A}_{\mathbf{C}},\mathbf{Z})$ (see [BL04, Section 1.1]), the functor can be interpreted as $\mathscr{A}\mapsto(\Phi(\mathfrak{m}),\rho_r(\pi))$. This establishes a functorial map from the abelian varieties over $\mathbf{F}_q$ of fixed endomorphism ring $\mathcal{O}$ to the complex abelian varieties $\mathbf{C}^g/\Phi(\mathfrak{m})$ where $\mathfrak{m}$ are lattices in K with order $\mathcal{O}(\mathfrak{m})=\mathcal{O}$. Conversely, Deligne's theorem shows that any such $\mathbf{C}^g/\Phi(\mathfrak{m})$ is the lift of an abelian variety over $\mathbf{F}_q$ with

endomorphism ring $\mathcal{O}$: the variety corresponding to the pair $(\Phi(\mathfrak{m}), \rho_r(\pi))$, where $\rho_r(\pi)$ is the rational representation of π. Moreover, from [Del69, Section 3], the polarisations also lift properly. In particular $\mathscr{A}$ is principally polarisable if and only if $\mathscr{A}_{\mathbf{C}}$ is, and the Shimura class group $\mathfrak{C}(\mathcal{O})$ acts on varieties over $\mathbf{F}_q$ just as it acts on varieties over $\mathbf{C}$. See [How95] for a more detailed treatment of polarisations through Deligne's equivalence.

Example 3.15 (Horizontal isogeny graph of principally polarisable abelian varieties over a finite field)**.** If $\mathscr{A}$ is a principally polarisable abelian variety over a finite field, and $H = \mathscr{P}(\mathcal{O})$, the orbit $H(\mathscr{A})$ (in this case also denoted $\mathscr{P}(\mathscr{A})$) is a set of isomorphism classes of principally polarisable abelian varieties isogenous to $\mathscr{A}$ and with same endomorphism ring. Via the construction described above, any choice of a generating set of $\mathscr{P}(\mathcal{O})$ yields a graph of the set of vertices $\mathscr{P}(\mathscr{A})$. Whenever $\mathscr{A}$ has maximal real multiplication (i.e., $\mathcal{O}_{K^+} \subset \mathcal{O}$), the endomorphism ring $\mathcal{O}$ is Gorenstein, so the action of $\mathrm{Cl}(\mathcal{O})$ is transitive on the set of *all* abelian varieties isogenous to $\mathscr{A}$ and with same endomorphism ring. We can conclude via [ST61, Section 17] that when $\mathscr{A}$ has maximal real multiplication, the orbit $\mathscr{P}(\mathscr{A})$ is exactly the set of all isomorphism classes of principally polarisable abelian varieties isogenous to $\mathscr{A}$ and with same endomorphism ring.

3.3. Expander graphs and ray class groups

We have seen that horizontal isogeny graphs are isomorphic to certain Cayley graphs of class groups of orders in number fields, or subgroups thereof. In this section, we shift our attention to these Cayley graphs, and show that they are expander graphs, i.e., they are strongly connected, and rapidly mix random walks.

3.3.1. Eigenvalues and Cayley graphs. Let $\mathscr{G}$ be an undirected (multi)graph with set of vertices $\mathcal{V}$ and set of edges $\mathcal{E}$. Suppose $\mathscr{G}$ is finite and k-regular, i.e., each vertex has k incident edges. The *adjacency operator* A of $\mathscr{G}$ is the operator defined for any function f from $\mathcal{V}$ to $\mathbf{C}$ by

$$Af(x) = \sum_{y \in \mathcal{N}_{\mathscr{G}}(x)} f(y),$$

for any $x \in \mathcal{V}$, where $\mathcal{N}_{\mathscr{G}}(x)$ denotes the (multi)set of neighbors of x in $\mathscr{G}$. This operator is represented by the adjacency matrix of $\mathscr{G}$ with respect to the basis $\{\mathbf{1}_{\{x\}} : x \in \mathcal{V}\}$, where $\mathbf{1}_S$ denotes the characteristic function of a set S. It is a real symmetric matrix, so by the spectral theorem, A has $n = |\mathcal{V}|$ real eigenvalues $\lambda_1 \geq \lambda_2 \geq ... \geq \lambda_n$. Since the graph is k-regular, the constant function $\mathbf{1}_{\mathcal{V}} : x \mapsto 1$ is an eigenvector with eigenvalue k. We call k the *trivial eigenvalue*, and denote it by λ_{triv}. This λ_{triv} is the largest eigenvalue in absolute value, i.e., $\lambda_1 = k$, and its multiplicity is the number of connected components of $\mathscr{G}$.

Definition 3.16 (Expander graph)**.** Let $\delta > 0$. The k-regular graph $\mathscr{G}$ is *(one-sided) δ-expander* if $\lambda_2 \leq (1-\delta)\lambda_{\mathrm{triv}}$. It is a *two-sided δ-expander* if the stronger bound $|\lambda_2| \leq (1-\delta)\lambda_{\mathrm{triv}}$ holds.

Observe that such a graph is connected whenever $\delta > 0$. The main reason for our interest in expander graphs is that they rapidly mix random walks. The following lemma is a classical result on expander graphs and can be found in, e.g., [JMV09].

Lemma 3.17. *Let $\mathscr{G}$ be a finite k-regular graph. Suppose the trivial eigenvalue has multiplicity one and the non-trivial eigenvalues λ of the adjacency operator A satisfy the bound $|\lambda| \leq c$, for some $c < k$. Let S be a subset of the vertices of $\mathscr{G}$, and v a*

vertex of $\mathscr{G}$. Any random walk from v of length at least $\frac{\log(2|\mathscr{G}|/|S|^{1/2})}{\log(k/c)}$ will end in S with probability between $\frac{1}{2}\frac{|S|}{|\mathscr{G}|}$ and $\frac{3}{2}\frac{|S|}{|\mathscr{G}|}$.

For any finite group G and generating set S with $S = S^{-1}$, observe that a character $\chi : G \to \mathbf{C}^*$ is an eigenvector for the adjacency operator A on $\mathrm{Cay}(G, S)$. Indeed,

$$A\chi(x) = \sum_{s\in S} \chi(sx) = \sum_{s\in S} \chi(s)\chi(x) = \lambda_\chi \chi(x), \text{ where } \lambda_\chi = \sum_{s\in S} \chi(s).$$

If G is abelian, these characters form a basis of the $\mathbf{C}$-vector space of functions of G. In particular, any eigenvalue is of the form λ_χ for some character χ. The trivial eigenvalue corresponds to the trivial character $\mathbf{1}_G$.

3.3.2. Cayley graphs of subgroups of ray class groups. We prove in this section that Cayley graphs of subgroups of narrow ray class groups, with generators the classes of ideals of bounded prime norm, are expander graphs. We start by giving bounds on the eigenvalues of the graph, in Theorem 3.18. Note that a similar result is proven in [JMV09] for the full narrow ray class group, rather than a subgroup. It was sufficient for studying isogeny graphs of elliptic curves, which can be represented as Cayley graphs of class groups in imaginary quadratic fields. However, that result is not strong enough for higher dimensions, where one might need to work on subgroups to account for the extra condition of principal polarisability. Since properties of expander graphs do not transfer nicely to subgraphs in general, the refinement provided by Theorem 3.18 is crucial.

Theorem 3.18. *Consider a number field K of degree n and discriminant d_K, and an integral ideal $\mathfrak{m}$ of $\mathcal{O}_K$. Let G be the narrow ray class group of K modulo $\mathfrak{m}$, and consider a subgroup H of G. For any ideal $\mathfrak{l}$ of $\mathcal{O}_K$ coprime to $\mathfrak{m}$, let $[\mathfrak{l}]$ denote its image in G. Let*

$$\mathcal{T}_{H,\mathfrak{m}}(B) = \{\text{prime ideals } \mathfrak{l} \text{ of } \mathcal{O}_K \mid (\mathfrak{l}, \mathfrak{m}) = 1, N(\mathfrak{l}) \leq B \text{ is prime and } [\mathfrak{l}] \in H\}.$$

Let $T_{H,\mathfrak{m}}(B)$ be the multiset of the projection of $\mathcal{T}_{H,\mathfrak{m}}(B)$ in G. Let $\mathscr{G}_B$ be the graph whose vertices are the elements of H and whose non-oriented edges are precisely (h, sh) for any $h \in H$ and $s \in T_{H,\mathfrak{m}}(B)$. Assuming the extended Riemann hypothesis, for any character χ of H, the corresponding eigenvalue λ_χ of the Cayley graph $\mathscr{G}_B$ satisfies

$$\lambda_\chi = \frac{2\delta(\chi)}{[G : H]}\mathrm{li}(B) + O\left(nB^{1/2}\log(Bd_K N(\mathfrak{m}))\right),$$

where $\delta(\chi)$ is 1 if χ is trivial, and 0 otherwise, and li *denotes the logarithmic integral. The implied constants are absolute.*

Proof. Since G is abelian, any character χ of H can be extended to a character of G. Take any such extension and, by abuse of notation, also denote it by χ. Note that for any ideal $\mathfrak{l}$ of $\mathcal{O}_K$ coprime to $\mathfrak{m}$, we have

$$\sum_{\theta\in\widehat{G/H}} \theta([\mathfrak{l}]H) = \begin{cases} [G : H] & \text{if } [\mathfrak{l}] \in H, \\ 0 & \text{otherwise,} \end{cases}$$

where $\widehat{G/H} = \mathrm{Hom}(G/H, \mathbf{C}^*)$ is the character group of the quotient G/H. Therefore this sum can be used to filter the condition that $[\mathfrak{l}] \in H$, and we can rewrite

$$\begin{aligned}\lambda_\chi &= \sum_{\mathfrak{l}\in\mathcal{T}_{H,\mathfrak{m}}(B)} \left(\chi([\mathfrak{l}]) + \chi([\mathfrak{l}])^{-1}\right) \\ &= \frac{2}{[G:H]}\mathfrak{Re}\left(\sum_{\substack{\mathfrak{l}:N(\mathfrak{l})<B \text{ prime}\\(\mathfrak{l},\mathfrak{m})=1}} \chi([\mathfrak{l}]) \sum_{\theta\in\widehat{G/H}} \theta([\mathfrak{l}]H)\right) \\ &= \frac{2}{[G:H]}\mathfrak{Re}\left(\sum_{\theta\in\widehat{G/H}} \sum_{\substack{\mathfrak{l}:N(\mathfrak{l})<B \text{ prime}\\(\mathfrak{l},\mathfrak{m})=1}} \chi([\mathfrak{l}])\theta([\mathfrak{l}]H)\right).\end{aligned}$$

We are then left with estimating a character sum $\sum \chi([\mathfrak{l}])\theta([\mathfrak{l}]H)$. Each of the summands of the latter defines a multiplicative function

$$\nu_{\chi,\theta}\colon \mathscr{I}_{\mathfrak{m}}(K) \longrightarrow \mathbf{C}^* : \mathfrak{l} \longmapsto \chi([\mathfrak{l}])\theta([\mathfrak{l}]H)$$

where $\mathscr{I}_{\mathfrak{m}}(K)$ is the group of fractional ideals of K coprime to $\mathfrak{m}$. It extends to a function of $\mathscr{I}(K)$, the group of all the fractional ideals of K, by setting $\nu_{\chi,\theta}(\mathfrak{l}) = 0$ for all prime divisors $\mathfrak{l}$ of $\mathfrak{m}$ (notice that it might not be the unique way to extend it, but this is not an issue: we do not require the characters to be primitive). The expression of λ_χ becomes

$$\lambda_\chi = \frac{2}{[G:H]}\mathfrak{Re}\left(\sum_{\theta\in\widehat{G/H}} \sum_{\mathfrak{l}:N(\mathfrak{l})<B \text{ prime}} \nu_{\chi,\theta}(\mathfrak{l})\right). \tag{3.3}$$

From the classical estimate that can be found in [IK04, Theorem 5.15], the extended Riemann hypothesis implies that

$$\sum_{\mathfrak{a}:N(\mathfrak{a})<B} \Lambda(\mathfrak{a})\nu_{\chi,\theta}(\mathfrak{a}) = \delta(\nu_{\chi,\theta})B + O\left(nB^{1/2}\log(B)\log(Bd_KN(\mathfrak{m}))\right),$$

where Λ is the von Mangoldt function (i.e., $\Lambda(\mathfrak{a})$ is $\log(N(\mathfrak{l}))$ if $\mathfrak{a}$ is a power of a prime ideal $\mathfrak{l}$, and 0 otherwise), and $\delta(\nu_{\chi,\theta})$ is 1 if $\nu_{\chi,\theta}$ is principal, and 0 otherwise (a principal character is a character that only takes the values 1 or 0). Observe that if $\nu_{\chi,\theta}$ is principal, then χ must be the trivial character, so that $\delta(\nu_{\chi,\theta}) = \delta(\chi)\delta(\theta)$. Indeed, suppose that $\nu_{\chi,\theta}$ is principal, and let $[\mathfrak{l}] \in H$, for a prime $\mathfrak{l}$ coprime to $\mathfrak{m}$. Then,

$$1 = \nu_{\chi,\theta}(\mathfrak{l}) = \chi([\mathfrak{l}])\theta([\mathfrak{l}]H) = \chi([\mathfrak{l}])\theta(1_{G/H}) = \chi([\mathfrak{l}]),$$

so χ must be the trivial character of H.

We now want to replace each instance of $\Lambda(\mathfrak{a})$ in the above sum by $P(\mathfrak{a})$, where

$$P(\mathfrak{a}) = \begin{cases}\log(N(\mathfrak{a})) & \text{if } N(\mathfrak{a}) \text{ is prime,}\\ 0 & \text{otherwise.}\end{cases}$$

To do so, it is sufficient to prove that

$$\sum_{\mathfrak{a}:N(\mathfrak{a})<B} \Lambda(\mathfrak{a})\nu_{\chi,\theta}(\mathfrak{a}) - \sum_{\mathfrak{a}:N(\mathfrak{a})<B} P(\mathfrak{a})\nu_{\chi,\theta}(\mathfrak{a}) = O\left(nB^{1/2}\right). \tag{3.4}$$

The non-zero terms $(\Lambda(\mathfrak{a}) - P(\mathfrak{a}))\nu_{\chi,\theta}(\mathfrak{a})$ correspond to ideals $\mathfrak{a}$ which are powers of a prime ideal $\mathfrak{l}$, and $N(\mathfrak{a}) = N(\mathfrak{l})^k$ is not a prime number — but it is a power of a prime ℓ.

Since K is of degree n, there are at most n different prime ideals $\mathfrak{l}$ above any given prime number ℓ. Therefore the difference (3.4) is bounded in absolute value by

$$n \sum_{\substack{\ell^k < B \\ k \geq 2}} \log(\ell) = n \sum_{\substack{\ell < B^{1/2} \\ 2 \leq k < \frac{\log(B)}{\log(\ell)}}} \log(\ell) \leq n \sum_{\ell < B^{1/2}} \log(\ell) \frac{\log(B)}{\log(\ell)} = n\pi(B^{1/2}) \log(B),$$

which, by the Prime Number Theorem, is $O(nB^{1/2})$. Therefore,

$$\sum_{\mathfrak{a}: N(\mathfrak{a}) < B} P(\mathfrak{a}) \nu_{\chi,\theta}(\mathfrak{a}) = \delta(\nu_{\chi,\theta}) B + O\left(nB^{1/2} \log(B) \log(B d_K N(\mathfrak{m}))\right).$$

Applying the Abel partial summation formula, we derive that

$$\sum_{\mathfrak{l}: N(\mathfrak{l}) < B \text{ prime}} \nu_{\chi,\theta}(\mathfrak{l}) = \delta(\nu_{\chi,\theta}) \mathrm{li}(B) + O\left(nB^{1/2} \log(B d_K N(\mathfrak{m}))\right).$$

Replacing this into the expression (3.3) of λ_χ, we finally obtain

$$\lambda_\chi = \frac{2\delta(\chi)}{[G : H]} \mathrm{li}(B) + O\left(nB^{1/2} \log(B d_K N(\mathfrak{m}))\right),$$

which proves the theorem. □

Consider a number field K of degree n, an order $\mathcal{O}$ of conductor $\mathfrak{f}$ in K, and any subgroup H of $\mathrm{Cl}(\mathcal{O})$. Let $B > 0$, and $\mathfrak{a}$ an integral ideal of $\mathcal{O}_K$, and define the following set of ideals of $\mathcal{O}_K$,

$$\mathcal{S}_B = \{\mathfrak{l} \mid N(\mathfrak{l}) < B \text{ is prime}, (\mathfrak{l}, \mathfrak{f}\mathfrak{a}) = 1, \text{ and } [\mathfrak{l} \cap \mathcal{O}] \in H\},$$

where $[\mathfrak{l} \cap \mathcal{O}]$ is the class in $\mathrm{Cl}(\mathcal{O})$. Let S_B be the multiset of the image of $\mathcal{S}_B$ in the class group, plus the inverses. Using Theorem 3.18, one can bound the spectral gap of $\mathscr{G}_B = \mathrm{Cay}(H, S_B)$.

Theorem 3.19. *For any character χ of H,the corresponding eigenvalue of $\mathscr{G}_B$ is*

$$\lambda_\chi = \frac{2\delta(\chi)}{[\mathrm{Cl}(\mathcal{O}) : H]} \mathrm{li}(B) + O(nB^{1/2} \log(B d_K N(\mathfrak{f}\mathfrak{a}))),$$

where $\delta(\chi)$ if 1 if χ is trivial, and 0 otherwise.

Proof. Using the notations from Section 3.1.5, the group $P^{\mathfrak{f}}_{K,1}$ is a subgroup of $P^{\mathfrak{f}}_{K,\mathcal{O}}$, so there is a natural surjection $\mathrm{Cl}_{\mathfrak{f}}(K) \to \mathrm{Cl}(\mathcal{O})$. Furthermore, the canonical injection of $\mathscr{I}_{\mathfrak{f}\mathfrak{a}}(K)$ in $\mathscr{I}_{\mathfrak{f}}(K)$ induces a surjection from $\mathrm{Cl}_{\mathfrak{f}\mathfrak{a}}(K)$ to $\mathrm{Cl}_{\mathfrak{f}}(K)$. Therefore we have a natural surjection $\pi : G \to \mathrm{Cl}(\mathcal{O})$, where G is the narrow ray class group of K modulo $\mathfrak{f}\mathfrak{a}$, which sends the class of any integral ideal $\mathfrak{b}$ of $\mathcal{O}_K$ to the class of $\mathfrak{b} \cap \mathcal{O}$. Consider the subgroup $\widetilde{H} = \pi^{-1}(H)$ of G, and its Cayley graph $\widetilde{\mathscr{G}_B} = \mathrm{Cay}(\widetilde{H}, T_{\widetilde{H},\mathfrak{f}\mathfrak{a}}(B))$ where $T_{\widetilde{H},\mathfrak{f}\mathfrak{a}}(B)$ is the multiset defined in the statement of Theorem 3.18. The Cayley graph $\mathscr{G}_B$ on H is the image of the Cayley graph $\widetilde{\mathscr{G}_B}$ on $\widetilde{H}$ via the projection π, taking into account the multiplicity of the edges. The eigenvalues of $\mathscr{G}_B$ are exactly the eigenvalues λ_θ of $\widetilde{\mathscr{G}_B}$ corresponding to characters θ of $\widetilde{H}$ that are trivial on the kernel of $\pi|_{\widetilde{H}} : \widetilde{H} \to H$. The result follows by applying Theorem 3.18 to $\widetilde{\mathscr{G}_B}$. □

Corollary 3.20. *For any $0 < \delta < 1$ and $\varepsilon > 0$, there is a function*

$$B_{\delta,\varepsilon}(H, \mathfrak{a}) = O\left((n[\mathrm{Cl}(\mathcal{O}) : H] \log(d_K N(\mathfrak{f}\mathfrak{a})))^{2+\varepsilon}\right),$$

such that $\mathscr{G}_{B_{\delta,\varepsilon}(H,\mathfrak{a})}$ is a two-sided δ-expander.

Proof. Let $x > 0$, and write $k = [\mathrm{Cl}(\mathcal{O}) : H]$. The graph $\mathscr{G}_x$ is a two-sided δ-expander if $|\lambda_\chi| \leq (1-\delta)\lambda_{\mathrm{triv}}$ for any non-trivial character χ. From Theorem 3.19, and the fact that $\mathrm{li}(x) \sim x/\log(x)$ and $\mathrm{li}(x) \geq x/\log(x)$ for any $x \geq 4$, there are absolute constants C and D such that for any $x \geq C$, we have

$$\lambda_{\mathrm{triv}} \geq \frac{2x}{\log(x)k} - Dnx^{1/2}\log(xd_K N(\mathfrak{fa})),$$

and $|\lambda| \leq Dnx^{1/2}\log(xd_K N(\mathfrak{fa}))$. So

$$\frac{\lambda_{\mathrm{triv}}}{|\lambda|} \geq \frac{4x^{1/2}}{(\log x)^2 Dkn(\log(d_K N(\mathfrak{fa})) + 1)} - 1.$$

We have that $x^{1/(2+\varepsilon)} = O(x^{1/2}/(\log x)^2)$ for any $\varepsilon > 0$, so considering larger constants C and D if necessary, we have the inequality

$$\frac{\lambda_{\mathrm{triv}}}{|\lambda|} \geq \frac{4x^{1/(2+\varepsilon)}}{Dkn(\log(d_K N(\mathfrak{fa})) + 1)} - 1.$$

The constants C and D are not absolute anymore but they only depend on ε. Let

$$B_{\delta,\varepsilon}(H, \mathfrak{a}) = \max\left(C, \left(\frac{1}{2}\left(\frac{1}{1-\delta} + 1\right) Dkn(\log(d_K N(\mathfrak{fa})) + 1)\right)^{2+\varepsilon}\right).$$

Then, for $x = B_{\delta,\varepsilon}(H, \mathfrak{a})$, we have $\frac{\lambda_{\mathrm{triv}}}{|\lambda|} \geq \frac{1}{1-\delta}$, so $\mathscr{G}_x$ is δ-expander. □

3.4. Horizontal isogeny graphs rapidly mix random walks

The two previous sections lead us to the main result of this chapter: horizontal isogeny graphs are expander graphs. More precisely, fix an absolutely simple, ordinary abelian variety $\mathscr{A}$ of dimension g over a finite field, and let $K = \mathrm{End}(\mathscr{A}) \otimes \mathbf{Q}$ be the corresponding CM-field. The endomorphism ring $\mathrm{End}(\mathscr{A})$ is isomorphic to an order $\mathcal{O}$ of conductor $\mathfrak{f}$ in K. The ideal class group $\mathrm{Cl}(\mathcal{O})$ acts freely on the set of varieties isogenous to $\mathscr{A}$ with same endomorphism ring $\mathcal{O}$. Let $H \subseteq \mathrm{Cl}(\mathcal{O})$ be any subgroup and let $H(\mathscr{A})$ be the H-orbit of $\mathscr{A}$. The choice of a set $\mathcal{S}$ of invertible ideals in $\mathcal{O}$ generating H induces a graph whose set of vertices is $H(\mathscr{A})$ and whose edges are labelled with isogenies between these abelian varieties. The norms of the ideals in $\mathcal{S}$ are exactly the degrees of the induced isogenies. For any $B > 0$ and ideal $\mathfrak{m}$ in $\mathcal{O}$, let $\mathcal{S}_B$ be the set of ideals in $\mathcal{O}$ of prime norm and coprime to $\mathfrak{fm}$. Let $\mathscr{G}_B$ be the induced isogeny graph, where all the degrees are bounded by B.

Theorem 3.21 (Rapid mixing for $H(\mathscr{A})$)**.** *Assuming the extended Riemann hypothesis, for any $\varepsilon > 0$, there exists a bound*

$$B = O\left((g[\mathrm{Cl}(\mathcal{O}) : H]\log(d_K N(\mathfrak{fm})))^{2+\varepsilon}\right),$$

such that for any subset W of $H(\mathscr{A})$, any random walk in the graph $\mathscr{G}_B$ of length at least $\log(2|H|/|W|^{1/2})$ starting from a given vertex will end in W with probability between $|W|/(2|H|)$ and $3|W|/(2|H|)$. In particular, the regular graph $\mathscr{G}_B$ is connected and rapidly mixes random walks.

Proof. Theorem 3.21 is an easy combination of the graph isomorphism expounded in Section 3.1.4, together with Corollary 3.20 establishing that these graphs are expanders, and Lemma 3.17 on random walks on such graphs. □

Remark 3.22. It is worth noting that even the connectivity of the graph is new: the classical bounds for connectivity are derived from Bach's bounds [Bac90], which can only be applied when H is the full class group $\mathrm{Cl}(\mathcal{O})$. However, the new bounds provide much more than connectivity, so one might wonder if better bounds can be obtained. In chapter 4, we generalise Bach's work to subgroups of ray class groups, resulting in tighter, explicit bounds for the connectivity of horizontal isogeny graphs.

3.5. Random walks on isogeny graphs of Jacobians in genus 2

Throughout this section, we will restrict to ordinary abelian surfaces that are Jacobians of genus 2 hyperelliptic curves over a finite field $\mathbf{F}_q$ (the main object of interest of hyperelliptic cryptography). Let $\mathscr{J} = \mathrm{Jac}(\mathscr{C})$ be such a Jacobian with endomorphism algebra K and whose endomorphism ring is isomorphic to an order $\mathcal{O}$ in K. Let $\mathcal{O}^+ = \mathcal{O} \cap K^+$ where K^+ is the real subfield of K. Let $\mathscr{A}$ be the isomorphism class of $\mathscr{J}$ as an abelian variety.

As explained in Section 3.2.2, the orbit $\mathscr{P}(\mathscr{A})$ of the CM-action of $\mathscr{P}(\mathcal{O})$ on $\mathscr{A}$ is a set of $\mathbf{F}_q$-isomorphism classes of principally polarisable abelian surfaces isogenous to $\mathscr{A}$ and with same endomorphism ring $\mathcal{O}$. This orbit contains *all* such isomorphism classes when the CM-action is transitive, for instance when $\mathcal{O}$ has maximal real multiplication (i.e., $\mathcal{O}_{K^+} \subset \mathcal{O}$). The choice of any set of ideals generating $\mathscr{P}(\mathcal{O})$ yields an isogeny graph on the set of vertices $\mathscr{P}(\mathscr{A})$, as described in Example 3.15. Now, Theorem 3.21 provides generating sets $\mathcal{S}$ with very convenient properties: (i) the corresponding isogeny graph rapidly mixes random walks, and (ii) every edge is an isogeny of small prime degree. In fact, all the occurring isogenies are computable in polynomial time by a recent algorithm of Dudeanu, Jetchev, Robert and Vuille [DJRV16, Dud16] (henceforth, the DJRV algorithm).

3.5.1. Computing isogenies of small degree. More precisely, the DJRV algorithm allows to compute any isogeny from $\mathscr{J}$, defined over $\mathbf{F}_q$ and of odd prime degree ℓ (i.e., given a generator of the kernel, it finds an equation of a hyperelliptic curve $\mathscr{C}'$ such that the target Jacobian is isomorphic to $\mathrm{Jac}(\mathscr{C}')$) under the following conditions:

(1) $\mathscr{J}$ has maximal real multiplication, i.e., $\mathcal{O}^+$ is the maximal order of K^+,
(2) the index $[\mathcal{O} : \mathbf{Z}[\pi, \bar{\pi}]]$ is prime to 2ℓ, and
(3) there exists a totally positive element $\beta \in \mathcal{O}^+$ of norm ℓ which annihilates the kernel of the isogeny (the isogeny is called β-*cyclic*, and the polarisation computed on the target curve depends on the choice of this β).

The cost of the algorithm is $O(\ell^2)$ operations in $\mathbf{F}_q$, assuming some precomputations of polynomial time in $\log(q)$ and ℓ (see [Dud16, Theorem 4.8.2]).

Observe that Condition (3) exactly means that the isogeny corresponds to an ideal in the kernel $\mathscr{P}(\mathcal{O})$ of the map $N_{K/K^+} : \mathrm{Cl}(\mathcal{O}) \to \mathrm{Cl}^+(\mathcal{O}^+)$. Therefore this condition is, by construction, satisfied by all the isogenies of the graph. Also, we can choose the generating set $\mathcal{S}$ so that it does not contain any ideal of norm dividing the index $[\mathcal{O} : \mathbf{Z}[\pi, \bar{\pi}]]$, so the isogenies of the graph all satisfy Condition (2) if and only if $[\mathcal{O} : \mathbf{Z}[\pi, \overline{\pi}]]$ is odd. Therefore, the conditions

(1) $\mathscr{J}$ has maximal real multiplication, and
(2) the index $[\mathcal{O} : \mathbf{Z}[\pi, \overline{\pi}]]$ is odd,

are sufficient for constructing a graph whose edges can all be computed by the DJRV algorithm. Before the work of Dudeanu et al., one was only able to compute (ℓ, ℓ)-isogenies [CR15], which are not sufficient to obtain a connected graph.

For the same computational cost, the DJRV algorithm can compute the image of a point of order coprime to $2q[\mathcal{O} : \mathbf{Z}[\pi, \overline{\pi}]]$, given some additional precomputations of polynomial cost in $\log(q)$. This cost, as expressed in [DJRV16, Theorem 1.3], relies on the existence of an efficient algorithm $\mathrm{RM}(\alpha, y)$ to compute the action of a real endomorphism y on a 4-torsion point α (see [DJRV16, Hypothesis H.4]); this hypothesis is satisfied in dimension 2, thanks to Mumford coordinates.

Remark 3.23. Recall that we want an undirected graph, meaning that $\mathcal{S} = \mathcal{S}^{-1}$. This is already the case for the subgroup $\mathscr{P}(\mathcal{O})$ and the set $\mathcal{S}$ of ideals of small prime norm, because $\mathcal{S}$ is closed for complex conjugation, and the complex conjugate of an ideal class in $\mathscr{P}(\mathcal{O})$ is also its inverse. However, it is worth noting that even in a more general situation, inverses can easily be added to $\mathcal{S}$ while still giving rise to a graph of computable isogenies. Indeed, let $\mathfrak{a} \in \mathcal{S}$, and suppose that the isogenies corresponding to the Galois conjugates of $\mathfrak{a}$ can all be computed efficiently. Then, the ideal

$$N_{K/\mathbf{Q}}(\mathfrak{a})\mathfrak{a}^{-1} = \prod_{\sigma \in \mathrm{Gal}(K/\mathbf{Q}) \setminus \{\mathrm{id}_K\}} \mathfrak{a}^{\sigma}$$

is a class inverse for $\mathfrak{a}$, which induces the dual of the isogeny induced by $\mathfrak{a}$, and can be computed as a sequence of $2g - 1$ computable isogenies.

3.5.2. Navigating in the graph with polarisations. The vertices of the graph represent principally *polarisable* (as opposed to *polarised*) abelian surfaces. As a consequence, two distinct Jacobians can represent the same vertex if they are isomorphic as abelian varieties, but have non-isomorphic polarisations. For computations, it is important to be able to determine whether two vertices of the graph are distinct or not, and to this end, the way the vertices are represented is crucial.

As explained in [CR15] and [DJRV16], it is possible to distinguish between isomorphism classes of Jacobians as principally polarised abelian varieties by simply comparing the Rosenhain invariants[2]. The DJRV algorithm computes these explicitly for the target curve of an isogeny. Therefore, if $U(\mathcal{O}) = \mathrm{TP}(\mathcal{O})/N_{K/K^+}(\mathcal{O}^\times)$ is trivial, as discussed in Section 3.2.2, the map $\mathfrak{C}(\mathcal{O}) \to \mathscr{P}(\mathcal{O})$ forgetting the polarisation is an isomorphism so the vertices of the graph can simply be represented as Jacobians, or their Rosenhain invariants.

But if $U(\mathcal{O})$ is of order 2, more work is required. In this case, for any Jacobian $\mathscr{J}_1$, there exists another Jacobian $\mathscr{J}_2$ which is isomorphic as a non-polarised abelian variety (and thus represents the same vertex in the graph), but not as a *principally polarised* abelian variety. To solve this issue, one can simply represent the vertices of the graph as pairs of Jacobians, isomorphic as abelian varieties, but with non-isomorphic polarisations. It is still possible to use the DJRV algorithm to navigate in this graph. Indeed, let $u \in \mathrm{TP}(\mathcal{O})$ be a generator of $U(\mathcal{O})$. Starting from $\mathscr{J}$, given an appropriate kernel, the DJRV algorithm chooses a β and computes the isogeny as a β-isogeny, resulting in a target Jacobian $\mathscr{J}_1$. If β is replaced by $u\beta$, the DJRV algorithm finds the Jacobian $\mathscr{J}_2$ which is isomorphic to $\mathscr{J}_1$ as an abelian variety, but with a different polarisation. Therefore the representation of the vertex $\{\mathscr{J}_1, \mathscr{J}_2\}$ can be fully computed.

A last point must be addressed: given a Jacobian $\mathscr{J}$ and a prime ℓ, the DJRV algorithm allows to find isogenies of degree ℓ from that Jacobian, but it is unclear a priori which of these isogenies remain within the graph we constructed. Indeed, it could well be that some of these isogenies change the endomorphism order $\mathcal{O}$. Luckily,

[2]Since the varieties are absolutely simple, ordinary, and over $\mathbf{F}_q$, two of them are $\mathbf{F}_q$-isomorphic if and only if they are $\bar{\mathbf{F}}_q$-isomorphic (a consequence of [Wat69, Theorem 7.2]).

this is not a concern if only primes ℓ that cannot change the endomorphism order are picked. An isogeny over $\mathbf{F}_q$ of degree ℓ can change the order only if ℓ divides the index $[\mathcal{O}_K : \mathbf{Z}[\pi, \bar{\pi}]]$ (such isogenies are studied in Chapter 5; see Proposition 5.10). Therefore, in the generating set $\mathcal{S}$, we avoid the prime ideals dividing that index.

3.6. Random self-reducibility of the discrete logarithm problem in genus 2.

The rapid mixing properties of isogeny graphs allow to prove that the discrete logarithm problem in genus 2 is random self-reducible in isogeny subclasses of ordinary Jacobians of genus 2 curves over a finite field, thus extending the similar result for elliptic curves proved in [JMV09, Theorem 1.6].

Theorem 3.24 (Random self-reducibility in genus 2)**.** *Let K be a primitive quartic CM-field, K^+ its maximal real subfield, and $\mathcal{O}$ an order in K. Let $\mathscr{J}$ be a Jacobian defined over $\mathbf{F}_q$ of endomorphism ring isomorphic to $\mathcal{O}$. Let $\mathcal{V}$ be the set of all $\mathbf{F}_q$-isomorphism classes of Jacobians defined over $\mathbf{F}_q$, isogenous to $\mathscr{J}$ and with endomorphism ring isomorphic to $\mathcal{O}$. Let G be a subgroup of $\mathscr{J}(\mathbf{F}_q)$ of order Q. Suppose that*

(1) there is an algorithm $\mathcal{A}$ that solves the DLP in time $f(q)$ for a proportion $\mu > 0$ of the Jacobians in $\mathcal{V}$, the "weak" Jacobians,
(2) there is an algorithm $\mathcal{B}$ that can decide in time $g(q)$ whether a Jacobian belongs to this "weak" family, and
(3) $\mathcal{O} \cap K^+$ is the ring of integers of K^+, and $[\mathcal{O} : \mathbf{Z}[\pi, \bar{\pi}]]$ is coprime to $2Q$.

Then, assuming the extended Riemann hypothesis, there is an absolute polynomial P in two variables such that the DLP can be solved in G by a probabilistic algorithm of expected runtime

$$\frac{P(\log(q), h^+_{\mathcal{O}^+}) + 2g(q)}{\mu} + f(q),$$

where $h^+_{\mathcal{O}^+}$ is the narrow class number of the order $\mathcal{O}^+ = \mathcal{O} \cap K^+$.

Remark 3.25. It is worth explaining the formal description of what input data the algorithm $\mathcal{A}$ takes. It is well known that in any cryptographically meaningful context, the points of the Jacobian are represented as divisor classes of degree zero. The latter are more compactly represented by *reduced divisors* leading to points being represented by the so-called Mumford coordinates. Thus, the input to the algorithm is a hyperelliptic curve of genus 2 together with an instance of the discrete logarithm problem (in Mumford coordinates). The above theorem uses the DJRV algorithm, which takes the input points as well as the Jacobian in theta coordinates (see [DJRV16, Theorem 1.1]). The conversion between Mumford coordinates and theta coordinates is well known and has been used in a number of prior works on isogeny computations [Rob10, Cos11, CR15].

Remark 3.26. The conditions that $\mathcal{O} \cap K^+$ is the ring of integers of K^+, and the index $[\mathcal{O} : \mathbf{Z}[\pi, \bar{\pi}]]$ is coprime to $2Q$ appear because they are required by the DJRV algorithm. Assuming that one has an algorithm that does not suffer these restrictions, one could replace these two conditions by $\mathcal{O}$ being Gorenstein (required for the action of $\mathscr{P}(\mathcal{O})$ to be transitive).

Proof. Let $\mathcal{W} \subset \mathcal{V}$ be the subset of all isomorphism classes for which the algorithm $\mathcal{A}$ applies (the "weak" Jacobians). For any two polarised abelian varieties $\mathscr{A}$ and $\mathscr{B}$, write $\mathscr{A} \sim \mathscr{B}$ if they are isomorphic as non-polarised abelian varieties. Recall that as discussed in Section 3.5.2, if $\mathcal{A}$ can solve the discrete logarithm problem in one Jacobian $\mathscr{J} \in \mathcal{W}$, then it can solve the discrete logarithm problem in the other Jacobians $\mathscr{J}' \sim \mathscr{J}$. Let

$V = \mathcal{V}/\sim$ and $W = \mathcal{W}/\sim$. Let π be a q-Weil number characterising the fixed isogeny class. From Example 3.15, the set V is naturally in bijection with $\mathscr{P}(\mathscr{A})$, the orbit for the CM-action of $\mathscr{P}(\mathcal{O})$. We can therefore apply Theorem 3.21 on the graph with set of vertices V induced by the set of invertible ideals in $\mathcal{O}$, coprime to $2[\mathcal{O}_K : \mathbf{Z}[\pi, \bar{\pi}]]$, of prime norm bounded by

$$\begin{aligned} B_\varepsilon(\mathcal{O}) &= O\left(\left(h^+_{\mathcal{O}^+} \log\left(d_K N(\mathfrak{f})[\mathcal{O}_K : \mathbf{Z}[\pi, \bar{\pi}]]\right)\right)^{2+\varepsilon}\right) \\ &= O\left(\left(h^+_{\mathcal{O}^+} \log(q)\right)^{2+\varepsilon}\right), \end{aligned}$$

where $\mathfrak{f}$ is the conductor of $\mathcal{O}$. Any path of length at least $\log(2|V|/|W|^{1/2}) \leq \log(2h_{\mathcal{O}})$ starting from any vertex will end in W with probability between $\mu/2$ and $3\mu/2$. So the strategy to solve the discrete logarithm problem on $\mathscr{A} \in V$ is to build random paths from $\mathscr{A}$ in $\mathscr{G}_B$ of length $\log(2h_{\mathcal{O}})$ until one of them ends in W. This membership in W can be verified in time $g(q)$ with the algorithm $\mathcal{B}$, and happens with probability higher than $\mu/2$, so after an expected number of independent trials smaller than $2/\mu$. The length of each path is polynomial in $\log(h_{\mathcal{O}})$, and the degree of each isogeny on the path is bounded by $B_\varepsilon(\mathcal{O})$. So the algorithm computes a polynomial (in $\log(q)$) number of isogenies, and each of them can be computed in polynomial time (in $\log(q)$ and $h^+_{\mathcal{O}^+}$) by the DJRV algorithm. □

3.7. Computing an explicit isogeny between two given Jacobians

In [Gal99], Galbraith considers the problem of computing an explicit isogeny between two isogenous ordinary elliptic curves E_1 and E_2 over $\mathbf{F}_q$. His approach is based on considering isogeny graphs and growing trees rooted at both E_1 and E_2 of small-degree computable isogenies until a collision is found. Galbraith's original algorithm is proven to finish in probabilistic polynomial time (in $\log(q)$), finding a path of length $O(\log(h_K))$ from E_1 to E_2, under ERH and a heuristic assumption claiming that the distribution of the new random points found in the process of growing the trees is close to uniform. In this section, the expander properties of horizontal isogeny graphs are used to construct and analyse an algorithm similar to the one from [Gal99]. The contribution of this new algorithm is two-fold. First, using expander properties of these graphs, our analysis relies solely on ERH, without heuristics. Second, while Galbraith's algorithm constructs isogenies between elliptic curves, we provide a more general framework for large families of horizontal isogeny graphs. Precisely, we require:

(1) An order $\mathcal{O}$ of conductor $\mathfrak{f}$ in a CM-field K, and two isogenous abelian varieties $\mathscr{A}$ and $\mathscr{B}$ over a finite field $\mathbf{F}_q$ with endomorphism ring $\mathcal{O}$;
(2) A set $\mathcal{S}$ of ideals in $\mathcal{O}$ generating a subgroup H of the class group $\mathrm{Cl}(\mathcal{O})$, such that the orbits $H(\mathscr{A})$ and $H(\mathscr{B})$ coincide;
(3) The isogeny graph $\mathscr{G}$ induced by the action of H on $H(\mathscr{A})$ has the rapid mixing property, as described in Theorem 3.21;
(4) The isogenies corresponding to the edges of the graph can be computed in time bounded by some $t_H > 0$.

For elliptic curves, one can choose $H = \mathrm{Cl}(\mathcal{O})$, and $\mathcal{S}$ the set of all ideals of prime norm bounded by a bound $B = O(\log(d_K N(\mathfrak{f}))^{2+\varepsilon}) = O((\log q)^{2+\varepsilon})$. All these isogenies can be computed in time t_H polynomial in $\log q$, and Theorem 3.21, or even the less general results of [JMV05, JMV09], shows that $\mathscr{G}$ has the rapid mixing property. The smaller bound $O(\log(d_K N(\mathfrak{f}))^2)$ was used in Galbraith's approach; the induced graph

is then connected, but is not an expander, therefore some heuristic assumptions were required for the analysis.

For Jacobians of genus 2 curves, one can choose $H = \mathscr{P}(\mathcal{O})$, and $\mathcal{S}$ to be a generating set of ideals of prime norms bounded by a bound $O\left((h^+_{\mathcal{O}^+}\log(q))^{2+\varepsilon}\right)$, where $\mathcal{O}^+ = \mathcal{O} \cap K^+$. As seen in Section 3.5.1, the corresponding isogenies can then be computed using the DJRV algorithm when $\mathcal{O}^+$ is maximal and $[\mathcal{O} : \mathbf{Z}[\pi, \bar{\pi}]]$ is odd.

Write $h = |H|$. The idea is to find $h^{1/2}$ varieties "close" to $\mathscr{A}$ (in the sense that we know a path of polynomial length from these to $\mathscr{A}$), and then to build paths out of $\mathscr{B}$ until one of the neighbors of $\mathscr{A}$ is reached. In practice one could simply use the same tree-growing strategy as Galbraith [Gal99], but the analysis of our algorithm requires the various random paths to be independent in order to use the expanding properties (this independence misses in the "tree" approach). The algorithm goes as follows, presented in the most general setting.

Step 1 Build independent random paths in $\mathscr{G}$ of length $\log(2h)$ from $\mathscr{A}$ until $h^{1/2}$ vertices are reached. Those are the *neighbors* of $\mathscr{A}$.

Step 2 Build independent random paths of length $\log(2h)$ from $\mathscr{B}$ until a neighbor of $\mathscr{A}$ is reached. There is now a short path between $\mathscr{A}$ and $\mathscr{B}$.

Now, let us prove that the number of paths considered at each step is on average $O(h^{1/2})$. Let Y be a subset of the vertices of $\mathscr{G}$, smaller than $2h/3$. By a *trial*, we mean the computation of a random path of length $\log(2h)$ from of A, and a trial is a *success* if the path ends outside Y. Let us estimate the number N_Y of independent trials we need to obtain a success,

$$\begin{aligned}\mathbf{E}[N_Y] &= \sum_{i=1}^{\infty} i \Pr[i-1 \text{ failures and } 1 \text{ success}] \\ &\leq \sum_{i=1}^{\infty} i \left(\frac{3|Y|}{2h}\right)^{i-1},\end{aligned}$$

and from the generating function $(1-x)^{-2} = \sum_{i=0}^{\infty}(i+1)x^i$, we obtain the inequality

$$\mathbf{E}[N_Y] \leq \left(1 - \frac{3|Y|}{2h}\right)^{-2} = \frac{4h^2}{(2h-3|Y|)^2}.$$

Now consider the experiment consisting in a sequence of independent trials, and let Y_n be the first n distinct points obtained from the first experiments. The number M_n of trials required to find n distinct points can be estimated as

$$\mathbf{E}[M_n] = \sum_{i=1}^{n-1} \mathbf{E}[N_{Y_i}] \leq \sum_{i=1}^{n-1} \frac{4h^2}{(2h-3i)^2} \leq \frac{4nh^2}{(2h-3n)^2}.$$

In particular, to find $h^{1/2}$ neighbors of $\mathscr{A}$, the expected number of trials $\mathbf{E}[M_{h^{1/2}}]$ is at most $4h^{1/2}$, assuming that h is at least 9. Of course, in practice, we expect to need much fewer trials since we count here only the end point of each path. This proves that the expected number of paths we have to compute in Step 1 is $O\left(h^{1/2}\right)$.

The expected number of paths considered in Step 2 can be found to be $O\left(h^{1/2}\right)$ in a similar fashion. In total, we build $O\left(h^{1/2}\right)$ paths of length $O(\log(h))$. So the algorithm needs to compute $O\left(h^{1/2}\log(h)\right)$ isogenies, each of them being computable in time t_H, and finds a path of length $O(\log(h))$ between $\mathscr{A}$ and $\mathscr{B}$.

4

Small generators for subgroups of class groups

Abstract. This chapter is based on an article presented at the Thirteenth Algorithmic Number Theory Symposium, ANTS-XIII, as

[Wes18b] B. Wesolowski, *Generating subgroups of ray class groups with small prime ideals*, Thirteenth Algorithmic Number Theory Symposium – ANTS-XIII, 2018, proceedings to appear in the Open Book Series, Mathematical Sciences Publishers.

Original abstract. Explicit bounds are given on the norms of prime ideals generating arbitrary subgroups of ray class groups of number fields, assuming the extended Riemann hypothesis. These are the first explicit bounds for this problem, and are significantly better than previously known asymptotic bounds. Applied to the integers, they express that any subgroup of index i of the multiplicative group of integers modulo m is generated by prime numbers smaller than $16(i \log m)^2$, subject to the generalised Riemann hypothesis. Two particular consequences relate to mathematical cryptology. Applied to cyclotomic fields, they provide explicit bounds on generators of the relative class group, needed in some previous work on the shortest vector problem on ideal lattices. Applied to Jacobians of hyperelliptic curves, they allow one to derive bounds on the degrees of isogenies required to make their horizontal isogeny graphs connected. Such isogeny graphs are used to study the discrete logarithm problem on said Jacobians.

Consider a number field K, and an order $\mathcal{O}$ in this field. Let Δ be the absolute value of the discriminant of K, and let $\mathfrak{f}$ be the conductor of $\mathcal{O}$. Assuming the extended Riemann hypothesis (henceforth, ERH), the class group of the order $\mathcal{O}$ is generated by the classes of invertible prime ideals of prime norm smaller than

$$18 \log(\Delta^2 N(\mathfrak{f}))^2.$$

This bound was computed by Bach in 1990 [Bac90]. In particular, when $\mathcal{O}$ is the endomorphism ring of an abelian variety, it implies that the corresponding horizontal isogeny graphs with isogenies of prime degrees bounded by $18 \log(\Delta^2 N(\mathfrak{f}))^2$ is connected. Bach's bounds made explicit the earlier work of Lagarias, Montgomery and Odlyzko [LMO79], and have proved to be a crucial tool in the design and analysis of many number theoretic algorithms. However, these bounds do not tell anything about the norms of prime ideals generating any particular subgroup of the class group. Indeed, a generating set for the full group might not contain any element of the subgroup. In particular, they do not allow to construct connected isogeny graphs of principally polarisable abelian

varieties. In this chapter, we generalise Bach's explicit bounds to arbitrary subgroups of ray class groups (Theorem 4.1 for characters, and Theorem 4.16 for generating sets), with implications not only for isogeny graphs, but also for the third part of this thesis on ideal lattices in cyclotomic fields (this however is left to be discussed later, in Chapter 7).

With K a number field of degree n, and Δ the absolute value of its discriminant, the results of [LMO79] show that the class group $\mathrm{Cl}(K)$ is generated by prime ideals of norm bounded by $O((\log \Delta)^2)$. Now, let H be an arbitrary subgroup of the class group $\mathrm{Cl}(K)$. Some asymptotic bounds on the norm of prime ideals generating H have already been computed in Chapter 3 by analysing spectral properties of the underlying Cayley graphs. They are of the form $O((n[\mathrm{Cl}(K) : H] \log \Delta)^{2+\varepsilon})$, for an arbitrary $\varepsilon > 0$. Taking H to be the full class group reveals a clear gap with the bounds of [LMO79]. The new explicit bounds provided in the present chapter eliminate this gap, as they are asymptotically $O(([\mathrm{Cl}(K) : H] \log \Delta)^2)$.

4.1. Ray class characters

This section summarises the definitions, notation and facts related to ray class characters that will be used in the rest of the chapter. We assume the terminology and notation introduced in Section 3.1.5 for ray class groups.

Throughout this chapter, K denotes a number field of degree n, with r_1 embeddings into $\mathbf{R}$ and $2r_2$ embeddings into $\mathbf{C}$. Our main tools in what follows are ray class characters. We call a *ray class character modulo* $\mathfrak{m}$ what Neukirch [NS99, Definition VII.6.8] calls a (generalised) Dirichlet character modulo $\mathfrak{m}$, that is a Größencharakter $\chi : \mathscr{I}_{\mathfrak{m}}(K) \to \mathbf{C}^\times$ that factors through the ray class group $\mathrm{Cl}_{\mathfrak{m}}(K)$ via the canonical projection. A character is *principal* if it takes only the value 1. Let $\delta(\chi)$ be 1 if χ is principal and 0 otherwise. A ray class character is *primitive modulo* $\mathfrak{m}$ if it does not factor through $\mathrm{Cl}_{\mathfrak{m}'}(K)$ for any modulus $\mathfrak{m}'$ smaller[1] than $\mathfrak{m}$. The conductor $\mathfrak{f}_\chi$ of χ is the smallest modulus $\mathfrak{f}$ such that χ is the restriction of a ray class character modulo $\mathfrak{f}$. Let $\beta_\chi = |\mathfrak{f}_\infty|$ be the number of infinite places in the conductor $\mathfrak{f}$. From [NS99, Proposition 6.9], any ray class character χ is the restriction of a primitive ray class character of modulus $\mathfrak{f}_\chi$, which is also primitive as a Größencharakter.

The Hecke L-function associated to a character χ modulo $\mathfrak{m}$ is defined as

$$L_\chi(s) = \sum_{\mathfrak{a}} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s},$$

for $\mathfrak{Re}(s) > 1$, where the sum is taken over all ideals of $\mathcal{O}_K$. Note that χ is implicitly extended to all ideals by defining $\chi(\mathfrak{a}) = 0$ whenever $(\mathfrak{a}, \mathfrak{m}_0) \neq 1$. When χ is the trivial character on $\mathscr{I}(K)$, we obtain the Dedekind zeta function of K, $\zeta_K(s) = \sum_{\mathfrak{a}} N(\mathfrak{a})^{-s}$. These L-functions are extended meromorphically on the complex plane with at most a simple pole at $s = 1$, which occurs if and only if χ is principal. Let R_χ be the set of zeros of L_χ on the critical strip $0 < \mathfrak{Re}(s) < 1$. The ERH states that for all Hecke L-functions the zeros on the critical strip satisfy $\mathfrak{Re}(s) = 1/2$.

We will make an extensive use of the logarithmic derivatives L'_χ/L_χ. For any s such that $\mathfrak{Re}(s) > 1$, they admit the absolutely convergent representation

$$\frac{L'_\chi}{L_\chi}(s) = -\sum_{\mathfrak{a}} \frac{\Lambda(\mathfrak{a})\chi(\mathfrak{a})}{N(\mathfrak{a})^s}, \tag{4.1}$$

[1] A modulus $\mathfrak{m}'$ is (strictly) smaller than $\mathfrak{m}$ if $\mathfrak{m}'_0 \mid \mathfrak{m}_0$, $\mathfrak{m}'_\infty \subseteq \mathfrak{m}_\infty$ and $\mathfrak{m}' \neq \mathfrak{m}$.

TABLE 4.1. Residues of the logarithmic derivative of Hecke L-functions, when χ is a primitive ray class character ([Bac90, p. 361]).

place	**residue of ζ_K'/ζ_K**	**residue of L_χ'/L_χ**
1	-1	0
$\rho \in R_1$	1	0 if $\rho \notin R_\chi$, 1 otherwise
$\rho \in R_\chi$	0 if $\rho \notin R_1$, 1 otherwise	1
0	$r_1 + r_2 - 1$	$r_1 + r_2 - \beta_\chi$
$-2n+1, n \in \mathbf{N}_{>0}$	r_2	$r_2 + \beta_\chi$
$-2n, n \in \mathbf{N}_{>0}$	$r_1 + r_2$	$r_1 + r_2 - \beta_\chi$

where Λ is the von Mangoldt function (i.e., $\Lambda(\mathfrak{a}) = \log N(\mathfrak{p})$ if $\mathfrak{a}$ is a power of a prime ideal $\mathfrak{p}$, and 0 otherwise). The residues of L_χ'/L_χ when χ is primitive modulo $\mathfrak{m}$ are summarised in Table 4.1, which comes from [Bac90, p. 361] (with the observation that β in [Bac90] coincides with $\beta_\chi = |\mathfrak{m}_\infty|$ for characters χ which are primitive modulo $\mathfrak{m}$).

Let ψ be the logarithmic derivative of the gamma function, and for any ray class character χ on K, define

$$\psi_\chi(s) = \frac{r_1 + r_2 - \beta_\chi}{2}\psi\left(\frac{s}{2}\right) + \frac{r_2 + \beta_\chi}{2}\psi\left(\frac{s+1}{2}\right) - \frac{n\log\pi}{2}. \tag{4.2}$$

The main reason to introduce these functions is the following formula: for any complex number s, if χ is primitive then

$$-\mathfrak{Re}\frac{L_\chi'}{L_\chi}(s) = \frac{1}{2}\log(\Delta N(\mathfrak{f}_\chi)) + \mathfrak{Re}\left(\delta(\chi)\left(\frac{1}{s} + \frac{1}{s-1}\right) - \sum_{\rho\in R_\chi}\frac{1}{s-\rho} + \psi_\chi(s)\right). \tag{4.3}$$

A proof can be found in [LO77, Lemma 5.1].

4.2. Small primes for non-trivial characters

Let K be a number field of degree n, and $\mathfrak{m}$ a modulus of K. Consider any subgroup H of the ray class group $\mathrm{Cl}_\mathfrak{m}(K)$, and any character χ that is not trivial on that subgroup. The main theorem of this chapter generalises [Bac90] by providing explicit bounds on the smallest prime ideal $\mathfrak{p}$ whose class is in H and such that $\chi(\mathfrak{p}) \neq 1$. Note that all statements containing the mention (ERH) assume the extended Riemann hypothesis.

Theorem 4.1 (ERH)**.** *Let K be any number field, and Δ the absolute value of the discriminant of K. Let $\mathfrak{m}$ be a modulus of K, with finite part $\mathfrak{m}_0$ and infinite part $\mathfrak{m}_\infty$. Let H be any subgroup of the ray class group $\mathrm{Cl}_\mathfrak{m}(K)$. Let χ be a ray class character modulo $\mathfrak{m}$ that is not trivial on H. Then there is a prime ideal $\mathfrak{p}$ such that $(\mathfrak{p}, \mathfrak{m}_0) = 1$, the class of $\mathfrak{p}$ in $\mathrm{Cl}_\mathfrak{m}(K)$ is in the subgroup H, $\chi(\mathfrak{p}) \neq 1$, $\deg(\mathfrak{p}) = 1$ and*

$$N(\mathfrak{p}) \leq \left([\mathrm{Cl}_\mathfrak{m}(K) : H]\,(2.71\log(\Delta N(\mathfrak{m}_0)) + 1.29|\mathfrak{m}_\infty| + 1.38\omega(\mathfrak{m}_0)) + 4.13\right)^2,$$

where $\omega(\mathfrak{m}_0)$ denotes the number of distinct prime ideals dividing $\mathfrak{m}_0$.

The proof of this theorem is the object of Section 4.3, and its consequences are discussed in Section 4.4.

Remark 4.2. When H is the full group and $n \geq 2$, the above bound can be compared to Bach's bound $N(\mathfrak{p}) \leq 18(\log(\Delta^2 N(\mathfrak{m}_0)))^2$ given by [Bac90, Theorem 4]. Let us put

the expression of Theorem 4.1 in a comparable form. From [Bac90, Lemma 7.1], we have

$$|\mathfrak{m}_\infty| \leq n \leq \frac{\log(\Delta N(\mathfrak{m}_0)) + 3/2}{\log(2\pi) - \psi(2)} \leq 0.71 \log(\Delta N(\mathfrak{m}_0)) + 1.07,$$

where ψ is the logarithmic derivative of the gamma function. Moreover, we have the bound $\omega(\mathfrak{m}_0) \leq \log(\Delta N(\mathfrak{m}_0))/\log(2)$. The bound of Theorem 4.1 becomes $N(\mathfrak{p}) \leq (5.62 \log(\Delta N(\mathfrak{m}_0)) + 5.52)^2$. Whenever $\Delta N(\mathfrak{m}_0) < 12$, the corresponding ray class group is trivial, so we can suppose that $\log(\Delta N(\mathfrak{m}_0)) \geq \log(12) \geq 2.48$. These estimates lead to

$$N(\mathfrak{p}) \leq (5.62 + 5.52/2.48)^2 (\log(\Delta N(\mathfrak{m}_0)))^2 \leq 62(\log(\Delta N(\mathfrak{m}_0)))^2. \tag{4.4}$$

Even in this form, direct comparison with [Bac90, Lemma 7.1] is not obvious. With the unrefined estimate $\Delta^2 N(\mathfrak{m}_0) \leq (\Delta N(\mathfrak{m}_0))^2$, Bach's bound becomes

$$N(\mathfrak{p}) \leq 72(\log(\Delta N(\mathfrak{m}_0)))^2.$$

The constant factor is slightly worse than in the bound (4.4), but this comparison does not do justice to either theorem.

4.3. Proof of the main theorem

In this section, we prove Theorem 4.1. Throughout, we consider a ray class character χ modulo $\mathfrak{m}$ that is not trivial on a given subgroup H of $G = \mathrm{Cl}_{\mathfrak{m}}(K)$. Recall that K is a number field of degree n, with r_1 embeddings into $\mathbf{R}$ and $2r_2$ embeddings into $\mathbf{C}$. An inequality such as $x \leq y$ between complex numbers means that the relation holds between the real parts.

4.3.1. Outline of the proof. For any $0 < a < 1$, $x > 0$, and ideal $\mathfrak{a}$, let

$$P(\mathfrak{a}, x) = \Lambda(\mathfrak{a}) \left(\frac{N(\mathfrak{a})}{x}\right)^a \log\left(\frac{x}{N(\mathfrak{a})}\right).$$

Let us start by recalling a lemma that is the starting point of the original proof of Bach's bounds.

Lemma 4.3 ([Bac90, Lem. 4.2])**.** *For $0 < a < 1$ and any character η,*

$$\sum_{N(\mathfrak{a}) < x} \eta(\mathfrak{a}) P(\mathfrak{a}, x) = \frac{-1}{2\pi i} \int_{2-i\infty}^{2+i\infty} \frac{x^s}{(s+a)^2} \cdot \frac{L'_\eta}{L_\eta}(s) ds.$$

Bach then considers the difference between two instances of this equality at $\eta = 1$ and at $\eta = \chi$, and proves the bounds by estimating the right-hand side as $x + O(\sqrt{x})$, while the left-hand side is zero if the character is trivial on all prime ideals of norm smaller than x; therefore such an x cannot be too large.

The proof of Theorem 4.1 follows the same strategy. It exploits the series of lemmata provided in [Bac90, Section 5], interlacing them with a game of characters of G/H in order to account for the new condition $[\mathfrak{a}]_{\mathfrak{m}} \in H$. Consider the group of characters of the quotient G/H, namely $\widehat{G/H} = \mathrm{Hom}(G/H, \mathbf{C}^\times)$. Given any character $\theta \in \widehat{G/H}$, let θ^* be the primitive ray class character such that $\theta^*(\mathfrak{a}) = \theta([\mathfrak{a}]_{\mathfrak{m}} H)$ whenever $(\mathfrak{a}, \mathfrak{m}_0) = 1$. For any $\theta \in \widehat{G/H}$, write L_θ for the L-function of θ^*. For any ray class character η and any $\theta \in \widehat{G/H}$, let η_θ denote the primitive character inducing the product $\eta\theta^*$.

Lemma 4.4. *Let $\mathfrak{a}$ be any ideal in K. Let $\mathfrak{n}_0$ be the largest divisor of $\mathfrak{m}_0$ coprime to $\mathfrak{a}$, and $\mathfrak{n} = \mathfrak{n}_0\mathfrak{m}_\infty$. Let $\pi : \mathrm{Cl}_\mathfrak{m}(K) \to \mathrm{Cl}_\mathfrak{n}(K)$ be the natural projection. Then,*

$$\sum_{\theta \in \widehat{G/H}} \theta^*(\mathfrak{a}) = \begin{cases} [\mathrm{Cl}_\mathfrak{n}(K) : \pi(H)] & \text{if } [\mathfrak{a}]_\mathfrak{n} \in \pi(H), \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Let $\Theta_\mathfrak{a} = \{\theta \in \widehat{G/H} \mid \theta^*(\mathfrak{a}) \neq 0\} = \{\theta \in \widehat{G/H} \mid (\mathfrak{f}_{\theta^*}, \mathfrak{a}) = 1\}$. This set is naturally in bijection with the group X of characters of $\mathrm{Cl}_\mathfrak{n}(K)/\pi(H)$. We obtain

$$\sum_{\theta \in \widehat{G/H}} \theta^*(\mathfrak{a}) = \sum_{\theta \in \Theta_\mathfrak{a}} \theta^*(\mathfrak{a}) = \sum_{\nu \in X} \nu([\mathfrak{a}]_\mathfrak{n}) = \begin{cases} [\mathrm{Cl}_\mathfrak{n}(K) : \pi(H)] & \text{if } [\mathfrak{a}]_\mathfrak{n} \in \pi(H), \\ 0 & \text{otherwise.} \end{cases}$$

□

Lemma 4.5. *For any $0 < a < 1$, we have*

$$\mathscr{S}_\mathfrak{m}(x) + \mathscr{S}_H(x) = \frac{-1}{[G:H]} \sum_{\theta \in \widehat{G/H}} I(x, \theta),$$

where

$$\mathscr{S}_H(x) = \sum_{\substack{N(\mathfrak{a}) < x \\ [\mathfrak{a}]_\mathfrak{m} \in H}} (1 - \chi(\mathfrak{a}))\, P(\mathfrak{a}, x),$$

$$\mathscr{S}_\mathfrak{m}(x) = \frac{1}{[G:H]} \sum_{\theta \in \widehat{G/H}} \sum_{\substack{N(\mathfrak{a}) < x \\ (\mathfrak{a}, \mathfrak{m}) \neq 1}} (\theta^*(\mathfrak{a}) - \chi_\theta(\mathfrak{a}))\, P(\mathfrak{a}, x), \text{ and}$$

$$I(x, \theta) = \frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} \frac{x^s}{(s+a)^2} \left(\frac{L'_\theta}{L_\theta} - \frac{L'_{\chi_\theta}}{L_{\chi_\theta}} \right)(s) ds.$$

Proof. From Lemma 4.4, for any ray class character η, we have

$$\begin{aligned} \sum_{\substack{N(\mathfrak{a}) < x \\ [\mathfrak{a}]_\mathfrak{m} \in H}} \eta(\mathfrak{a}) P(\mathfrak{a}, x) &= \sum_{\substack{N(\mathfrak{a}) < x \\ (\mathfrak{a}, \mathfrak{m}) = 1}} \frac{\sum_{\theta \in \widehat{G/H}} \theta^*(\mathfrak{a})}{[G:H]} \eta(\mathfrak{a}) P(\mathfrak{a}, x) \\ &= \frac{1}{[G:H]} \sum_{\theta \in \widehat{G/H}} \sum_{\substack{N(\mathfrak{a}) < x \\ (\mathfrak{a}, \mathfrak{m}) = 1}} \eta_\theta(\mathfrak{a}) P(\mathfrak{a}, x). \end{aligned}$$

Subtracting two instances of this equality, for $\eta = 1$ and $\eta = \chi$, we get

$$\mathscr{S}_H(x) = \frac{1}{[G:H]} \sum_{\theta \in \widehat{G/H}} \sum_{N(\mathfrak{a}) < x} (\theta^*(\mathfrak{a}) - \chi_\theta(\mathfrak{a}))\, P(\mathfrak{a}, x) - \mathscr{S}_\mathfrak{m}(x),$$

and conclude by applying Lemma 4.3. □

Lemma 4.6. *For $0 < a < 1$, and with the notation from Lemma 4.5,*

$$\frac{x}{(a+1)^2} = [G:H](\mathscr{S}_H(x) + \mathscr{S}_\mathfrak{m}(x)) + \sum_{\theta \in \widehat{G/H}} \big(I_{1/2}(x, \theta) + I_0(x, \theta) + I_-(x, \theta) \big)$$

where

$$I_{1/2}(x,\theta) = \sum_{\rho\in R_\theta} \frac{x^\rho}{(\rho+a)^2} - \sum_{\rho\in R_{\chi_\theta}} \frac{x^\rho}{(\rho+a)^2},$$

$$I_0(x,\theta) = \frac{\log(x)}{x^a}\left(\frac{L'_\theta}{L_\theta} - \frac{L'_{\chi_\theta}}{L_{\chi_\theta}}\right)(-a) + \frac{1}{x^a}\left(\frac{L'_\theta}{L_\theta} - \frac{L'_{\chi_\theta}}{L_{\chi_\theta}}\right)'(-a)$$
$$+ (\beta_{\chi_\theta} - \beta_\theta)\left(\frac{1}{a^2} - \frac{1}{x(a-1)^2}\right) - \frac{\delta(\theta)}{a^2},\ \textit{and}$$

$$I_-(x,\theta) = (\beta_{\chi_\theta} - \beta_\theta)\sum_{k=2}^{\infty} \frac{(-1)^k}{(a-k)^2 x^k}.$$

Recall that for any character η, we denote by R_η the set of zeros of L_η on the strip $0 < \mathfrak{Re}(s) < 1$.

Proof. This lemma is an analogue of [Bac90, Lemma 4.4]. Evaluating each integral $I(x,\theta)$ by residue using Table 4.1 yields

$$I(x,\theta) = I_{1/2}(x,\theta) + I_0(x,\theta) + I_-(x,\theta) - \frac{\delta(\theta)x}{(a+1)^2}.$$

The residue calculations can be justified as in the proof of [LO77, Theorem 28]. The result follows from Lemma 4.5. □

4.3.2. Explicit estimates. This section adopts the notation from Lemma 4.5 and Lemma 4.6. The remainder of the proof consists in evaluating each term in the formula of Lemma 4.6. More precisely, we bound the quantities

(1) $I_{1/2}$ in Lemma 4.9,
(2) I_0 in Lemma 4.11,
(3) $\mathscr{S}_{\mathfrak{m}}$ in Lemma 4.12,
(4) $\mathscr{S}_H$ in Lemma 4.14.

Remains the quantity I_-, which is easy to bound thanks to [Bac90, Lemma 5.1]. All these estimates are combined in Lemma 4.13. Let

$$\mathscr{R}(a,\chi) = \sum_{\theta\in\widehat{G/H}} \left(\sum_{\rho\in R_\theta} \frac{1}{|\rho+a|^2} + \sum_{\rho\in R_{\chi_\theta}} \frac{1}{|\rho+a|^2}\right).$$

We bound that quantity in Lemma 4.8, but first, we need the following lemma.

Lemma 4.7. *For $\mathfrak{Re}(s) > 1$, we have*

$$\sum_{\theta\in\widehat{G/H}} \left(\frac{L'_\theta}{L_\theta} + \frac{L'_{\chi_\theta}}{L_{\chi_\theta}}\right)(s) \le 0.$$

Proof. Equation (4.1) on page 56 yields

$$\sum_{\theta\in\widehat{G/H}} \left(\frac{L'_\theta}{L_\theta} + \frac{L'_{\chi_\theta}}{L_{\chi_\theta}}\right)(s) = -\sum_{\theta\in\widehat{G/H}} \sum_{\mathfrak{a}} \frac{\Lambda(\mathfrak{a})(\theta^*(\mathfrak{a}) + \chi_\theta(\mathfrak{a}))}{N(\mathfrak{a})^s}$$
$$= -\sum_{\mathfrak{a}} \frac{\Lambda(\mathfrak{a})}{N(\mathfrak{a})^s} \sum_{\theta\in\widehat{G/H}} (\theta^*(\mathfrak{a}) + \chi_\theta(\mathfrak{a})).$$

Fix an ideal $\mathfrak{a}$. If $\chi_\theta(\mathfrak{a}) = 0$ for all θ, Lemma 4.4 implies that

$$\sum_{\theta \in \widehat{G/H}} (\theta^*(\mathfrak{a}) + \chi_\theta(\mathfrak{a})) \geq 0.$$

Now suppose that there exists an $\eta \in \widehat{G/H}$ such that $\chi_\eta(\mathfrak{a}) \neq 0$. The fact that any given character is induced by a unique primitive character implies that for any $\theta \in \widehat{G/H}$, we have $\chi_\theta(\mathfrak{a}) = \chi_\eta(\mathfrak{a}) \left(\theta\eta^{-1}\right)^* (\mathfrak{a})$. Indeed, if $\left(\theta\eta^{-1}\right)^* (\mathfrak{a}) \neq 0$, the equality follows from the fact that χ_θ is the primitive character inducing $\chi_\eta \cdot \left(\theta\eta^{-1}\right)^*$, and if $\left(\theta\eta^{-1}\right)^* (\mathfrak{a}) = 0$, then one must have $\chi_\theta(\mathfrak{a}) = 0$ because $\left(\theta\eta^{-1}\right)^*$ is the primitive character inducing χ_θ/χ_η. We deduce that

$$\begin{aligned}\sum_{\theta \in \widehat{G/H}} (\theta^*(\mathfrak{a}) + \chi_\theta(\mathfrak{a})) &= \sum_{\theta \in \widehat{G/H}} \theta^*(\mathfrak{a}) + \chi_\eta(\mathfrak{a}) \sum_{\theta \in \widehat{G/H}} \left(\frac{\theta}{\eta}\right)^* (\mathfrak{a}) \\ &= (1 + \chi_\eta(\mathfrak{a})) \sum_{\theta \in \widehat{G/H}} \theta^*(\mathfrak{a}),\end{aligned}$$

whose real part is non-negative (using again Lemma 4.4). □

Lemma 4.8 (ERH)**.** *Let $0 < a < 1$. The sum $\mathscr{R}(a, \chi)$ is at most*

$$\frac{2[G:H]}{2a+1}\Bigg(\log(\Delta N(\mathfrak{m}_0)) + n(\psi(a+1) - \log(2\pi)) \\ - \frac{|\mathfrak{m}_\infty|}{2}\left(\psi\left(\frac{a+1}{2}\right) - \psi\left(\frac{a+2}{2}\right)\right)\Bigg) + \frac{2}{2a+1}\left(\frac{1}{a+1} + \frac{1}{a}\right).$$

Proof. Writing $\sigma = 1 + a$, we have $\frac{2a+1}{|\rho+a|^2} = \frac{1}{\sigma-\rho} + \frac{1}{\sigma-\bar{\rho}}$ for any $\mathfrak{Re}(\rho) = 1/2$ (as observed in [Bac90, Lemma 5.5]), so for any ray class character η

$$\sum_{\rho \in R_\eta} \frac{1}{|\rho + a|^2} = \frac{1}{2a+1} \sum_{\rho \in R_\eta} \left(\frac{1}{\sigma - \rho} + \frac{1}{\sigma - \bar{\rho}}\right).$$

As in [LO77, Lemma 5.1], we get from Equation (4.3) that

$$\sum_{\rho \in R_\eta} \left(\frac{1}{\sigma - \rho} + \frac{1}{\sigma - \bar{\rho}}\right) = 2\mathfrak{Re}\frac{L'_\eta}{L_\eta}(\sigma) + \log(\Delta N(\mathfrak{f}_\eta)) + 2\delta(\eta)\left(\frac{1}{\sigma} + \frac{1}{\sigma - 1}\right) + 2\psi_\eta(\sigma).$$

Then, $\mathscr{R}(a, \eta)$ is at most

$$\frac{1}{2a+1} \sum_{\theta \in \widehat{G/H}} \Bigg(2\mathfrak{Re}\left(\frac{L'_\theta}{L_\theta} + \frac{L'_{\chi_\theta}}{L_{\chi_\theta}}\right)(\sigma) + \log(\Delta^2 N(\mathfrak{f}_\theta \mathfrak{f}_{\chi_\theta})) \\ + 2\delta(\theta)\left(\frac{1}{\sigma} + \frac{1}{\sigma - 1}\right) + 2(\psi_\theta(\sigma) + \psi_{\chi_\theta}(\sigma))\Bigg). \tag{4.5}$$

From Lemma 4.7, we have $\sum_{\theta\in\widehat{G/H}}\left(\frac{L'_\theta}{L_\theta}+\frac{L'_{\chi_\theta}}{L_{\chi_\theta}}\right)(\sigma)\le 0$, and the corresponding term can be discarded from the expression in (4.5). Also, with $\alpha_{\chi_\theta}=r_1-\beta_{\chi_\theta}$,

$$\begin{aligned}2\left(\psi_\theta(\sigma)+\psi_{\chi_\theta}(\sigma)\right) &= (n+\alpha_{\chi_\theta}-\beta_\theta)\psi\left(\frac{a+1}{2}\right)+(n-\alpha_{\chi_\theta}+\beta_\theta)\psi\left(\frac{a+2}{2}\right)-2n\log\pi\\ &= 2n(\psi(a+1)-\log(2\pi))+(\alpha_{\chi_\theta}-\beta_\theta)\left(\psi\left(\frac{a+1}{2}\right)-\psi\left(\frac{a+2}{2}\right)\right)\\ &\le 2n(\psi(a+1)-\log(2\pi))-|\mathfrak{m}_\infty|\left(\psi\left(\frac{a+1}{2}\right)-\psi\left(\frac{a+2}{2}\right)\right),\end{aligned}$$

where the first equality uses the expression (4.2) and the second one follows from the duplication formula $(\psi(z/2)+\psi((z+1)/2)=2(\psi(z)-\log(2)))$. □

Lemma 4.9 (ERH)**.** *For $0<a<1$ and $x\ge 1$, $\sum_{\theta\in\widehat{G/H}}|I_{1/2}(x,\theta)|\le\sqrt{x}\cdot\mathscr{R}(a,\chi)$.*

Proof. From the ERH, for any ray class character η, and any zero $\rho\in R_\eta$ of L_η on the critical strip, we have $\mathfrak{Re}(\rho)\le 1/2$. Therefore $|x^\rho|=|x|^{\mathfrak{Re}(\rho)}\le\sqrt{x}$. □

Lemma 4.10. *For any s,*

$$\begin{aligned}\left(\frac{L'_\theta}{L_\theta}-\frac{L'_{\chi_\theta}}{L_{\chi_\theta}}\right)(s) = &\sum_{\rho\in R_\theta}\left(\frac{1}{s-\rho}-\frac{1}{2-\rho}\right)-\sum_{\rho\in R_{\chi_\theta}}\left(\frac{1}{s-\rho}-\frac{1}{2-\rho}\right)\\ &-\frac{\beta_{\chi_\theta}-\beta_\theta}{2}\left(\psi\left(\frac{s}{2}\right)-\psi\left(\frac{s+3}{2}\right)-\psi(1)+\psi\left(\frac{3}{2}\right)\right)\\ &-\frac{\beta_{\chi_\theta}-\beta_\theta}{s+1}+\delta(\theta)\left(\frac{3}{2}-\frac{1}{s}-\frac{1}{s-1}\right)+\left(\frac{L'_\theta}{L_\theta}-\frac{L'_{\chi_\theta}}{L_{\chi_\theta}}\right)(2),\end{aligned}$$

and

$$\begin{aligned}\left(\frac{L'_\theta}{L_\theta}-\frac{L'_{\chi_\theta}}{L_{\chi_\theta}}\right)'(s) = &\sum_{\rho\in R_{\chi_\theta}}\frac{1}{(s-\rho)^2}-\sum_{\rho\in R_\theta}\frac{1}{(s-\rho)^2}\\ &-\frac{\beta_{\chi_\theta}-\beta_\theta}{4}\left(\psi'\left(\frac{s}{2}\right)-\psi'\left(\frac{s+3}{2}\right)\right)\\ &+\frac{\beta_{\chi_\theta}-\beta_\theta}{(s+1)^2}+\delta(\theta)\left(\frac{1}{s^2}+\frac{1}{(s-1)^2}\right).\end{aligned}$$

Proof. This is essentially the same proof as [Bac90, Lemma 5.2], with an additional use of the recurrence relations $\psi(z)=\psi(z+1)-1/z$ and $\psi'(z)=\psi'(z+1)+1/z^2$. □

Lemma 4.11 (ERH)**.** *Let $0<a<1$ and $x\ge 1$. Then,*

$$\begin{aligned}\sum_{\theta\in\widehat{G/H}}I_0(x,\theta)\le &\frac{(2+a)\log(x)+1}{x^a}\cdot\mathscr{R}(a,\chi)+\frac{[G:H]|\mathfrak{m}_\infty|}{a^2}-\frac{1}{a^2}\\ &+\frac{\log(x)}{x^a}\left(\frac{3}{2}+\frac{1}{a}+\frac{1}{a+1}\right)+\frac{1}{x^a}\left(\frac{1}{a^2}+\frac{1}{(a+1)^2}\right)\\ &+\frac{[G:H]|\mathfrak{m}_\infty|}{x}\left(\frac{1}{(1-a)^2}-\frac{\log(x)}{(a-1)x^{a-1}}-\frac{1}{(a-1)^2x^{a-1}}\right).\end{aligned}$$

Proof. For any $0 < a < 1$, Lemma 4.10 implies that

$$\sum_{\theta \in \widehat{G/H}} \left(\frac{L'_\theta}{L_\theta} - \frac{L'_{\chi_\theta}}{L_{\chi_\theta}} \right)(-a) \leq (2+a) \cdot \mathscr{R}(a,\chi) + \frac{3}{2} + \frac{1}{a} + \frac{1}{a+1} - \sum_{\theta \in \widehat{G/H}} \frac{\beta_{\chi_\theta} - \beta_\theta}{1-a},$$

and

$$\sum_{\theta \in \widehat{G/H}} \left(\frac{L'_\theta}{L_\theta} - \frac{L'_{\chi_\theta}}{L_{\chi_\theta}} \right)'(-a) \leq \mathscr{R}(a,\chi) + \frac{1}{a^2} + \frac{1}{(a+1)^2} + \sum_{\theta \in \widehat{G/H}} \frac{\beta_{\chi_\theta} - \beta_\theta}{(1-a)^2}.$$

We used the facts that $\psi\left(\frac{-a}{2}\right) - \psi\left(\frac{3-a}{2}\right) - \psi(1) + \psi\left(\frac{3}{2}\right) \geq 0$, and $\psi'\left(\frac{-a}{2}\right) - \psi'\left(\frac{3-a}{2}\right) \geq 0$, which are easily derived from the recurrence relations $\psi(z) = \psi(z+1) - 1/z$ and $\psi'(z) = \psi'(z+1) + 1/z^2$, and the monotonicity of ψ and ψ'. From [Bac90, Lemma 5.3], for any $0 < a < 1$, we have $\left(\frac{\log(x)}{(a-1)x^{a-1}} + \frac{1}{(a-1)^2 x^{a-1}} - \frac{1}{(1-a)^2} \right) \leq 0$, therefore

$$\begin{aligned} &\sum_{\theta \in \widehat{G/H}} \frac{\beta_{\chi_\theta} - \beta_\theta}{x} \left(\frac{\log(x)}{(a-1)x^{a-1}} + \frac{1}{(a-1)^2 x^{a-1}} - \frac{1}{(1-a)^2} \right) \\ &\leq \frac{[G:H]|\mathfrak{m}_\infty|}{x} \left(\frac{1}{(1-a)^2} - \frac{\log(x)}{(a-1)x^{a-1}} - \frac{1}{(a-1)^2 x^{a-1}} \right). \end{aligned}$$

The result follows by applying these estimates to $I_0(x,\theta)$ (as defined in Lemma 4.6). □

Lemma 4.12. *For any $0 < a < 1$,*

$$\mathscr{S}_{\mathfrak{m}}(x) \leq \frac{2\log(x)}{ea} \omega(\mathfrak{m}_0) \leq \frac{2\log(x)}{ea\log(2)} \log(N(\mathfrak{m}_0)),$$

where $\omega(\mathfrak{m}_0)$ is the number of distinct prime ideals dividing $\mathfrak{m}_0$.

Proof. We have

$$\mathscr{S}_{\mathfrak{m}}(x) = \frac{1}{[G:H]} \sum_{\substack{N(\mathfrak{a}) < x \\ (\mathfrak{a},\mathfrak{m}) \neq 1}} \left(\sum_{\theta \in \widehat{G/H}} (\theta^*(\mathfrak{a}) - \chi_\theta(\mathfrak{a})) \right) P(\mathfrak{a},x) \leq \sum_{\substack{N(\mathfrak{a}) < x \\ (\mathfrak{a},\mathfrak{m}) \neq 1}} 2P(\mathfrak{a},x),$$

and the result follows from [Bac90, Lemma 5.7]. □

Lemma 4.13 (ERH)**.** *For any $0 < a < 1$, the fraction $\sqrt{x}/(a+1)^2$ is at most*

$$[G:H]\left(s_1(x)\log(\Delta N(\mathfrak{m}_0)) + s_5(x)n + s_4(x)|\mathfrak{m}_\infty| + s_3(x)\omega(\mathfrak{m}_0) + \frac{\mathscr{S}_H(x)}{\sqrt{x}} \right) + s_2(x),$$

where

$$
\begin{aligned}
s_1(x) &= \frac{2}{2a+1}\left(1+\frac{(2+a)\log(x)+1}{x^{a+1/2}}\right),\\
s_2(x) &= s_1(x)\left(\frac{1}{a}+\frac{1}{a+1}\right)+\frac{\log(x)}{x^{a+1/2}}\left(\frac{3}{2}+\frac{1}{a}+\frac{1}{a+1}\right)+\frac{1}{x^{a+1/2}}\left(\frac{1}{a^2}+\frac{1}{(a+1)^2}\right),\\
s_3(x) &= \frac{2\log(x)}{ea\sqrt{x}},\\
s_4(x) &= \frac{1}{(a-2)^2x^{5/2}}-\frac{s_1(x)}{2}\left(\psi\left(\frac{a+1}{2}\right)-\psi\left(\frac{a+2}{2}\right)\right)+\frac{1}{a^2\sqrt{x}}\\
&\quad+\frac{1}{x^{3/2}}\left(\frac{1}{(1-a)^2}-\frac{\log(x)}{(a-1)x^{a-1}}-\frac{1}{(a-1)^2x^{a-1}}\right),\\
s_5(x) &= s_1(x)(\psi(a+1)-\log(2\pi)).
\end{aligned}
$$

Proof. As in [Bac90, Lemma 5.1], we have $0 \le \sum_{k=2}^{\infty}\frac{(-1)^k}{(a-k)^2x^k} \le \frac{1}{(a-2)^2x^2}$. We deduce that $I_-(x,\theta) \le \frac{|\beta_{\chi_\theta}-\beta_\theta|}{(a-2)^2x^2} \le \frac{|\mathfrak{m}_\infty|}{(a-2)^2x^2}$. Together with Lemma 4.9, the bound from Lemma 4.6 becomes

$$\frac{\sqrt{x}}{(a+1)^2} \le \frac{[G:H]|\mathfrak{m}_\infty|}{(a-2)^2x^{5/2}}+\mathscr{R}(a,\chi)+\frac{1}{\sqrt{x}}\sum_{\theta\in\widehat{G/H}} I_0(x,\theta)+[G:H]\frac{\mathscr{S}_H(x)+\mathscr{S}_{\mathfrak{m}}(x)}{\sqrt{x}}.$$

The result then follows from Lemma 4.8, Lemma 4.11 and Lemma 4.12. □

Lemma 4.14. *Suppose that $\chi(\mathfrak{p})=1$ for all prime ideals $\mathfrak{p}$ such that $N(\mathfrak{p})<x$, $[\mathfrak{p}]_{\mathfrak{m}}\in H$, and $\deg(\mathfrak{p})=1$. Then, for any $0<a<1$,*

$$\mathscr{S}_H(x) \le \frac{2n}{ea}\sum_{m<\sqrt{x}}\Lambda(m).$$

Proof. We start as in [Bac90, Lemma 5.7] by observing that when $t\ge 1$, the function $t^{-a}\log t$ is bounded above by $1/ea$. We deduce

$$\mathscr{S}_H(x) = \sum_{\substack{N(\mathfrak{a})<x\\ [\mathfrak{a}]_{\mathfrak{m}}\in H}}(1-\chi(\mathfrak{a}))\,P(\mathfrak{a},x) \le \frac{2}{ea}\sum_{\substack{N(\mathfrak{a})<x\\ [\mathfrak{a}]_{\mathfrak{m}}\in H\\ \chi(\mathfrak{a})\neq 1}}\Lambda(\mathfrak{a}). \tag{4.6}$$

Fix a prime ideal $\mathfrak{p}$ (above a rational prime p) of norm smaller than x and consider the contribution of its powers to the last sum above. First suppose that $\deg(\mathfrak{p})>1$. Then,

$$\sum_{\substack{N(\mathfrak{p}^k)<x\\ [\mathfrak{p}^k]_{\mathfrak{m}}\in H\\ \chi(\mathfrak{p}^k)\neq 1}}\Lambda(\mathfrak{p}^k) \le \sum_{N(\mathfrak{p}^k)<x}\deg(\mathfrak{p})\Lambda(p^k) \le \deg(\mathfrak{p})\sum_{p^k<\sqrt{x}}\Lambda(p^k).$$

Now suppose that $\deg(\mathfrak{p})=1$, and let ℓ be the smallest integer such that $[\mathfrak{p}^\ell]_{\mathfrak{m}}\in H$. If $\ell=1$, then $\chi(\mathfrak{p}^k)=1$ for any integer k, so the contribution of $\mathfrak{p}$ is zero. Suppose that $\ell\ge 2$. Then,

$$\sum_{\substack{N(\mathfrak{p}^k)<x\\ [\mathfrak{p}^k]_{\mathfrak{m}}\in H\\ \chi(\mathfrak{p}^k)\neq 1}}\Lambda(\mathfrak{p}^k) \le \sum_{N(\mathfrak{p}^{k\ell})<x}\Lambda(\mathfrak{p}^{k\ell}) \le \deg(\mathfrak{p})\sum_{p^k<\sqrt{x}}\Lambda(p^k).$$

Summing over all rational primes p and ideals $\mathfrak{p}$ above p, we obtain

$$\sum_p \sum_{\mathfrak{p}|p} \sum_{\substack{N(\mathfrak{p}^k)<x \\ [\mathfrak{p}^k]_{\mathfrak{m}}\in H \\ \chi(\mathfrak{p}^k)\neq 1}} \Lambda(\mathfrak{p}^k) \leq \sum_p \sum_{\mathfrak{p}|p} \deg(\mathfrak{p}) \sum_{p^k<\sqrt{x}} \Lambda(p^k) \leq n \sum_{m<\sqrt{x}} \Lambda(m).$$

We conclude by applying this inequality to Equation (4.6). □

Lemma 4.15. *For any $x > 0$,*

$$\lim_{a\to 1}\left(\frac{1}{(1-a)^2} - \frac{\log(x)}{(a-1)x^{a-1}} - \frac{1}{(a-1)^2x^{a-1}}\right) = \frac{(\log x)^2}{2}.$$

Proof. A simple application of l'Hôpital's rule yields

$$\begin{aligned}
&\lim_{a\to 1}\left(\frac{1}{(1-a)^2} - \frac{\log(x)}{(a-1)x^{a-1}} - \frac{1}{(a-1)^2x^{a-1}}\right) \\
&= \lim_{b\to 0}\left(\frac{x^b - b\log(x) - 1}{b^2x^b}\right) = \lim_{b\to 0}\left(\frac{x^b\log(x) - \log(x)}{bx^b(b\log(x)+2)}\right) \\
&= \lim_{b\to 0}\left(\frac{(\log x)^2}{b^2(\log x)^2 + 4b\log(x) + 2}\right) = \frac{(\log x)^2}{2}.
\end{aligned}$$

□

4.3.3. Proof of Theorem 4.1. Let x be the norm of the smallest prime ideal $\mathfrak{p}$ such that $[\mathfrak{p}]_{\mathfrak{m}} \in H$, $\deg(\mathfrak{p}) = 1$ and $\chi(\mathfrak{p}) \neq 1$. First suppose that $x \leq 95$, and consider the quantity

$$B = \big([G:H]\,(2.71\log(\Delta N(\mathfrak{m}_0)) + 1.29|\mathfrak{m}_\infty| + 1.38\omega(\mathfrak{m}_0)) + 4.13\big)^2.$$

We want to show that $x \leq B$.

Suppose $n = 1$. For the ray class group G not to be trivial, one must have either $|\mathfrak{m}_\infty| = 1$ and $N(\mathfrak{m}_0) \geq 3$, in which case

$$B \geq \big(2.71\log(3) + 1.29 + 1.38 + 4.13\big)^2 = 95.59\cdots \geq x,$$

or $|\mathfrak{m}_\infty| = 0$ and $N(\mathfrak{m}_0) \geq 5$, in which case

$$B \geq \big(2.71\log(5) + 1.38 + 4.13\big)^2 = 97.44\cdots \geq x.$$

Suppose $n = 2$. Suppose that $\Delta N(\mathfrak{m}_0) \geq 8$. Then

$$B \geq (2.71\log(8) + 4.13)^2 = 95.36\cdots \geq x.$$

Now, one must investigate the cases where $\Delta N(\mathfrak{m}_0) \leq 7$. All quadratic fields with a discriminant of absolute value at most 7 have a trivial (narrow) class group. Therefore, one must have $N(\mathfrak{m}_0) \geq 2$. There is only one quadratic field of discriminant of absolute value at most 3, namely $\mathbf{Q}(\sqrt{-3})$. It has discriminant of absolute value 3 and no ideal of norm 2, so the condition $\Delta N(\mathfrak{m}_0) \leq 7$ is impossible.

Suppose $n > 2$. From [Bac90, Lemma 7.1], we get

$$\log(\Delta N(\mathfrak{m}_0)) \geq n(\log(2\pi) - \psi(2)) - \frac{3}{2} \geq 2.74,$$

and we deduce

$$B \geq (2.71 \cdot 2.74 + 4.13)^2 = 133.52\cdots \geq x.$$

It remains to consider the case $x > 95$. From Lemma 4.14 and [RS62, Theorem 12],

$$\mathscr{S}_H(x) \leq \frac{2n}{ea} \sum_{m<\sqrt{x}} \Lambda(m) \leq \frac{2nC\sqrt{x}}{ea},$$

where $C = 1.03883$. We now apply Lemma 4.13 with $a \to 1$. From Lemma 4.15 (applied to the s_4-term), and the facts that for $x \geq 95$, the value $\left(s_5(x) + \frac{2C}{ea}\right)$ is negative, and s_1, s_2, s_3 and s_4 are decreasing, we get

$$\begin{aligned} x &\leq 2^4\big([G:H]\,(s_1(95)\log(\Delta N(\mathfrak{m}_0)) + s_4(95)|\mathfrak{m}_\infty| + s_3(95)\omega(\mathfrak{m}_0)) + s_2(95)\big)^2 \\ &\leq \big([G:H]\,(2.71\log(\Delta N(\mathfrak{m}_0)) + 1.29|\mathfrak{m}_\infty| + 1.38\omega(\mathfrak{m}_0)) + 4.13\big)^2, \end{aligned}$$

which proves the theorem. □

4.4. Consequences

In this section, a series of notable consequences is derived from Theorem 4.1.

4.4.1. Generating subgroups of ray class groups. Foremost, Theorem 4.1 allows us to obtain sets of small prime ideals generating any given subgroup of a ray class group. This is made precise in the following theorem.

Theorem 4.16 (ERH)**.** *Let K be any number field, and Δ the absolute value of the discriminant of K. Let $\mathfrak{m}$ be a modulus of K, with finite part $\mathfrak{m}_0$ and infinite part $\mathfrak{m}_\infty$. Let $\mathfrak{h}$ be any ideal in K. Let H be a non-trivial subgroup of the ray class group $\mathrm{Cl}_\mathfrak{m}(K)$. Then H is generated by the classes of the prime ideals in*

$$\{\mathfrak{p} \text{ prime ideal in } K \mid (\mathfrak{p}, \mathfrak{h}\mathfrak{m}_0) = 1, [\mathfrak{p}]_\mathfrak{m} \in H, \deg(\mathfrak{p}) = 1 \text{ and } N(\mathfrak{p}) < B\},$$

where $B = ([\mathrm{Cl}_\mathfrak{m}(K) : H]\,(2.71\log(\Delta N(\mathfrak{h}\mathfrak{m}_0)) + 1.29|\mathfrak{m}_\infty| + 1.38\omega(\mathfrak{h}\mathfrak{m}_0)) + 4.13)^2$.

Proof. With B the bound from the theorem, let

$$\mathscr{N} = \{\mathfrak{p} \in \mathscr{I}_\mathfrak{m}(K) \mid \mathfrak{p} \text{ is prime}, (\mathfrak{p}, \mathfrak{h}) = 1, [\mathfrak{p}]_\mathfrak{m} \in H, \deg(\mathfrak{p}) = 1 \text{ and } N(\mathfrak{p}) < B\},$$

and N the subgroup of H generated by $\mathscr{N}$. By contradiction, suppose $N \neq H$. Then, there is a non-trivial character of H that is trivial on N. Since G is abelian, this character on H extends to a character on G, thereby defining a ray class character χ modulo $\mathfrak{m}$ that is not trivial on H. From Theorem 4.1, there is a prime ideal $\mathfrak{p} \in \mathscr{I}_{\mathfrak{h}\mathfrak{m}}(K)$ such that $[\mathfrak{p}]_\mathfrak{m} \in H$, $\chi(\mathfrak{p}) \neq 1$, $\deg(\mathfrak{p}) = 1$ and $N(\mathfrak{p}) \leq B$. All these conditions imply that $\mathfrak{p} \in \mathscr{N} \subseteq N$, whence $\chi(\mathfrak{p}) = 1$, a contradiction. □

4.4.2. Multiplicative subgroups of integers modulo m. Applying Theorem 4.1 to Dirichlet characters, one can obtain new results on subgroups of the multiplicative group $(\mathbf{Z}/m\mathbf{Z})^\times$. Let m be a positive integer, and H a non-trivial subgroup of $G = (\mathbf{Z}/m\mathbf{Z})^\times$. It is already known that, assuming ERH, H contains a prime number smaller than $O(([G:H]\log m)^2)$ (see [BS96, LLS15]). But these bounds do not provide a generating set for H: they only guarantee the existence of one such prime number. The following theorem gives a set of generators of H, whose norms are also $O(([G:H]\log m)^2)$.

Theorem 4.17 (ERH)**.** *Let m be a positive integer, and H a non-trivial subgroup of $G = (\mathbf{Z}/m\mathbf{Z})^\times$. Then H is generated by the set of prime numbers p such that $p \bmod m \in H$ and $p \leq 16\left([G:H]\log m\right)^2$.*

Proof. Let $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ where $\mathfrak{m}_0 = m\mathbf{Z}$ and $\mathfrak{m}_\infty$ is the real embedding of $\mathbf{Q}$. Then, the group $\mathrm{Cl}_\mathfrak{m}(\mathbf{Q})$ is isomorphic to $G = (\mathbf{Z}/m\mathbf{Z})^\times$. An isomorphism is given by the map sending the class of $a\mathbf{Z}$ to $a \bmod m$. The subgroup H of $(\mathbf{Z}/m\mathbf{Z})^\times$ corresponds to a subgroup H' of $\mathrm{Cl}_\mathfrak{m}(\mathbf{Q})$ through this isomorphism. From Theorem 4.16, H' is generated by prime numbers smaller than

$$B = \left([G:H]\left(2.71\log(m) + 1.29 + 1.38\omega(m)\right) + 4.13\right)^2,$$

and so is H. If H is the full group, then the theorem follows from [Bac90, Theorem 3]; and for $m \leq 11000$, the result can be checked by an exhaustive computation. So we can assume that $m/|H| \geq 2$ and $m > 11000$. From [Bac90, Lemma 6.4],

$$\frac{\omega(m)}{\log m} \leq \frac{\mathrm{li}(\log m) + 0.12\sqrt{\log m}}{\log m} \leq \frac{\mathrm{li}(\log 11000) + 0.12\sqrt{\log 11000}}{\log 11000} \leq 0.67,$$

where li is the logarithmic integral function. We get

$$B \leq \left([G:H]\log(m)\left(2.71 + \frac{1.29 + 4.13/2}{\log 11000} + 1.38\cdot 0.67\right)\right)^2,$$

and we conclude by computing the constant. □

4.4.3. Connected horizontal isogeny graphs. Finally, we go back to our original motivation, and derive bounds on the degrees of cyclic isogenies required to connect all isogenous principally polarisable abelian varieties over a finite field sharing the same endomorphism ring.

Theorem 4.18 (ERH)**.** *Let $\mathscr{A}$ be a principally polarised, absolutely simple, ordinary abelian variety over a finite field $\mathbf{F}_q$, with endomorphism algebra K and endomorphism ring isomorphic to an order $\mathcal{O}$ in K. Let K^+ be the maximal real subfield of K, and $\mathfrak{f}$ the conductor of $\mathcal{O}$. For any $B > 0$, let $\mathscr{G}(B)$ be the isogeny graph whose vertices are the principally polarisable varieties isogenous to $\mathscr{A}$ and with the same endomorphism ring, and whose edges are isogenies connecting them, of prime degree smaller than B. Then, if $\mathcal{O}^+ = \mathcal{O} \cap K^+$ is the ring of integers of K^+, the graph*

$$\mathscr{G}\left(26\left(h^+_{\mathcal{O}^+}\log(\Delta N(\mathfrak{f}))\right)^2\right)$$

is connected, with Δ the absolute value of the discriminant of K, and $h^+_{\mathcal{O}^+}$ the narrow class number of $\mathcal{O}^+$.

Remark 4.19. In particular, the above holds in dimension 2, where, as already mentioned, *principally polarised* translates to *Jacobian of a genus 2 hyperelliptic curve*.

Proof. As explained in Section 3.1.4, the graph $\mathscr{G}(B)$ is isomorphic to the Cayley graph of

$$\mathscr{P}(\mathcal{O}) = \ker(\mathrm{Cl}(\mathcal{O}) \to \mathrm{Cl}^+(\mathcal{O}\cap K^+))$$

with set of generators the classes of ideals of prime norm smaller than B. Let $g \geq 2$ be the dimension of $\mathscr{A}$, and $n = 2g$ the degree of its endomorphism algebra K. The natural map $\pi : \mathrm{Cl}_\mathfrak{f}(K) \to \mathrm{Cl}(\mathcal{O})$ is a surjection (see Section 3.1.5), so it is sufficient to find a generating set for $H = \pi^{-1}(\mathscr{P}(\mathcal{O}))$. From Lemma 3.14, we have the inequality

$$[\mathrm{Cl}_\mathfrak{f}(K) : H] \leq [\mathrm{Cl}(\mathcal{O}) : \mathscr{P}(\mathcal{O})] \leq h^+_{\mathcal{O}^+}.$$

From Theorem 4.16, $\mathscr{G}(B)$ is connected for

$$B = \left(2.71 + 1.38\frac{\omega(\mathfrak{f})}{\log(\Delta N(\mathfrak{f}))} + \frac{4.13}{\log(\Delta N(\mathfrak{f}))}\right)^2 \left(h^+_{\mathcal{O}^+} \log(\Delta N(\mathfrak{f}))\right)^2, \tag{4.7}$$

and it remains to show that the constant factor in this expression is at most 26. First, we need a lower bound on the quantity $\log(\Delta N(\mathfrak{f}))$. From [Odl90, Table 3], if $n = 4$, $\log(\Delta N(\mathfrak{f})) \geq 4\log(3.263) \geq 4.73$ (this result assumes ERH). For $n \geq 6$, [Bac90, Lemma 7.1] implies

$$\log(\Delta N(\mathfrak{f})) \geq n(\log(2\pi) - \psi(2)) - \frac{3}{2} \geq 6.99.$$

Therefore for any degree $n \geq 4$, we have $\log(\Delta N(\mathfrak{f})) \geq 4.73$. Now, for $n = 2$, smaller values of $\log(\Delta N(\mathfrak{f}))$ are possible. One can check that the constant factor in the expression (4.7) is at most 26 for all pairs $(\Delta, N(\mathfrak{f}))$ such that $\log(\Delta N(\mathfrak{f})) < 4.73$ by an exhaustive computation. There are however five exceptions: when the field is $\mathbf{Q}(\sqrt{-1})$ and $N(\mathfrak{f}) \in \{1, 2\}$, when the field is $\mathbf{Q}(\sqrt{-3})$ and $N(\mathfrak{f}) \in \{1, 3\}$, and when the field is $\mathbf{Q}(\sqrt{5})$ and $N(\mathfrak{f}) = 1$. Since $\mathfrak{f}$ is the conductor of an order in a quadratic field, it is generated by an integer, so $N(\mathfrak{f})$ must be a square. This discards the cases $N(\mathfrak{f}) \in \{2, 3\}$. When $N(\mathfrak{f}) = 1$, the order $\mathcal{O}$ is the ring of integers, which has a trivial (narrow) class group for $\mathbf{Q}(\sqrt{-1})$, $\mathbf{Q}(\sqrt{-3})$ and $\mathbf{Q}(\sqrt{5})$.

Then, irrespective of the value of n, we can assume in the rest of the proof that $\log(\Delta N(\mathfrak{f})) \geq 4.73$. If $\omega(\mathfrak{f}) \leq 5$, then

$$\frac{\omega(\mathfrak{f})}{\log(\Delta N(\mathfrak{f}))} \leq \frac{5}{4.73} \leq 1.06.$$

If $\omega(\mathfrak{f}) > 5$, then $N(\mathfrak{f}) \geq 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13^{\omega(\mathfrak{f})-5}$, and

$$\frac{\omega(\mathfrak{f})}{\log(\Delta N(\mathfrak{f}))} \leq \frac{\omega(\mathfrak{f})}{\log(2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13^{\omega(\mathfrak{f})-5})} \leq \frac{5}{\log(2 \cdot 3 \cdot 5 \cdot 7 \cdot 11)} + \frac{1}{\log(13)} \leq 1.06.$$

Then,

$$\left(2.71 + \frac{1.38 \cdot \omega(\mathfrak{f})}{\log(\Delta N(\mathfrak{f}))} + \frac{4.13}{\log(\Delta N(\mathfrak{f}))}\right)^2 \leq (2.71 + 1.38 \cdot 1.06 + 4.13/4.73)^2 \leq 26,$$

which concludes the proof. □

5

Vertical structure of isogeny graphs

Abstract. This chapter is based on a joint work with Ernest Hunter Brooks and Dimitar Jetchev, which was published in the journal Research in Number Theory as

[BJW17] E. H. Brooks, D. Jetchev, and B. Wesolowski, *Isogeny graphs of ordinary abelian varieties*, Research in Number Theory **3** (2017), no. 1, 28.

Original abstract. Fix a prime number ℓ. Graphs of isogenies of degree a power of ℓ are well-understood for elliptic curves, but not for higher-dimensional abelian varieties. We study the case of absolutely simple ordinary abelian varieties over a finite field. We analyse graphs of so-called $\mathfrak{l}$-isogenies, resolving that, in arbitrary dimension, their structure is similar, but not identical, to the "volcanoes" occurring as graphs of isogenies of elliptic curves. Specialising to the case of principally polarisable abelian surfaces, we then exploit this structure to describe graphs of a particular class of isogenies known as (ℓ, ℓ)-isogenies: those whose kernels are maximal isotropic subgroups of the ℓ-torsion for the Weil pairing. We use these two results to write an algorithm giving a path of computable isogenies from an arbitrary absolutely simple ordinary abelian surface towards one with maximal endomorphism ring. This has immediate consequences for the CM-method in genus 2, for computing explicit isogenies, and for the random self-reducibility of the discrete logarithm problem in genus 2 cryptography.

5.1. Isogeny volcanoes

The previous two chapters have focused on horizontal isogeny graphs, where all the abelian varieties have the same endomorphism ring. However, two abelian varieties in the same isogeny class *can* have different endomorphism rings. There is thus an interest in understanding the structure of *vertical* isogenies, which change the endomorphism ring. To study horizontal graphs, we were looking simultaneously at isogenies of various degrees, up to some bound. To study the vertical structure, it is more enlightening to work locally at some fixed prime ℓ, and consider graphs where isogenies are of degree a power of ℓ.

In the case of ordinary elliptic curves, the structure of the ℓ-isogeny graph is well-understood (the graph containing all isogenies of degree ℓ), thanks to the work of Kohel [Koh96], who showed that such a graph is a *volcano* (the name and modern definition first appearing in [FM02]):

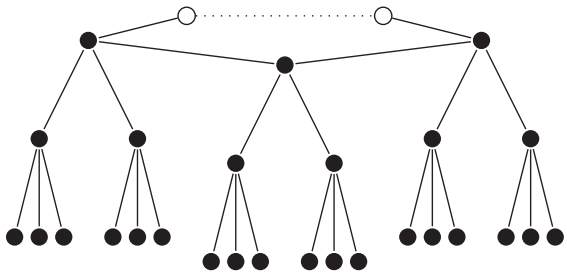


FIGURE 5.1. Isogeny volcanoes for elliptic curves. The cycle at the top is the surface (level 0). The points just below the surface are at level 1, and the leaves are at level 2.

Definition 5.1 (Volcano)**.** Let n be a positive integer. An (infinite) *n-volcano* $\mathscr{V}$ is an $(n+1)$-regular, connected, undirected graph whose vertices are partitioned into *levels* $\{\mathscr{V}_i\}_{i\in\mathbf{Z}_{\geq 0}}$ such that:

(i) The subgraph $\mathscr{V}_0$, the *surface*, is a finite regular graph of degree at most 2,
(ii) For each $i > 0$, each vertex in $\mathscr{V}_i$ has exactly one neighbor in $\mathscr{V}_{i-1}$, and these are exactly the edges of the graph that are not on the surface.

For any positive integer h, the corresponding (finite) volcano of height h is the restriction of $\mathscr{V}$ to its first h levels.

An example of a volcano constructed out of isogenies of elliptic curves over finite fields is given in Figure 5.1. This description has seen numerous applications, including point-counting on elliptic curves [FM02], random self-reducibility of the elliptic curve discrete logarithm problem in isogeny classes [JMV05, JMV09], generating elliptic curves with a prescribed number of points via the CM method [Sut12], and computing modular polynomials [BLS12].

There is great interest in generalising these results to higher dimension, and that would require a similar description of isogeny graphs for other ordinary abelian varieties.

5.1.1. Volcanoes and endomorphism rings. At the heart of Kohel's results for elliptic curves lies a deep connection between graphs of ℓ-isogenies and endomorphism rings of elliptic curves. As explained in Chapter 4, the endomorphism ring of an ordinary elliptic curve over a finite field is isomorphic to an order in an imaginary quadratic field, the endomorphism algebra of the curve, and the endomorphism rings of two isogenous ordinary elliptic curves are isomorphic to orders (possibly distinct) in the *same* imaginary quadratic field. Orders in imaginary quadratic fields are well-understood: fix such a field K, and let $\mathcal{O}_K$ be its ring of integers. The orders in K are exactly the rings of the form $\mathbf{Z} + f\mathcal{O}_K$ for positive integers f. For any volcano of ℓ-isogenies with endomorphism algebra K, there is a unique positive integer f coprime to ℓ such that the endomorphism ring of any elliptic curve at level i is isomorphic to $\mathbf{Z} + \ell^i f\mathcal{O}_K$. The linear structure $\mathbf{Z} + f\mathcal{O}_K \supset \mathbf{Z} + \ell f\mathcal{O}_K \supset \mathbf{Z} + \ell^2 f\mathcal{O}_K \supset \dots$ corresponds to the levels of the volcano.

As a motivation for our search of similar graph structures in higher dimensions, let us sketch a simple application of isogeny volcanoes: the computation of the endomorphism ring of an elliptic curve E defined over a finite field $k = \mathbf{F}_q$. First, one can find the endomorphism algebra $K = \mathbf{Q}(\pi)$ by computing the characteristic polynomial of the Frobenius endomorphism π. This polynomial is of the form $X^2 - tX + q$, where t is called the trace of Frobenius. This trace is related to the number of rational points of

the curve by the equation $|E(\mathbf{F}_q)| = q + 1 - t$, and there are efficient methods to count rational points in elliptic curves (notably the Schoof-Elkies-Atkin algorithm [Sch95] in large characteristic, and p-adic methods [Sat00] in small characteristic). Once K is known, it remains to determine which order $\mathcal{O}$ corresponds to the endomorphism ring. Due to the classification of orders in quadratic fields, it is sufficient to retrieve the conductor $f \in \mathbf{Z}$ of the order. First, we know that this order contains the Frobenius endomorphism π. The discriminant of $\mathbf{Z}[\pi]$ is $d_\pi = t^2 - 4q$, and its conductor f_π is the largest integer such that f_π^2 divides d_π and $d_\pi/f_\pi^2 \equiv 0$ or $1 \mod 4$. For ordinary elliptic curves, f_π is not divisible by the characteristic of k. Since $\mathcal{O}$ contains $\mathbf{Z}[\pi]$, we deduce that f divides f_π. For each prime divisor ℓ of f_π, it remains to determine the valuation of f at ℓ. As already mentioned, this valuation at ℓ coincides with the level of our elliptic curve E in the isogeny volcano. And in fact, the level of E can easily be determined by computing a few isogenies of degree ℓ. If there is only one isogeny out of E (over the field k), then E is at the bottom of the volcano, and the valuation of f at ℓ equals the valuation of f_π at ℓ. Otherwise, there are at least three outgoing isogenies, so construct three distinct, non-backtracking paths of ℓ-isogenies from E until one of them reaches a dead-end. This path must have reached the bottom of the volcano, and since it was non-backtracking and the shortest of three, it must be a straight path down, so that its length is exactly the distance from E to the bottom. We know that the bottom level is the valuation of f_π at ℓ, and we can deduce the valuation of f at ℓ.

5.1.2. Almost volcanoes in higher dimension. For higher-dimensional ordinary abelian varieties, graph descriptions are largely unknown. The role played by imaginary quadratic fields for elliptic curves is now played by CM-fields of higher degree. The key obstruction to generalising Kohel's results to higher dimension is the relative complexity of the set of orders in CM-fields of arbitrary degree. The case of elliptic curves and imaginary quadratic fields enjoys a complete and simple classification, but even for quartic CM-fields, the orders are not easy to classify.

The *real endomorphism ring* of an absolutely simple ordinary abelian variety is the ring of totally real elements in its endomorphism ring. We say that the real endomorphism ring is maximal if it is integrally closed in its field of fractions. The real endomorphism ring of an ordinary elliptic curve is $\mathbf{Z}$, so it is always maximal. Isogeny volcanoes of elliptic curves are therefore naturally isogeny graphs of abelian varieties with maximal real endomorphism ring. This maximality condition, which becomes non-trivial in higher dimension, turns out to be crucial to obtain "volcano-like" structures.

In higher dimension, the family of ℓ-isogenies (giving rise to the ℓ-isogeny volcanoes for elliptic curves) does not seem to be a pertinent choice, either practically or theoretically: not all ℓ-isogenies are efficiently computable, and at any rate, they do not provide the most enlightening graph structures. Theorem 5.13 provides a full description of graphs for a key family of isogenies called $\mathfrak{l}$-isogenies, in any dimension, and a number-theoretic condition is derived for determining when these graphs are volcanoes. These $\mathfrak{l}$-isogenies are isogenies whose kernels are proper subgroups of the $\mathfrak{l}$-torsion of ordinary abelian varieties, where $\mathfrak{l}$ is a fixed ideal in their real endomorphism ring that is assumed locally maximal (see Definition 5.11).

Thanks to this assumption, the proof of Theorem 5.13 avoids the difficult problem of classifying arbitrary orders in a CM-field by working with a well-behaved class: those whose intersection with the totally real subfield is maximal. This classification, which is Theorem 5.2, is a result in pure commutative algebra, which does not need any results about abelian varieties, or even about CM-fields.

5.1.3. Levels of real multiplication for abelian surfaces. Our next results specialise to the case of dimension 2. Using Theorem 5.13, we describe graphs of a second important family of isogenies, known as (ℓ, ℓ)-isogenies. These isogenies are isogenies of polarised abelian varieties whose kernels are maximal isotropic with respect to the Weil pairing; see Section 5.6 for the precise definition. The (ℓ, ℓ)-isogenies are important for the following reason: algorithms for computing isogenies of elliptic curves from a given kernel (such as Vélu's formulae [Vél71]) are difficult to generalise in higher dimension, as cyclic isogenies do not preserve the property of being principally polarisable in genus 2. The known methods such as [Ric37], [DL08], [Rob10], [LR12b], [Smi12], [BFT14], [Fly15], [CE15], [CR15] apply only to (ℓ, ℓ)-isogenies. Only the very recent method of [DJRV16] allows to compute isogenies of certain cyclic kernels. The interest in (ℓ, ℓ)-isogenies stems from the fact that they preserve principal polarisability, and are computable with the algorithms of [CR15].

We provide two structural results on (ℓ, ℓ)-isogenies. First, Theorem 5.36 gives a local description of the graph of all (ℓ, ℓ)-isogenies by analysing how these isogenies can change the real endomorphism ring. Second, we provide in Proposition 5.63 a complete description of the subgraph of (ℓ, ℓ)-isogenies which preserve maximal real multiplication, the key input to which is Theorem 5.37, describing the local structure of this graph.

These structures lead to a "going up" algorithm (Algorithm 5.1). This algorithm, given as input a principally polarised abelian surface and a prime ℓ, finds a path of computable isogenies leading to an abelian surface whose endomorphism ring is maximal at ℓ, when it exists (our result also precisely characterises when it does not exist). It has various applications, in particular in generating curves of genus 2 over finite fields with suitable security parameters via the CM method, in extending results about the random self-reducibility of the discrete logarithm problem in genus 2 cryptography, or in finding explicit isogenies between two isogenous principally polarised abelian surfaces. Applications are discussed in more detail in Section 5.9.1.

5.1.4. Previous work. Before describing the proofs of these results, we mention some previous work. Following Kohel's techniques, Bisson [Bis15, Chapter 5] sketched the relation between isogeny graphs and the lattice of orders in the endomorphism algebra for abelian varieties of higher dimension. This provides a first approximation of the global structure of the graphs, but allows no fine-grained analysis.

Ionica and Thomé [IT14] observed that the graph of (ℓ, ℓ)-isogenies, when restricted to surfaces with maximal real endomorphism ring, could be studied through what they called $\mathfrak{l}$-isogenies, where $\mathfrak{l}$ is a prime ideal above ℓ in the maximal real endomorphism ring. Even though their definition of $\mathfrak{l}$-isogeny differs from ours, it does coincide in the particular case they analyse (i.e., in dimension 2, when the real endomorphism ring has trivial class group, and $\mathfrak{l}$ is above a split prime).

Finally, if $\mathfrak{l}$ is principal, of prime norm, generated by a real, totally positive endomorphism β, then $\mathfrak{l}$-isogenies coincide with the cyclic β-isogenies of [DJRV16] — an important notion, since these are the cyclic isogenies preserving principal polarisability. In parallel to the present work, Chloe Martindale has recently announced a similar result on cyclic β-isogenies, that can be found in her Ph.D. thesis [Mar18].

5.1.5. Proof strategy: ℓ-adic lattices and Tate's theorem. The results above are proven using a different approach from the currently available analyses of the structure of ℓ-power isogeny graphs. Rather than working with complex tori via the theory of canonical lifts (presented in Section 3.2), we attach to an ℓ-isogeny of abelian varieties

a pair of lattices in an ℓ-adic symplectic space, whose relative position is determined by the kernel of the isogeny, following the proof of Tate's isogeny theorem [Tat66].

Inspired by [CV04, Section 6], where the theory of Hecke operators on GL_2 is used to understand the CM elliptic curves isogenous to a fixed curve, we analyse the possible local endomorphism rings (i.e., the tensor products of endomorphism rings with $\mathbf{Q}_\ell$) for an analogous notion of "neighboring" lattices.

This perspective also explains why our most complete results are restricted to abelian varieties with maximal real endomorphism ring: the techniques of [CV04], which reduce questions about arbitrary free modules over a ring to sublattices of its field of fractions, rely on that ring satisfying the Gorenstein property. This property holds for all quadratic orders and for any order with maximal real suborder (Lemma 5.14), but not for a general order (even in a quartic field).

5.2. Orders with maximal real multiplication

Before considering any isogeny or abelian variety, we prove a classification theorem for orders in quadratic extensions. This classification lays the groundwork for our "vertical" study of isogeny graphs.

Recall that an order in a number field is a full rank $\mathbf{Z}$-lattice which is also a subring. If ℓ is a prime, and L is a finite extension of $\mathbf{Q}_\ell$ or a finite product of finite extensions of $\mathbf{Q}_\ell$, an order in L is a subring of $\mathcal{O}_L$ that is also a full rank $\mathbf{Z}_\ell$-lattice. If K is a number field, write $K_\ell = K \otimes_{\mathbf{Q}} \mathbf{Q}_\ell$.

Given a number field K and a sequence $R(\ell)$ of orders in K_ℓ, such that $R(\ell)$ is the maximal order in K_ℓ for almost all ℓ, it is a classical consequence of the strong approximation theorem for SL_n that there exists a unique order $\mathcal{O}$ in K such that $\mathcal{O} \otimes_{\mathbf{Z}} \mathbf{Z}_\ell = R(\ell)$ for all ℓ. In fact, $\mathcal{O}$ can be recovered as $\mathcal{O} = \bigcap_\ell (R(\ell) \cap K)$.

Suppose that K^+ is a number field or a finite product of extensions of $\mathbf{Q}_\ell$ for some fixed prime ℓ, and let K be a quadratic extension of K^+ (i.e., an algebra of the form $K^+[x]/f(x)$, where f is a separable quadratic polynomial). The non-trivial element of $\mathrm{Aut}(K/K^+)$ will be denoted $\dagger$. In the case that K is a CM-field and K^+ its maximally real subfield, Goren and Lauter [GL09] proved that if K^+ has a trivial class group, the orders with maximal real multiplication, i.e., the orders containing $\mathcal{O}_{K^+}$, are characterized by their conductor — under the assumption that ideals of $\mathcal{O}_K$ fixed by $\mathrm{Gal}(K/K^+)$ are ideals of $\mathcal{O}_{K^+}$ augmented to $\mathcal{O}_K$, which is rather restrictive, since it implies that no finite prime of K^+ ramifies in K. In that case, these orders are exactly the orders $\mathcal{O}_{K^+} + \mathfrak{f}_+\mathcal{O}_K$, for any ideal $\mathfrak{f}_+$ in $\mathcal{O}_{K^+}$. We generalise this result to an arbitrary quadratic extension; abusing language, we will continue to say an order of K has "maximal real multiplication" if it contains $\mathcal{O}_{K^+}$ even if the field extension in question is not a CM extension. Recall the conductor $\mathfrak{f}$ of an order $\mathcal{O}$ in K is defined as

$$\mathfrak{f} = \{x \in K \mid x\mathcal{O}_K \subseteq \mathcal{O}\},$$

and is the largest subset of K which is an ideal in both $\mathcal{O}_K$ and $\mathcal{O}$.

Theorem 5.2. *The map $\mathfrak{f}_+ \mapsto \mathcal{O}_{K^+} + \mathfrak{f}_+\mathcal{O}_K$ is a bijection between the set of ideals in $\mathcal{O}_{K^+}$ and the set of orders in K containing $\mathcal{O}_{K^+}$. More precisely,*

(i) for any ideal $\mathfrak{f}_+$ in $\mathcal{O}_{K^+}$, the conductor of $\mathcal{O}_{K^+} + \mathfrak{f}_+\mathcal{O}_K$ is $\mathfrak{f}_+\mathcal{O}_K$, and
(ii) for any order $\mathcal{O}$ in K with maximal real multiplication and conductor $\mathfrak{f}$, one has $\mathcal{O} = \mathcal{O}_{K^+} + (\mathfrak{f} \cap \mathcal{O}_{K^+})\mathcal{O}_K$.

Lemma 5.3. *An order $\mathcal{O}$ in K is stable under $\dagger$ if and only if $\mathcal{O} \cap K^+ = (\mathcal{O} + \mathcal{O}^\dagger) \cap K^+$.*

Proof. The direct implication is obvious. For the other direction, suppose that $\mathcal{O} \cap K^+ = (\mathcal{O} + \mathcal{O}^\dagger) \cap K^+$, and let $x \in \mathcal{O}$. Then, $x + x^\dagger \in (\mathcal{O} + \mathcal{O}^\dagger) \cap K^+ = \mathcal{O} \cap K^+ \subset \mathcal{O}$, which proves that $x^\dagger \in \mathcal{O}$. □

Lemma 5.4. *Let $\mathfrak{f}$ and $\mathfrak{g}$ be two ideals in $\mathcal{O}_K$, such that $\mathfrak{g}$ divides $\mathfrak{f}$. Let $\pi : \mathcal{O}_K \to \mathcal{O}_K/\mathfrak{f}$ be the natural projection. The canonical isomorphism between $(\mathcal{O}_{K^+} + \mathfrak{f})/\mathfrak{f}$ and $\mathcal{O}_{K^+}/(\mathcal{O}_{K^+} \cap \mathfrak{f})$ induces a bijection between $\pi(\mathcal{O}_{K^+}) \cap \pi(\mathfrak{g})$ and $(\mathcal{O}_{K^+} \cap \mathfrak{g})/(\mathcal{O}_{K^+} \cap \mathfrak{f})$.*

Proof. Any element in $\pi(\mathcal{O}_{K^+}) \cap \pi(\mathfrak{g})$ can be written as $\pi(x) = \pi(y)$ for some $x \in \mathcal{O}_{K^+}$ and $y \in \mathfrak{g}$. Then, $x - y \in \mathfrak{f} \subset \mathfrak{g}$, so $x = (x - y) + y \in \mathfrak{g}$. So

$$\pi(\mathfrak{g}) \cap \pi(\mathcal{O}_{K^+}) = \pi(\mathfrak{g} \cap \mathcal{O}_{K^+}) \cong (\mathfrak{g} \cap \mathcal{O}_{K^+})/(\mathfrak{f} \cap \mathcal{O}_{K^+}),$$

where the last relation comes from the canonical isomorphism between the rings $(\mathcal{O}_{K^+} + \mathfrak{f})/\mathfrak{f}$ and $\mathcal{O}_{K^+}/(\mathcal{O}_{K^+} \cap \mathfrak{f})$. □

Lemma 5.5. *Let $\mathcal{O}$ be an order in K of conductor $\mathfrak{f}$ with maximal real multiplication. Then, $\mathcal{O}$ is stable under $\dagger$ and $\mathfrak{f}$ comes from an ideal of $\mathcal{O}_{K^+}$, i.e., $\mathfrak{f} = \mathfrak{f}_+\mathcal{O}_K$, where $\mathfrak{f}_+$ is the $\mathcal{O}_{K^+}$-ideal $\mathfrak{f} \cap \mathcal{O}_{K^+}$.*

Proof. From Lemma 5.3, it is obvious that any order with maximal real multiplication is stable under $\dagger$. Its conductor $\mathfrak{f}$ is thereby a $\dagger$-stable ideal of $\mathcal{O}_K$. For any prime ideal $\mathfrak{p}_+$ in $\mathcal{O}_{K^+}$, let $\mathfrak{f}_{\mathfrak{p}_+}$ be the part of the factorization of $\mathfrak{f}$ that consists of prime ideals above $\mathfrak{p}_+$. Then, $\mathfrak{f} = \prod_{\mathfrak{p}_+} \mathfrak{f}_{\mathfrak{p}_+}$, and each $\mathfrak{f}_{\mathfrak{p}_+}$ is $\dagger$-stable. It is easy to see that each $\mathfrak{f}_{\mathfrak{p}_+}$ comes from an ideal of $\mathcal{O}_{K^+}$ when $\mathfrak{p}_+$ is inert or splits in $\mathcal{O}_K$. Now suppose it ramifies as $\mathfrak{p}_+\mathcal{O}_K = \mathfrak{p}^2$. Then $\mathfrak{f}_{\mathfrak{p}_+}$ is of the form $\mathfrak{p}^\alpha$. If α is even, $\mathfrak{f}_{\mathfrak{p}_+} = \mathfrak{p}_+^{\alpha/2}\mathcal{O}_K$. We now need to prove that α cannot be odd.

By contradiction, suppose $\alpha = 2\beta + 1$ for some integer β. Let $\pi : \mathcal{O}_K \to \mathcal{O}_K/\mathfrak{f}$ be the canonical projection. The ring $\pi(\mathcal{O})$ contains $\pi(\mathcal{O}_{K^+}) = (\mathcal{O}_{K^+} + \mathfrak{f})/\mathfrak{f}$. Write $\mathfrak{f} = \mathfrak{p}^\alpha\mathfrak{g}$. We will show that $\pi(\mathfrak{p}^{\alpha-1}\mathfrak{g}) \subset \pi(\mathcal{O}_{K^+})$. From Lemma 5.4,

$$\left|\pi(\mathcal{O}_{K^+}) \cap \pi(\mathfrak{p}^{\alpha-1}\mathfrak{g})\right| = |\mathfrak{p}_+^\beta\mathfrak{g}/\mathfrak{p}_+^{\beta+1}\mathfrak{g}| = N(\mathfrak{p}_+) = N(\mathfrak{p}) = |\pi(\mathfrak{p}^{\alpha-1}\mathfrak{g})|,$$

where N denotes the absolute norm, so $\pi(\mathfrak{p}^{\alpha-1}\mathfrak{g}) \subset \pi(\mathcal{O}_{K^+}) \subset \pi(\mathcal{O})$. Finally,

$$\mathfrak{p}^{\alpha-1}\mathfrak{g} = \pi^{-1}(\pi(\mathfrak{p}^{\alpha-1}\mathfrak{g})) \subset \pi^{-1}(\pi(\mathcal{O})) = \mathcal{O},$$

which contradicts the fact that $\mathfrak{f}$ is the biggest ideal of $\mathcal{O}_K$ contained in $\mathcal{O}$. □

Lemma 5.6. *Let $\mathfrak{f}_+$ be an ideal in $\mathcal{O}_{K^+}$, and $R = \mathcal{O}_{K^+}/\mathfrak{f}_+$. There is an element $\alpha \in \mathcal{O}_K$ such that $\mathcal{O}_K/\mathfrak{f}_+\mathcal{O}_K = R \oplus R\alpha$.*

Proof. The order $\mathcal{O}_K$ is a module over $\mathcal{O}_{K^+}$. It is locally free, and finitely generated, thus it is projective. Since $\mathcal{O}_{K^+}$ is a regular ring, the submodule $\mathcal{O}_{K^+}$ in $\mathcal{O}_K$ is a direct summand, i.e., there is an $\mathcal{O}_{K^+}$-submodule M of $\mathcal{O}_K$ such that $\mathcal{O}_K = \mathcal{O}_{K^+} \oplus M$. Then, $\mathcal{O}_K/\mathfrak{f}_+\mathcal{O}_K = R \oplus M/\mathfrak{f}_+M$. Let A be $\mathbf{Z}$ if K is a number field and $\mathbf{Z}_p$ if it is a finite product of extensions of $\mathbf{Q}_p$. In the number field case, write n for $[K : \mathbf{Q}]$, and in the local case, write n for the dimension of K_p as a $\mathbf{Q}_p$-vector space. As modules over A, one has that $\mathcal{O}_K$ is of rank $2n$ and $\mathcal{O}_{K^+}$ of rank n, hence M must be of rank n. Therefore, as an $\mathcal{O}_{K^+}$-module, M is isomorphic to an ideal $\mathfrak{a}$ in $\mathcal{O}_{K^+}$, so $M/\mathfrak{f}_+M \cong \mathfrak{a}/\mathfrak{f}_+\mathfrak{a} \cong R$. So there is an element $\alpha \in M$ such that $M/\mathfrak{f}_+M = R\alpha$. □

Proof of Theorem 5.2. For (i), let $\mathfrak{f}_+$ be an ideal in $\mathcal{O}_{K^+}$, and write $\mathfrak{f} = \mathfrak{f}_+\mathcal{O}_K$. Let $\mathfrak{c}$ be the conductor of $\mathcal{O}_{K^+} + \mathfrak{f}$. From Lemma 5.5, $\mathfrak{c}$ is of the form $\mathfrak{c}_+\mathcal{O}_K$ where $\mathfrak{c}_+ = \mathcal{O}_{K^+} \cap \mathfrak{c}$.

Clearly $\mathfrak{f} \subset \mathfrak{c}$, so $\mathfrak{c}_+ \mid \mathfrak{f}_+$ and we can write $\mathfrak{f}_+ = \mathfrak{c}_+\mathfrak{g}_+$. Let $\pi : \mathcal{O}_K \to \mathcal{O}_K/\mathfrak{f}$ be the canonical projection. Since $\mathfrak{c} \subset \mathcal{O}_{K^+} + \mathfrak{f}$, we have $\pi(\mathfrak{c}) \subset \pi(\mathcal{O}_{K^+})$. From Lemma 5.4,

$$|\pi(\mathfrak{c})| = |\pi(\mathcal{O}_{K^+}) \cap \pi(\mathfrak{c})| = |\mathfrak{c}_+/\mathfrak{f}_+| = N(\mathfrak{g}_+).$$

On the other hand, $|\pi(\mathfrak{c})| = |\mathfrak{c}/\mathfrak{f}| = N(\mathfrak{g}_+\mathcal{O}_K) = N(\mathfrak{g}_+)^2$, so $N(\mathfrak{g}_+) = 1$, hence $\mathfrak{c} = \mathfrak{f}$.

To prove (ii), let $\mathcal{O}$ be an order in K with maximal real multiplication and conductor $\mathfrak{f}$. From Lemma 5.5, $\mathcal{O}$ is $\dagger$-stable and $\mathfrak{f} = \mathfrak{f}_+\mathcal{O}_K$, where $\mathfrak{f}_+ = \mathfrak{f} \cap \mathcal{O}_{K^+}$. We claim that if $x \in \mathcal{O}$ then $x \in \mathcal{O}_{K^+} + \mathfrak{f}$. Let $R = \mathcal{O}_{K^+}/\mathfrak{f}_+$. By Lemma 5.6, $\mathcal{O}_K/\mathfrak{f} = R \oplus R\alpha$. The quotient $\mathcal{O}/\mathfrak{f}$ is an R-submodule of $\mathcal{O}_K/\mathfrak{f}$.

There are two elements $y, z \in R$ such that $x + \mathfrak{f} = y + z\alpha$. Then, $z\alpha \in \mathcal{O}/\mathfrak{f}$, and we obtain that $(zR)\alpha \subset \mathcal{O}/\mathfrak{f}$. There exists an ideal $\mathfrak{g}_+$ dividing $\mathfrak{f}_+$ such that $zR = \mathfrak{g}_+/\mathfrak{f}_+$. Therefore $(\mathfrak{g}_+/\mathfrak{f}_+)\alpha \subset \mathcal{O}/\mathfrak{f}$. Then,

$$\mathfrak{g}/\mathfrak{f} \subset R + (\mathfrak{g}_+/\mathfrak{f}_+)\alpha \subset \mathcal{O}/\mathfrak{f},$$

where $\mathfrak{g} = \mathfrak{g}_+\mathcal{O}_K$, which implies that $\mathfrak{g} \subset \mathcal{O}$. But $\mathfrak{g}$ divides $\mathfrak{f}$, and $\mathfrak{f}$ is the largest $\mathcal{O}_K$-ideal in $\mathcal{O}$, so $\mathfrak{g} = \mathfrak{f}$. Hence $z \in \mathfrak{f}$, and $x \in \mathcal{O}_{K^+} + \mathfrak{f}$. □

5.3. From abelian varieties to lattices, and vice-versa

For the remainder of the chapter, let $k = \mathbf{F}_q$ be a finite field. Fix an ordinary, absolutely simple abelian variety $\mathscr{A}$ defined over k. Let $K = \mathrm{End}(\mathscr{A}) \otimes_{\mathbf{Z}} \mathbf{Q}$ be its endomorphism algebra, and let K^+ be its maximal totally real subfield. Recall that $[K^+ : \mathbf{Q}] = \dim(\mathscr{A})$ and $[K : K^+] = 2$. We denote by $x \mapsto x^\dagger$ the generator of the Galois group $\mathrm{Gal}(K/K^+)$. We assume the notation introduced in Section 3.1.2, and in particular, the embedding $\imath_{\mathscr{B}} : \mathrm{End}(\mathscr{B}) \to K$ for any variety $\mathscr{B}$ that is isogenous to $\mathscr{A}$, and its image $\mathcal{O}(\mathscr{B})$, the order in K corresponding to the endomorphism ring of $\mathscr{B}$. Define the real suborder $\mathcal{O}^+(\mathscr{A}) = \mathcal{O}(\mathscr{A}) \cap K^+$. The variety $\mathscr{A}$ is said to have *real multiplication* (RM) by the order $\mathcal{O}^+(\mathscr{A})$.

Fix once and for all a prime number ℓ different from the characteristic of the finite field k, and write $\mathfrak{o}(\mathscr{A}) = \mathcal{O}(\mathscr{A}) \otimes_{\mathbf{Z}} \mathbf{Z}_\ell$, the *local order* of $\mathscr{A}$. It is an order in the algebra $K_\ell = K \otimes_{\mathbf{Q}} \mathbf{Q}_\ell$. Also, $\mathfrak{o}_K = \mathcal{O}_K \otimes_{\mathbf{Z}} \mathbf{Z}_\ell$ is the maximal order in K_ℓ. Finally, write $\mathfrak{o}^+(\mathscr{A})$ for the *local real order* $\mathcal{O}^+(\mathscr{A}) \otimes_{\mathbf{Z}} \mathbf{Z}_\ell$, which is an order in the algebra $K_\ell^+ = K^+ \otimes_{\mathbf{Q}} \mathbf{Q}_\ell$, and let $\mathfrak{o}_{K^+} = \mathcal{O}_{K^+} \otimes_{\mathbf{Z}} \mathbf{Z}_\ell$.

For the reader who is frustrated with the excessive notation for orders, the following general rules may be helpful: orders named with capital letters always live in global fields, with lowercase letters in (finite products of) local fields; orders in the totally real field and its completions always take the superscript +.

5.3.1. Tate modules and isogenies. For any positive integer n, the multiplication by ℓ induces a natural morphism $\mathscr{A}[\ell^{n+1}] \to \mathscr{A}[\ell^n]$. The inverse limit of the sequence of groups $\mathscr{A}[\ell^n]$ with respect to these maps is the ℓ-adic Tate module

$$T_\ell\mathscr{A} = \varprojlim_n \mathscr{A}[\ell^n].$$

Let $T = T_\ell\mathscr{A}$ be the Tate module of $\mathscr{A}$, and let V be the $\mathbf{Q}_\ell$ vector space $T \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$. Then V is a $2g$-dimensional $\mathbf{Q}_\ell$-vector space with an action of the algebra K_ℓ, over which it has rank one, and T is similarly of rank one over the ring $\mathfrak{o}(\mathscr{A}) = \mathcal{O}(\mathscr{A}) \otimes_{\mathbf{Z}} \mathbf{Z}_\ell$. Write π for the Frobenius endomorphism of $\mathscr{A}$, viewed as an element of $\mathcal{O}(\mathscr{A})$.

The elements of T are the sequences $(Q_n)_{n\geq 0}$ with $Q_n \in \mathscr{A}[\ell^n]$, such that $\ell Q_n = Q_{n-1}$ for all $n \geq 1$. An element of V identifies with a sequence $(P_n)_{n\geq 0}$ with $P_n \in \mathscr{A}[\ell^\infty]$

and $\ell P_n = P_{n-1}$ for $n \geq 1$ as follows:

$$(Q_n)_{n\geq 0} \otimes \ell^{-m} \longmapsto (Q_{n+m})_{n\geq 0},$$

and under this identification, T is the subgroup of V where $P_0 = 0 \in \mathscr{A}[\ell^\infty]$. The projection to the zeroth coordinate then yields a canonical identification

$$V/T \xrightarrow{\sim} \mathscr{A}[\ell^\infty](\overline{k}), \tag{5.1}$$

under which the action of π on the left-hand side corresponds to the action of the arithmetic Frobenius element in $\mathrm{Gal}(\overline{k}/k)$ on the right-hand side.

The main correspondence between lattices in V containing the Tate module T and ℓ-power isogenies from $\mathscr{A}$ is given by the following proposition which is essentially Tate's isogeny theorem (see, e.g., [Wat69, Section 3]):

Proposition 5.7. *There is a one-to-one correspondence*

$$\{\textit{lattices in } V \textit{ containing } T\} \cong \{\textit{finite subgroups of } \mathscr{A}[\ell^\infty]\},$$

where a lattice Γ *is sent to the subgroup* Γ/T*, through the identification* (5.1)*. Under this correspondence,*

(i) a lattice is stable under π^n *if and only if the corresponding subgroup is defined over the degree* n *extension* $\mathbf{F}_{q^n}$ *of* k*, and*
(ii) if a subgroup $\kappa \subset \mathscr{A}[\ell^\infty]$ *corresponds to a lattice* Γ*, then the order of* K_ℓ *of elements stabilising* Γ *is* $\mathfrak{o}(\mathscr{A}/\kappa)$*.*

Remark 5.8. For a finite subgroup $\kappa \subset \mathscr{A}[\ell^\infty]$, any two isogenies of kernel κ differ by an isomorphism of the targets and hence, if $\varphi : \mathscr{A} \to \mathscr{B}$ is any isogeny of kernel κ, then $\mathfrak{o}(\mathscr{A}/\kappa) = \mathfrak{o}(\mathscr{B})$.

Remark 5.9. All varieties and morphisms are *a priori* considered over $\overline{k}$. Since we are also interested in the structures arising from varieties and morphisms defined over k, we note that if a simple, ordinary abelian variety $\mathscr{B}$ is k-isogenous to $\mathscr{A}$, then any isogeny $\mathscr{A} \to \mathscr{B}$ is defined over k (this is an easy consequence of [Wat69, Theorem 7.2.]). By Proposition 5.7(ii), if $\pi \in \mathfrak{o}(\mathscr{A}/\kappa)$, then κ is defined over k, and is thereby the kernel of a k-isogeny[1], so subgroups κ defined over k correspond to lattices Γ stable under π.

5.3.2. Global and local endomorphism rings. The following proposition justifies the strategy of working locally at ℓ, as it guarantees that ℓ-power isogenies do not affect endomorphism rings at primes $\ell' \neq \ell$.

Proposition 5.10. *Let* $\varphi : \mathscr{A} \to \mathscr{B}$ *be an isogeny of abelian varieties of* ℓ*-power degree. Then for any prime* $\ell' \neq \ell$ *of* $\mathscr{A}$*, one has* $\mathcal{O}(\mathscr{A}) \otimes_{\mathbf{Z}} \mathbf{Z}_{\ell'} = \mathcal{O}(\mathscr{B}) \otimes_{\mathbf{Z}} \mathbf{Z}_{\ell'}$*.*

Proof. Let $\mathcal{C}_{\ell'}$ be the category whose objects are abelian varieties over $\overline{k}$ and whose morphisms are $\mathrm{Hom}_{\mathcal{C}_{\ell'}}(\mathscr{A}_1, \mathscr{A}_2) = \mathrm{Hom}(\mathscr{A}_1, \mathscr{A}_2) \otimes_{\mathbf{Z}} \mathbf{Z}_{\ell'}$. There exists an isogeny $\hat{\varphi} : \mathscr{B} \to \mathscr{A}$ such that $\hat{\varphi} \circ \varphi = [\ell^n]$, so φ induces an isomorphism in $\mathcal{C}_{\ell'}$; it follows that the endomorphism rings of $\mathscr{A}$ and $\mathscr{B}$ in this category are identified. □

5.4. Graphs of $\mathfrak{l}$-isogenies

In this section we study $\mathfrak{l}$-isogenies through the lens of lattices in an ℓ-adic vector space, endowed with an action of the algebra K_ℓ.

[1]Note that in general, if $\mathscr{B}$ is $\overline{k}$-isogenous to $\mathscr{A}$ and $\pi \in \mathcal{O}(\mathscr{B})$, then π does not necessarily correspond to the k-Frobenius of $\mathscr{B}$ unless $\mathscr{B}$ is actually k-isogenous to $\mathscr{A}$.

5.4.1. Definition of the graph and statement of results. To state the result, we review the definitions of $\mathfrak{l}$-isogenies and the associated graph.

Definition 5.11 ($\mathfrak{l}$-isogeny)**.** Let $\mathfrak{l}$ be a prime above ℓ in K^+, and $\mathscr{A}$ a variety in the fixed isogeny class. Suppose $\mathfrak{l}$ is coprime to the conductor of $\mathcal{O}^+(\mathscr{A})$. An $\mathfrak{l}$-isogeny from $\mathscr{A}$ is an isogeny whose kernel is a proper, $\mathcal{O}^+(\mathscr{A})$-stable subgroup of[2] $\mathscr{A}[\mathfrak{l}]$. Note that the degree of an $\mathfrak{l}$-isogeny is $N(\mathfrak{l})$ (the norm of $\mathfrak{l}$).

The graph $\mathscr{W}_\mathfrak{l}$ is defined precisely as follows: its vertices are the isomorphism classes of abelian varieties $\mathscr{A}$ in the fixed isogeny class, which have maximal real multiplication locally at ℓ (i.e., $\mathfrak{o}_{K^+} \subset \mathfrak{o}(\mathscr{A})$), and there is a directed edge of multiplicity m from such a vertex with representative $\mathscr{A}$ to a vertex $\mathscr{B}$ if there are m distinct subgroups $\kappa \subset \mathscr{A}$ that are kernels of $\mathfrak{l}$-isogenies such that $\mathscr{A}/\kappa \cong \mathscr{B}$ (of course, the multiplicity m does not depend on the choice of the representative $\mathscr{A}$).

Remark 5.12. When $\mathfrak{l}$ is trivial in the narrow class group of K^+, then $\mathfrak{l}$-isogenies preserve principal polarisability. The graph $\mathscr{W}_\mathfrak{l}$ does not account for polarisations, but it is actually easy to add polarisations back to graphs of unpolarised varieties, as will be discussed in Section 5.5.

Each vertex $\mathscr{A}$ of this graph $\mathscr{W}_\mathfrak{l}$ has a level given by the valuation $v_\mathfrak{l}(\mathscr{A})$ at $\mathfrak{l}$ of the conductor of $\mathcal{O}(\mathscr{A})$. Theorem 5.13 completely describes the structure of the connected components of $\mathscr{W}_\mathfrak{l}$, which turns out to be closely related to the volcanoes observed for cyclic isogenies of elliptic curves. The rest of this section is dedicated to the proof of this theorem.

Theorem 5.13. *Let $\mathscr{V}$ be any connected component of the levelled $\mathfrak{l}$-isogeny graph $(\mathscr{W}_\mathfrak{l}, v_\mathfrak{l})$. For each $i \geq 0$, let $\mathscr{V}_i$ be the subgraph of $\mathscr{V}$ at level i. We have:*

- *(i) For each $i \geq 0$, the varieties in $\mathscr{V}_i$ share a common endomorphism ring $\mathcal{O}_i$. The order $\mathcal{O}_0$ can be any order with locally maximal real multiplication at ℓ, whose conductor is not divisible by $\mathfrak{l}$;*
- *(ii) The level $\mathscr{V}_0$ is isomorphic to the Cayley graph of the subgroup of $\mathrm{Cl}(\mathcal{O}_0)$ with generators the prime ideals above $\mathfrak{l}$; fixing a vertex $\mathscr{A}$ of $\mathscr{V}_0$, an isomorphism is given by sending any ideal class $[\mathfrak{a}]$ to the isomorphism class of $\mathscr{A}/\mathscr{A}[\mathfrak{a}]$;*
- *(iii) For any $\mathscr{A} \in \mathscr{V}_0$, there are $\left(N(\mathfrak{l}) - \left(\frac{K}{\mathfrak{l}}\right)\right)/[\mathcal{O}_0^\times : \mathcal{O}_1^\times]$ edges of multiplicity $[\mathcal{O}_0^\times : \mathcal{O}_1^\times]$ from $\mathscr{A}$ to distinct vertices of $\mathscr{V}_1$ (where $\left(\frac{K}{\mathfrak{l}}\right)$ is -1, 0 or 1 if $\mathfrak{l}$ is inert, ramified, or split in K); these edges, plus the ones in $\mathscr{V}_0$, are all the edges from $\mathscr{A}$;*
- *(iv) For each $i > 0$, and any $\mathscr{A} \in \mathscr{V}_i$, there is one simple edge from $\mathscr{A}$ to a vertex of $\mathscr{V}_{i-1}$, and $N(\mathfrak{l})/[\mathcal{O}_i^\times : \mathcal{O}_{i+1}^\times]$ edges of multiplicity $[\mathcal{O}_i^\times : \mathcal{O}_{i+1}^\times]$ to distinct vertices of $\mathscr{V}_{i+1}$, and there is no other edge from $\mathscr{A}$;*
- *(v) For each path $\mathscr{A} \to \mathscr{B} \to \mathscr{C}$ where $\mathscr{A}$ and $\mathscr{C}$ are at some level i, and $\mathscr{B}$ at level $i+1$, we have $\mathscr{C} \cong \mathscr{A}/\mathscr{A}[\mathfrak{l}]$;*
- *(vi) For each edge $\mathscr{B} \to \mathscr{C}$ where $\mathscr{B}$ is at some level i and $\mathscr{C}$ is at level $i-1$, there is an edge $\mathscr{C} \to \mathscr{B}/\mathscr{B}[\mathfrak{l}]$, and $\mathscr{B}/\mathscr{B}[\mathfrak{l}]$ is at level i.*

In particular, the graph $\mathscr{V}$ is an $N(\mathfrak{l})$-volcano if and only if $\mathcal{O}_0^\times \subset K^+$ and $\mathfrak{l}$ is principal in $\mathcal{O}_0 \cap K^+$.

Also, if $\mathscr{V}$ contains a variety defined over the finite field k, the subgraph containing only the varieties defined over k consists of the subgraph of the first v levels, where v is the valuation at $\mathfrak{l}$ of the conductor of $\mathcal{O}_{K^+}[\pi] = \mathcal{O}_{K^+}[\pi, \pi^\dagger]$.

[2] By abuse of notation, we write $\mathscr{A}[\mathfrak{l}]$ in place of $\mathscr{A}[\mathfrak{l} \cap \mathcal{O}(\mathscr{A})]$.

5.4.2. Lattices with locally maximal real multiplication. Throughout this subsection, V is a $\mathbf{Q}_\ell$-vector space of dimension $2g$, where ℓ is a fixed prime number, and K is a degree $2g$ CM-field, with K^+ its maximal real subfield. The algebra K_ℓ is a $\mathbf{Q}_\ell$-algebra of dimension $2g$. Suppose that it acts ($\mathbf{Q}_\ell$-linearly) on V. Define the *order* of a full-rank $\mathbf{Z}_\ell$-lattice $\Lambda \subset V$ as

$$\mathfrak{o}(\Lambda) = \{x \in K_\ell \mid x\Lambda \subset \Lambda\}.$$

For any order $\mathfrak{o}$ in K_ℓ, say that Λ is an $\mathfrak{o}$-lattice if $\mathfrak{o}(\Lambda) = \mathfrak{o}$. Fix a lattice Λ and suppose that $\mathfrak{o}(\Lambda)$ has maximal real multiplication, i.e., that $\mathfrak{o}(\Lambda)$ contains the maximal order $\mathfrak{o}_{K^+}$ of $K_\ell^+ = K^+ \otimes_{\mathbf{Q}} \mathbf{Q}_\ell$. We now need some results on Gorenstein rings (see Definition 3.10).

Lemma 5.14. *Let A be a Dedekind domain with field of fractions F, and let L be a quadratic extension of F. If $\mathcal{O}$ is any A-subalgebra of the integral closure of A in L, with $\mathcal{O} \otimes K = L$, then $\mathcal{O}$ is Gorenstein.*

Proof. The hypotheses and result are local on Spec$A$, so we may take A a principal ideal domain. Then $\mathcal{O}$ is a free A-module, which must be 2-dimensional. The element $1 \in \mathcal{O}$ is not an A-multiple of any element of $\mathcal{O}$, so there is a basis $\{1, \alpha\}$ for $\mathcal{O}$ as an A-module; clearly $\mathcal{O} = A[\alpha]$ as A-algebras. The result then follows from [BL94, Example 2.8]. □

By Lemma 5.14, the order $\mathfrak{o}(\Lambda)$, which has maximal real multiplication, is a Gorenstein ring and Λ is a free $\mathfrak{o}(\Lambda)$-module of rank 1. Recall the notation $\mathfrak{o}_K = \mathcal{O}_K \otimes_{\mathbf{Z}} \mathbf{Z}_\ell$ and $\mathfrak{o}_{K^+} = \mathcal{O}_{K^+} \otimes_{\mathbf{Z}} \mathbf{Z}_\ell$. For any ideal $\mathfrak{f}$ in $\mathfrak{o}_{K^+}$, let $\mathfrak{o}_\mathfrak{f} = \mathfrak{o}_{K^+} + \mathfrak{f}\mathfrak{o}_K$. From Theorem 5.2, all the orders containing $\mathfrak{o}_{K^+}$ are of this form.

Definition 5.15 ($\mathfrak{l}$-neighbors)**.** Let Λ be a lattice with maximal real multiplication, and let $\mathfrak{l}$ be a prime ideal in $\mathfrak{o}_{K^+}$. The set $\mathscr{L}_\mathfrak{l}(\Lambda)$ of $\mathfrak{l}$-*neighbors* of Λ consists of all the lattices Γ such that $\mathfrak{l}\Lambda \subset \Gamma \subset \Lambda$, and $\Gamma/\mathfrak{l}\Lambda \cong \mathfrak{o}_{K^+}/\mathfrak{l}$, i.e., $\Gamma/\mathfrak{l}\Lambda \in \mathbf{P}^1(\Lambda/\mathfrak{l}\Lambda)$.

Using Proposition 5.7, we easily obtain the following proposition:

Proposition 5.16. *With $T = T_\ell \mathscr{A}$, the $\mathfrak{l}$-isogenies $\mathscr{A} \to \mathscr{B}$ correspond, under the correspondence in Proposition 5.7, to the lattices Γ with $T \subset \Gamma \subset \mathfrak{l}^{-1}T$ and Γ/T is an $\mathfrak{o}_{K^+}/\mathfrak{l}$-subspace of dimension one of $(\mathfrak{l}^{-1}T)/T$.*

The following lemma is key to understanding $\mathfrak{l}$-neighbors. It arises from the technique employed by Cornut and Vatsal [CV04, Section 6] to study the action of a certain Hecke algebra on quadratic CM-lattices.

Lemma 5.17. *Let K be a CM-field, and K^+ its maximal real subfield. Let $\mathfrak{l}$ be a prime ideal in $\mathfrak{o}_{K^+}$, and $\mathbf{F} = \mathfrak{o}_{K^+}/\mathfrak{l}$. Let $\mathfrak{f}$ be an ideal in $\mathfrak{o}_{K^+}$ and $\mathfrak{o}_\mathfrak{f} = \mathfrak{o}_{K^+} + \mathfrak{f}\mathfrak{o}_K$. The action of $\mathfrak{o}_\mathfrak{f}^\times$ on the set of $\mathbf{F}$-lines $\mathbf{P}^1(\mathfrak{o}_\mathfrak{f}/\mathfrak{l}\mathfrak{o}_\mathfrak{f})$ factors through $\mathfrak{o}_\mathfrak{f}^\times/\mathfrak{o}_{\mathfrak{l}\mathfrak{f}}^\times$. Let $\mathfrak{L}$ be a prime in $\mathfrak{o}_\mathfrak{f}$ above $\mathfrak{l}$. The fixed points are*

$$\mathbf{P}^1(\mathfrak{o}_\mathfrak{f}/\mathfrak{l}\mathfrak{o}_\mathfrak{f})^{\mathfrak{o}_\mathfrak{f}^\times} = \begin{cases} \emptyset & \text{if } \mathfrak{l} \nmid \mathfrak{f} \text{ and } \mathfrak{l}\mathfrak{o}_\mathfrak{f} = \mathfrak{L}, \\ \{\mathfrak{L}/\mathfrak{l}\mathfrak{o}_\mathfrak{f}, \mathfrak{L}^\dagger/\mathfrak{l}\mathfrak{o}_\mathfrak{f}\} & \text{if } \mathfrak{l} \nmid \mathfrak{f} \text{ and } \mathfrak{l}\mathfrak{o}_\mathfrak{f} = \mathfrak{L}\mathfrak{L}^\dagger, \\ \{(\mathfrak{l}\mathfrak{o}_{\mathfrak{l}^{-1}\mathfrak{f}})/\mathfrak{l}\mathfrak{o}_\mathfrak{f}\} & \text{if } \mathfrak{l} \mid \mathfrak{f}. \end{cases}$$

The remaining points are permuted simply transitively by $\mathfrak{o}_\mathfrak{f}^\times/\mathfrak{o}_{\mathfrak{l}\mathfrak{f}}^\times$.

Proof. The ring $\mathfrak{o}_{\mathfrak{l}\mathfrak{f}}^\times$ acts trivially on $\mathbf{P}^1(\mathfrak{o}_\mathfrak{f}/\mathfrak{l}\mathfrak{o}_\mathfrak{f})$, which proves the first statement. Observe that the projection $\mathfrak{o}_\mathfrak{f} \to \mathfrak{o}_\mathfrak{f}/\mathfrak{o}_{\mathfrak{l}\mathfrak{f}}$ induces a canonical isomorphism between $\mathfrak{o}_\mathfrak{f}^\times/\mathfrak{o}_{\mathfrak{l}\mathfrak{f}}^\times$ and $(\mathfrak{o}_\mathfrak{f}/\mathfrak{l}\mathfrak{o}_\mathfrak{f})^\times/\mathbf{F}^\times$. Suppose that $\mathfrak{l}$ divides $\mathfrak{f}$. Then, there exists an element $\epsilon \in \mathfrak{o}_\mathfrak{f}/\mathfrak{l}\mathfrak{o}_\mathfrak{f}$ such that $\mathfrak{o}_\mathfrak{f}/\mathfrak{l}\mathfrak{o}_\mathfrak{f} = \mathbf{F}[\epsilon]$ and $\epsilon^2 = 0$. But the only $\mathbf{F}$-line in $\mathbf{F}[\epsilon]$ fixed by the action of $\mathbf{F}[\epsilon]^\times$ is

$\epsilon\mathbf{F} = (\mathfrak{l}\mathfrak{o}_{\mathfrak{l}^{-1}\mathfrak{f}})/\mathfrak{l}\mathfrak{o}_{\mathfrak{f}}$, and this action is transitive on the ℓ other lines. Therefore the action of $\mathbf{F}[\epsilon]^\times/\mathbf{F}^\times = (\mathfrak{o}_{\mathfrak{f}}/\mathfrak{l}\mathfrak{o}_{\mathfrak{f}})^\times/\mathbf{F}^\times$ on these ℓ lines is simply transitive.

Now, suppose that $\mathfrak{l}$ does not divide $\mathfrak{f}$. If $\mathfrak{l}$ is inert in $\mathfrak{o}_{\mathfrak{f}}$, then $\mathfrak{o}_{\mathfrak{f}}/\mathfrak{l}\mathfrak{o}_{\mathfrak{f}} = \mathbf{K}$ is a quadratic field extension of $\mathbf{F}$, and $\mathbf{K}^\times/\mathbf{F}^\times$ acts simply transitively on the $\mathbf{F}$-lines $\mathbf{P}^1(\mathbf{K})$. The statement follows from the isomorphism between $\mathbf{K}^\times/\mathbf{F}^\times$ and $\mathfrak{o}_{\mathfrak{f}}^\times/\mathfrak{o}_{\mathfrak{l}\mathfrak{f}}^\times$. The cases where $\mathfrak{l}$ splits or ramifies in K are treated similarly, with $\mathfrak{o}_{\mathfrak{f}}/\mathfrak{l}\mathfrak{o}_{\mathfrak{f}} \cong \mathbf{F}^2$ in the first case, and $\mathfrak{o}_{\mathfrak{f}}/\mathfrak{l}\mathfrak{o}_{\mathfrak{f}} \cong \mathbf{F}[X]/(X^2)$ in the second case. □

Proposition 5.18 (Structure of $\mathscr{L}_{\mathfrak{l}}(\Lambda)$)**.** *Suppose Λ is an $\mathfrak{o}_{\mathfrak{f}}$-lattice, for some $\mathfrak{o}_{K^+}$-ideal $\mathfrak{f}$, and let $\mathfrak{l}$ be a prime ideal in $\mathfrak{o}_{K^+}$. The number of $\mathfrak{l}$-neighbors of Λ is $N(\mathfrak{l})+1$. The $\mathfrak{l}$-neighbors that have order $\mathfrak{o}_{\mathfrak{l}\mathfrak{f}}$ are permuted simply transitively by $(\mathfrak{o}_{\mathfrak{f}}/\mathfrak{o}_{\mathfrak{l}\mathfrak{f}})^\times$. The other $\mathfrak{l}$-neighbors have order $\mathfrak{o}_{\mathfrak{l}^{-1}\mathfrak{f}}$ if $\mathfrak{l}$ divides $\mathfrak{f}$, or $\mathfrak{o}_K$ otherwise.*

More explicitly, if $\mathfrak{l}$ divides $\mathfrak{f}$, there is one $\mathfrak{l}$-neighbor of order $\mathfrak{o}_{\mathfrak{l}^{-1}\mathfrak{f}}$, namely $\mathfrak{l}\mathfrak{o}_{\mathfrak{l}^{-1}\mathfrak{f}}\Lambda$, and $N(\mathfrak{l})$ of order $\mathfrak{o}_{\mathfrak{l}\mathfrak{f}}$. If $\mathfrak{l}$ does not divide $\mathfrak{f}$, we have:

(i) If $\mathfrak{l}$ is inert in K, all $N(\mathfrak{l})+1$ lattices of $\mathscr{L}_{\mathfrak{l}}(\Lambda)$ have order $\mathfrak{o}_{\mathfrak{l}}$;

(ii) If $\mathfrak{l}$ splits in K into prime ideals $\mathfrak{L}_1$ and $\mathfrak{L}_2$, then $\mathscr{L}_{\mathfrak{l}}(\Lambda)$ consists of two lattices of order $\mathfrak{o}_K$, namely $\mathfrak{L}_1\Lambda$ and $\mathfrak{L}_2\Lambda$, and $N(\mathfrak{l})-1$ lattices of order $\mathfrak{o}_{\mathfrak{l}}$;

(iii) If $\mathfrak{l}$ ramifies in K as $\mathfrak{L}^2$, then $\mathscr{L}_{\mathfrak{l}}(\Lambda)$ consists of one lattice of order $\mathfrak{o}_K$, namely $\mathfrak{L}\Lambda$, and $N(\mathfrak{l})$ lattices of order $\mathfrak{o}_{\mathfrak{l}}$.

Proof. This is a direct consequence of Lemma 5.17, together with the fact that Λ is a free $\mathfrak{o}_{\mathfrak{f}}$-module of rank 1. □

5.4.3. Graphs of $\mathfrak{l}$-isogenies. Fix again an absolutely simple ordinary abelian variety $\mathscr{A}$ of dimension g over k, with endomorphism algebra K. Suppose that $\mathscr{A}$ has locally maximal real multiplication at ℓ (i.e., $\mathfrak{o}_{K^+} \subset \mathfrak{o}(\mathscr{A})$). The $\mathfrak{l}$-neighbors correspond to $\mathfrak{l}$-isogenies in the world of varieties (see Proposition 5.16).

Definition 5.19. Suppose $\mathscr{A}$ has local order $\mathfrak{o}_{\mathfrak{f}}$, for some $\mathfrak{o}_{K^+}$-ideal $\mathfrak{f}$ and let $\mathfrak{l}$ be a prime ideal in $\mathfrak{o}_{K^+}$. An $\mathfrak{l}$-isogeny $\varphi : \mathscr{A} \to \mathscr{B}$ is *$\mathfrak{l}$-ascending* if $\mathfrak{o}(\mathscr{B}) = \mathfrak{o}_{\mathfrak{l}^{-1}\mathfrak{f}}$, it is *$\mathfrak{l}$-descending* if $\mathfrak{o}(\mathscr{B}) = \mathfrak{o}_{\mathfrak{l}\mathfrak{f}}$, and it is *$\mathfrak{l}$-horizontal* if $\mathfrak{o}(\mathscr{B}) = \mathfrak{o}_{\mathfrak{f}}$.

Proposition 5.20. *Suppose $\mathscr{A}$ has local order $\mathfrak{o}_{\mathfrak{f}}$ for some $\mathfrak{o}_{K^+}$-ideal $\mathfrak{f}$ and let $\mathfrak{l}$ be a prime ideal in $\mathfrak{o}_{K^+}$. There are $N(\mathfrak{l})+1$ kernels of $\mathfrak{l}$-isogenies from $\mathscr{A}$. The kernels of the $\mathfrak{l}$-descending $\mathfrak{l}$-isogenies are permuted simply transitively by the action of $(\mathfrak{o}_{\mathfrak{f}}/\mathfrak{o}_{\mathfrak{l}\mathfrak{f}})^\times$. The other $\mathfrak{l}$-isogenies are $\mathfrak{l}$-ascending if $\mathfrak{l}$ divides $\mathfrak{f}$, and $\mathfrak{l}$-horizontal otherwise.*

More explicitly, if $\mathfrak{l}$ divides $\mathfrak{f}$, there is a unique $\mathfrak{l}$-ascending $\mathfrak{l}$-kernel from $\mathscr{A}$, and $N(\mathfrak{l})$ that are $\mathfrak{l}$-descending. If $\mathfrak{l}$ does not divide $\mathfrak{f}$, we have:

(i) If $\mathfrak{l}$ is inert in K, all $N(\mathfrak{l})+1$ of the $\mathfrak{l}$-kernels are $\mathfrak{l}$-descending;

(ii) If $\mathfrak{l}$ splits in K into two prime ideals $\mathfrak{L}_1$ and $\mathfrak{L}_2$, there are two $\mathfrak{l}$-horizontal $\mathfrak{l}$-kernels, namely $\mathscr{A}[\mathfrak{L}_1]$ and $\mathscr{A}[\mathfrak{L}_2]$, and $N(\mathfrak{l})-1$ that are $\mathfrak{l}$-descending;

(iii) If $\mathfrak{l}$ ramifies in K as $\mathfrak{L}^2$, there is one $\mathfrak{l}$-horizontal $\mathfrak{l}$-kernel, namely $\mathscr{A}[\mathfrak{L}]$, and $N(\mathfrak{l})$ that are $\mathfrak{l}$-descending.

Proof. This proposition follows from Proposition 5.18 together with Proposition 5.16. □

Definition 5.21 ($\mathfrak{l}$-predecessor)**.** When it exists, let κ be the unique $\mathfrak{l}$-ascending kernel of Proposition 5.20. We call $\mathrm{pr}_{\mathfrak{l}}(\mathscr{A}) = \mathscr{A}/\kappa$ the *$\mathfrak{l}$-predecessor* of $\mathscr{A}$, and denote by $\mathrm{up}^{\mathfrak{l}}_{\mathscr{A}} : \mathscr{A} \to \mathrm{pr}_{\mathfrak{l}}(\mathscr{A})$ the canonical projection.

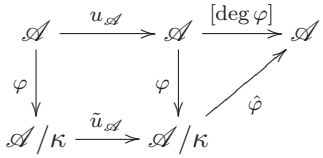
Let $\mathfrak{l}$ be a prime of K^+ above ℓ. Consider the $\mathfrak{l}$-isogeny graph $\mathscr{W}_{\mathfrak{l}}$. Note that it is a directed multigraph; we say that such a graph is *undirected* if for any vertices u and

v, the multiplicity of the edge from u to v is the same as the multiplicity from v to u. The remainder of this section is a proof of Theorem 5.13, which provides a complete description of the structure of the levelled $\mathfrak{l}$-isogeny graph $(\mathscr{W}_\mathfrak{l}, v_\mathfrak{l})$, closely related to volcanoes.

Lemma 5.22. *Suppose that $\mathcal{O}(\mathscr{B}) \subsetneq \mathcal{O}(\mathscr{A})$. If there exists an $\mathfrak{l}$-isogeny $\varphi : \mathscr{A} \to \mathscr{B}$, then there are at least $[\mathcal{O}(\mathscr{A})^\times : \mathcal{O}(\mathscr{B})^\times]$ pairwise distinct kernels of $\mathfrak{l}$-isogenies from $\mathscr{A}$ to $\mathscr{B}$.*

Proof. The elements $\alpha \in \mathcal{O}(\mathscr{A})$ act on the subgroups of $\mathscr{A}$ via the isomorphism $\mathcal{O}(\mathscr{A}) \cong \mathrm{End}(\mathscr{A})$, and we denote this action $\kappa \mapsto \kappa^\alpha$. Let $\kappa = \ker \varphi$. If $u \in \mathcal{O}(\mathscr{A})^\times$ is a unit, then κ^u is also the kernel of an $\mathfrak{l}$-isogeny. Furthermore, u canonically induces an isomorphism $\mathscr{A}/\kappa \to \mathscr{A}/\kappa^u$, so κ^u is the kernel of an $\mathfrak{l}$-isogeny with target $\mathscr{B}$.

It only remains to prove that the orbit of κ for the action of $\mathcal{O}(\mathscr{A})^\times$ contains at least $[\mathcal{O}(\mathscr{A})^\times : \mathcal{O}(\mathscr{B})^\times]$ distinct kernels. It suffices to show that if $\kappa^u = \kappa$, then $u \in \mathcal{O}(\mathscr{B})^\times$. Let $u \in \mathcal{O}(\mathscr{A})^\times$ such that $\kappa^u = \kappa$. Recall that for any variety $\mathscr{C}$ in our isogeny class, we have fixed an isomorphism $\imath_\mathscr{C} : \mathrm{End}(\mathscr{C}) \to \mathcal{O}(\mathscr{C})$, and that these isomorphisms are all compatible in the sense that for any isogeny $\psi : \mathscr{C} \to \mathscr{D}$, and $\gamma \in \mathrm{End}(\mathscr{C})$, we have $\imath_\mathscr{C}(\gamma) = \imath_\mathscr{D}(\psi \circ \gamma \circ \hat{\psi})/\deg \psi$ (see Section 3.1.2). Let $u_\mathscr{A} \in \mathrm{End}(\mathscr{A})$ be the endomorphism of $\mathscr{A}$ corresponding to u. It induces an isomorphism $\tilde{u}_\mathscr{A} : \mathscr{A}/\kappa \to \mathscr{A}/\kappa^u$, which is actually an automorphism of $\mathscr{A}/\kappa$ since $\kappa^u = \kappa$. Let $\varphi : \mathscr{A} \to \mathscr{A}/\kappa$ be the natural projection. We obtain the following commutative diagram:



Finally, we obtain

$$u = \imath_\mathscr{A}([\deg \varphi] \circ u_\mathscr{A})/\deg \varphi = \imath_\mathscr{A}(\hat{\varphi} \circ \tilde{u}_\mathscr{A} \circ \varphi)/\deg \varphi = \imath_\mathscr{B}(\tilde{u}_\mathscr{A}) \in \mathcal{O}(\mathscr{B}).$$

□

Lemma 5.23. *Let K be a CM-field and K^+ its maximal real subfield. Let $\mathcal{O}$ be an order in K of conductor $\mathfrak{f}$ such that $\mathfrak{o}_{K^+} \subset \mathcal{O} \otimes_\mathbf{Z} \mathbf{Z}_\ell$. Let $\mathcal{O}'$ be the order such that $\mathcal{O}' \otimes_\mathbf{Z} \mathbf{Z}_{\ell'} = \mathcal{O} \otimes_\mathbf{Z} \mathbf{Z}_{\ell'}$ for all prime $\ell' \neq \ell$, and $\mathcal{O}' \otimes_\mathbf{Z} \mathbf{Z}_\ell = \mathfrak{o}_{K^+} + \mathfrak{l}\mathfrak{f}\mathfrak{o}_K$. Then,*

$$|\mathrm{Cl}(\mathcal{O}')| = \frac{[(\mathcal{O} \otimes_\mathbf{Z} \mathbf{Z}_\ell)^\times : (\mathcal{O}' \otimes_\mathbf{Z} \mathbf{Z}_\ell)^\times]}{[\mathcal{O}^\times : \mathcal{O}'^\times]} |\mathrm{Cl}(\mathcal{O})|.$$

Proof. First, for any order $\mathcal{O}$ in K of conductor $\mathfrak{f}$ we have the classical formula (see [NS99, Theorem 12.12 and Proposition 12.11])

$$\begin{aligned} |\mathrm{Cl}(\mathcal{O})| &= \frac{h_K}{[\mathcal{O}_K^\times : \mathcal{O}^\times]} \frac{|(\mathcal{O}_K/\mathfrak{f})^\times|}{|(\mathcal{O}/\mathfrak{f})^\times|} \\ &= \frac{h_K}{[\mathcal{O}_K^\times : \mathcal{O}^\times]} \prod_{\ell' \text{ prime}} [(\mathcal{O}_K \otimes_\mathbf{Z} \mathbf{Z}_{\ell'})^\times : (\mathcal{O} \otimes_\mathbf{Z} \mathbf{Z}_{\ell'})^\times]. \end{aligned}$$

Now, consider $\mathcal{O}$ and $\mathcal{O}'$ as in the statement of the lemma. We obtain

$$\frac{|\mathrm{Cl}(\mathcal{O}')|}{|\mathrm{Cl}(\mathcal{O})|} = \frac{[\mathcal{O}_K^\times : \mathcal{O}^\times]}{[\mathcal{O}_K^\times : \mathcal{O}'^\times]}[(\mathcal{O}\otimes_{\mathbf{Z}}\mathbf{Z}_\ell)^\times : (\mathcal{O}'\otimes_{\mathbf{Z}}\mathbf{Z}_\ell)^\times] = \frac{[(\mathcal{O}\otimes_{\mathbf{Z}}\mathbf{Z}_\ell)^\times : (\mathcal{O}'\otimes_{\mathbf{Z}}\mathbf{Z}_\ell)^\times]}{[\mathcal{O}^\times : \mathcal{O}'^\times]}.$$

□

Remark 5.24. If one supposes that $\mathcal{O}_K^\times = \mathcal{O}_{K^+}^\times$, then $[\mathcal{O}^\times : \mathcal{O}'^\times]$ is always 1 in the above lemma. Indeed, one has $\mathcal{O}^\times \subset \mathcal{O}_{K^+}^\times \subset \mathfrak{o}_{K^+}^\times \subset (\mathcal{O}'\otimes_{\mathbf{Z}}\mathbf{Z}_\ell)^\times$, and therefore, since $\mathcal{O}$ and $\mathcal{O}'$ coincide at every other prime, we obtain $\mathcal{O}^\times \subset \mathcal{O}'^\times$, hence $\mathcal{O}^\times = \mathcal{O}'^\times$.

Remark 5.25. For $g = 2$, the field K is a primitive quartic CM-field. Then, the condition $\mathcal{O}_K^\times = \mathcal{O}_{K^+}^\times$ is simply equivalent to $K \neq \mathbf{Q}(\zeta_5)$ by [Str10, Lemma II.3.3]. So in dimension 2, if $K \neq \mathbf{Q}(\zeta_5)$, one always has $[\mathcal{O}^\times : \mathcal{O}'^\times] = 1$ in the above lemma. For $K = \mathbf{Q}(\zeta_5)$, we have $[\mathcal{O}_K^\times : \mathcal{O}_{K^+}^\times] = 5$, and since $\mathcal{O}_K$ is the only order in K containing complex units, we get

$$[\mathcal{O}^\times : \mathcal{O}'^\times] = \begin{cases} 5 \text{ if } \mathcal{O} = \mathcal{O}_K, \\ 1 \text{ otherwise.} \end{cases}$$

This pathological case is illustrated in Example 5.27.

Proof of Theorem 5.13. Let $\mathscr{V}$ be any of connected component of $\mathscr{W}_\mathfrak{l}$. First, it follows from Proposition 5.10 that locally at any prime other than ℓ, the endomorphism rings occurring in $\mathscr{V}$ all coincide. Also, locally at ℓ, Proposition 5.20 implies that an $\mathfrak{l}$-isogeny can only change the valuation at $\mathfrak{l}$ of the conductor. Therefore within $\mathscr{V}$, the endomorphism ring of a variety $\mathscr{A}$ is uniquely determined by its level $v_\mathfrak{l}(\mathscr{A})$. Let $\mathcal{O}_i$ be the endomorphism of any (and therefore every) variety $\mathscr{A}$ in $\mathscr{V}$ at level $v_\mathfrak{l}(\mathscr{A}) = i$. Write $\mathscr{V}_i$ for the corresponding subset of $\mathscr{V}$. Proposition 5.20 implies that, except at the surface, all the edges connect consecutive levels of the graph, and each vertex at level i has exactly one edge to the level $i-1$.

The structure of the connected components of the level $\mathscr{V}_0$ is already a consequence of the well-known free CM-action of $\mathrm{Cl}(\mathcal{O}_0)$ on ordinary abelian varieties with endomorphism ring $\mathcal{O}_0$. Note that if $\varphi : \mathscr{A} \to \mathscr{B}$ is a descending $\mathfrak{l}$-isogeny within $\mathscr{V}$, then the unique ascending $\mathfrak{l}$-isogeny from $\mathscr{B}$ is $\mathrm{up}_\mathscr{B}^\mathfrak{l} : \mathscr{B} \to \mathrm{pr}_\mathfrak{l}(\mathscr{B})$, and we have $\mathrm{pr}_\mathfrak{l}(\mathscr{B}) \cong \mathscr{A}/\mathscr{A}[\mathfrak{l}]$; also, we have $\mathrm{pr}_\mathfrak{l}(\mathscr{B}/\mathscr{B}[\mathfrak{l}]) \cong \mathrm{pr}_\mathfrak{l}(\mathscr{B})/\mathrm{pr}_\mathfrak{l}(\mathscr{B})[\mathfrak{l}]$. These facts easily follow from the lattice point of view (see Proposition 5.18, and observe that if $\Gamma \in \mathscr{L}_\mathfrak{l}(\Lambda)$, then $\mathfrak{l}\Gamma \in \mathscr{L}_\mathfrak{l}(\mathfrak{l}\Lambda)$). We can deduce in particular that $\mathscr{V}_0$ is connected: a path from $\mathscr{A} \in \mathscr{V}_0$ to another vertex of $\mathscr{V}_0$ containing only vertical isogenies can only end at a vertex $\mathscr{A}/\mathscr{A}[\mathfrak{l}^i]$, which can also be reached within $\mathscr{V}_0$.

We now need to look at a bigger graph. For each $i \geq 0$, let $\mathscr{U}_i$ be the orbit of the level $\mathscr{V}_i$ for the CM-action of $\mathrm{Cl}(\mathcal{O}_i)$. The action is transitive on $\mathscr{U}_0$ since the connected graph $\mathscr{V}_0$ is in a single orbit of the action of $\mathrm{Cl}(\mathcal{O}_0)$. Let us show by induction that each $\mathscr{U}_{i+1}$ consists of a single orbit, and that each vertex of $\mathscr{U}_{i+1}$ is reachable by an edge from $\mathscr{U}_i$. First, $\mathscr{U}_{i+1}$ is non-empty because, by induction, $\mathscr{U}_i$ is non-empty, and each vertex in $\mathscr{U}_i$ has neighbors in $\mathscr{U}_{i+1}$. Choose any isogeny $\varphi : \mathscr{A}' \to \mathscr{A}$ from $\mathscr{U}_i$ to $\mathscr{U}_{i+1}$. For any vertex $\mathscr{B}$ in the orbit of $\mathscr{A}$, there is an isogeny $\psi : \mathscr{A} \to \mathscr{B}$ of degree coprime to ℓ. The isogeny $\psi \circ \varphi$ factors through a variety $\mathscr{B}'$ via an isogeny $\psi' : \mathscr{A}' \to \mathscr{B}'$ of the same degree as ψ, and an isogeny $\nu : \mathscr{B}' \to \mathscr{B}$ of kernel $\psi'(\ker\varphi)$. In particular, ν is an $\mathfrak{l}$-isogeny, and $\mathscr{B}'$ is in the orbit of $\mathscr{A}'$ for the CM-action, so it is in $\mathscr{U}_i$. This proves that any vertex in the orbit of $\mathscr{A}$ is reachable by an isogeny down from $\mathscr{U}_i$.

Let $\mathscr{E}_i$ be the set of all edges (counted with multiplicities) from $\mathscr{U}_i$ to $\mathscr{U}_{i+1}$. From Proposition 5.20, we have

$$|\mathscr{E}_i| = \left[(\mathcal{O}_i \otimes_{\mathbf{Z}} \mathbf{Z}_\ell)^\times : (\mathcal{O}_{i+1} \otimes_{\mathbf{Z}} \mathbf{Z}_\ell)^\times\right] \cdot |\mathscr{U}_i|. \tag{5.2}$$

For any $\mathscr{B} \in \mathscr{U}_{i+1}$, let $d(\mathscr{B})$ be the number of edges in $\mathscr{E}_i$ targeting $\mathscr{B}$ (with multiplicities). We have seen that any $\mathscr{B}$ is reachable from $\mathscr{U}_i$, therefore $d(\mathscr{B}) \geq 1$, and we deduce from Lemma 5.22 that $d(\mathscr{B}) \geq \left[\mathcal{O}_i^\times : \mathcal{O}_{i+1}^\times\right]$. We deduce

$$|\mathscr{E}_i| = \sum_{\mathscr{B} \in \mathscr{U}_{i+1}} d(\mathscr{B}) \geq \left[\mathcal{O}_i^\times : \mathcal{O}_{i+1}^\times\right] \cdot |\mathscr{U}_{i+1}|.$$

Together with Equation (5.2), we obtain the inequality

$$|\mathscr{U}_{i+1}| \leq \frac{\left[(\mathcal{O}_i \otimes_{\mathbf{Z}} \mathbf{Z}_\ell)^\times : (\mathcal{O}_{i+1} \otimes_{\mathbf{Z}} \mathbf{Z}_\ell)^\times\right]}{\left[\mathcal{O}_i^\times : \mathcal{O}_{i+1}^\times\right]} \cdot |\mathscr{U}_i|. \tag{5.3}$$

Since the CM-action of the class group of $\mathcal{O}_i$ is free, we obtain from Lemma 5.23 that the right-hand side of Equation (5.3) is exactly the size of the orbit of any vertex in $\mathscr{U}_{i+1}$. So $\mathscr{U}_{i+1}$ contains at most one orbit, and thereby contains exactly one, turning Equation (5.3) into an equality. In particular, all the edges in $\mathscr{E}_i$ must have multiplicity $[\mathcal{O}_i^\times : \mathcal{O}_{i+1}^\times]$. This concludes the recursion.

Note that with all these properties, the graph is a volcano if and only if it is undirected and all the vertical multiplicities are 1. The latter is true if and only if $[\mathcal{O}_i^\times : \mathcal{O}_{i+1}^\times] = 1$ for any i, i.e., if $\mathcal{O}_0^\times \subset K^+$. For the following, suppose this is the case; it remains to decide when the graph is undirected. If $\mathfrak{l}$ is principal in $\mathcal{O}_0 \cap K^+$, the surface $\mathscr{V}_0$ is undirected because the primes above $\mathfrak{l}$ in $\mathcal{O}_0$ are inverses of each other. If $\varphi : \mathscr{A} \to \mathscr{B}$ is a descending $\mathfrak{l}$-isogeny within $\mathscr{V}$, then the unique ascending $\mathfrak{l}$-isogeny from $\mathscr{B}$ points to $\mathscr{A}/\mathscr{A}[\mathfrak{l}]$, which is isomorphic to $\mathscr{A}$ if and only if $\mathfrak{l}$ is principal in $\mathcal{O}(\mathscr{A})$. So for each descending edge $\mathscr{A} \to \mathscr{B}$ there is an ascending edge $\mathscr{B} \to \mathscr{A}$, and since we have proven above that each vertical edge has multiplicity 1, we conclude that the graph is undirected (so is a volcano) if and only if $\mathfrak{l}$ is principal in $\mathcal{O}_0 \cap K^+$ (if $\mathfrak{l}$ is not principal in $\mathcal{O}_0 \cap K^+$, there is a level i where $\mathfrak{l}$ is not principal in $\mathcal{O}_i$).

For Point (vi), choose a descending edge $\mathscr{A} \to \mathscr{B}$. We get that $\mathscr{C} \cong \mathscr{A}/\mathscr{A}[\mathfrak{l}]$. It is then easy to see that the isogeny $\mathscr{A} \to \mathscr{B}$ induces an isogeny $\mathscr{C} \to \mathscr{B}/\mathscr{B}[\mathfrak{l}]$. □

Theorem 5.13 gives a complete description of the graph: it allows one to construct an abstract model of any connected component corresponding to an order $\mathcal{O}_0$ from the knowledge of the norm of $\mathfrak{l}$, of the (labelled) Cayley graph of the subgroup of $\mathrm{Cl}(\mathcal{O}_0)$ with generators the prime ideals in $\mathcal{O}_0$ above $\mathfrak{l}$, of the order of $\mathfrak{l}$ in each class group $\mathrm{Cl}(\mathcal{O}_i)$, and of the indices $[\mathcal{O}_i^\times : \mathcal{O}_{i+1}^\times]$.

Example 5.26. For instance, suppose that $\ell = 2$ ramifies in K^+ as $\mathfrak{l}^2$, and $\mathfrak{l}$ is principal in $\mathcal{O}_K$, but is of order 2 in both $\mathrm{Cl}(\mathcal{O}_{K^+} + \mathfrak{l}\mathcal{O}_K)$ and $\mathrm{Cl}(\mathcal{O}_{K^+} + \mathfrak{l}^2\mathcal{O}_K)$, and that $\mathcal{O}_K^\times \subset K^+$. Then the first four levels of any connected component of the $\mathfrak{l}$-isogeny graph for which the largest order is $\mathcal{O}_K$ are isomorphic to the graph of Figure 5.2. It is not a volcano since $\mathfrak{l}$ is not principal in every order $\mathcal{O}_{K^+} + \mathfrak{l}^i\mathcal{O}_K$.

Example 5.27. When K is a primitive quartic CM-field, we have seen in Remark 5.25 that the multiplicities $[\mathcal{O}_i^\times : \mathcal{O}_{i+1}^\times]$ are always one, except maybe if $K = \mathbf{Q}(\zeta_5)$. Actually, even for $K = \mathbf{Q}(\zeta_5)$, only the maximal order $\mathcal{O}_K$ has units that are not in K^+. We give in Figure 5.3 examples of $\mathfrak{l}$-isogeny graphs when the order at the surface is $\mathcal{O}_K = \mathbf{Z}[\zeta_5]$ (which is a principal ideal domain). The primes 2 and 3 are inert in K, so we consider

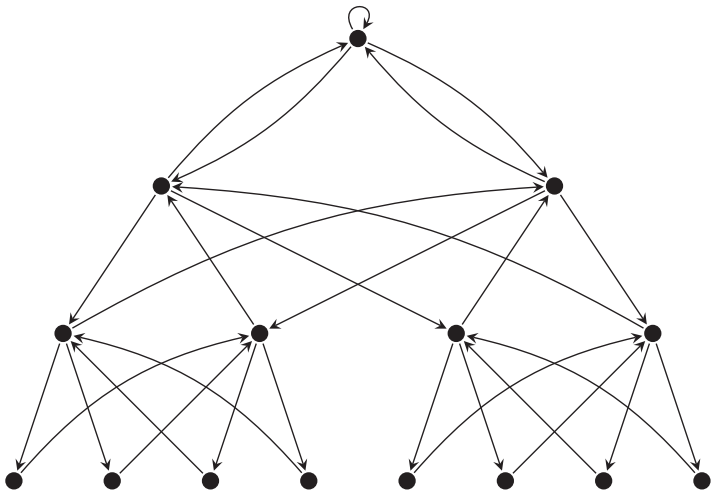


FIGURE 5.2. An example of an $\mathfrak{l}$-isogeny graph which is not a volcano, because the ideal $\mathfrak{l}$ is not principal. The vertical direction represents levels.

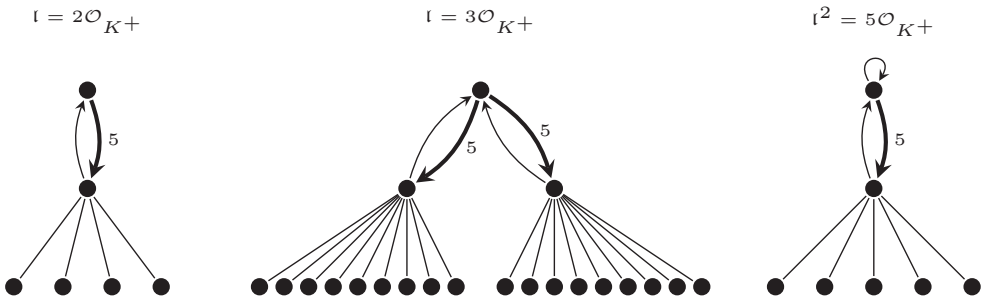


FIGURE 5.3. Some $\mathfrak{l}$-isogeny graphs for $K = \mathbf{Q}(\zeta_5)$, when the endomorphism ring at the surface is the maximal order $\mathbf{Z}[\zeta_5]$. All edges are simple except the thick ones, of multiplicity 5. The undirected edges are actually directed in both directions. The vertical direction represents levels.

$\mathfrak{l} = 2\mathcal{O}_{K^+}$ and $\mathfrak{l} = 3\mathcal{O}_{K^+}$, and the prime number 5 is ramified in K^+ so $\mathfrak{l}^2 = 5\mathcal{O}_{K^+}$ (and $\mathfrak{l}$ is also ramified in K, explaining the self-loop at the surface of the last graph).

5.5. Graphs of $\mathfrak{l}$-isogenies with polarisation

When $\mathfrak{l}$ is trivial in the narrow class group of K^+, then $\mathfrak{l}$-isogenies preserve principal polarisability. The graphs of $\mathfrak{l}$-isogenies studied in Section 5.4.3 do not account for polarisations. The present section fills this gap, by considering graphs of β-isogenies which take polarisations into account, where $\beta \in K^+$ is a totally positive generator of $\mathfrak{l}$. A β-isogeny is simply an $\mathfrak{l}$-isogeny, but the choice of the generator β carries more information than the ideal $\mathfrak{l}$ (see Proposition 5.28). The main result of this section is Theorem 5.31 which essentially states that the connected components of polarised isogeny graphs are either isomorphic to the corresponding components of the non-polarised isogeny graphs,

or non-trivial double-covers thereof. The precise statement is more complicated due to problems arising when the various abelian varieties occurring in a connected component have different automorphism groups.

5.5.1. Graphs with polarisation. Before defining the graph, we record the following proposition, which implies that one vertex of a fixed connected component of $(\mathscr{W}_\beta, v_\beta)$ is principally polarisable if and only if all of them are. Given an isogeny $\varphi : \mathscr{A} \to \mathscr{B}$ and a polarisation $\xi_{\mathscr{B}}$ on $\mathscr{B}$, we denote by $\varphi^*\xi_{\mathscr{B}}$ the pullback of $\xi_{\mathscr{B}}$ by φ (that is the polarisation on $\mathscr{A}$ with polarisation isogeny $\varphi^\vee \circ \varphi_{\xi_{\mathscr{B}}} \circ \varphi : \mathscr{A} \to \mathscr{A}^\vee$, where $\varphi_{\xi_{\mathscr{B}}}$ is the polarisation isogeny of $(\mathscr{B}, \xi_{\mathscr{B}})$ and $\varphi^\vee : \mathscr{B}^\vee \to \mathscr{A}^\vee$ is the dual of φ). Also, given a polarisation $\xi_{\mathscr{A}}$ (with polarisation isogeny $\varphi_{\xi_{\mathscr{A}}}$) and an endomorphism α of $\mathscr{A}$, we denote by $\xi_{\mathscr{A}}^\alpha$ the polarisation corresponding to the polarisation isogeny $\varphi_{\xi_{\mathscr{A}}} \circ \alpha$.

Proposition 5.28. *If $\varphi : \mathscr{A} \to \mathscr{B}$ is a β-isogeny, then given a principal polarisation $\xi_{\mathscr{A}}$ on $\mathscr{A}$, there is a unique principal polarisation $\xi_{\mathscr{B}}$ on $\mathscr{B}$ satisfying*

$$\varphi^*\xi_{\mathscr{B}} = \xi_{\mathscr{A}}^\beta.$$

Proof. Denoting by $\varphi_{\xi_{\mathscr{A}}}$ the polarisation isogeny, $\ker(\varphi) \subset \ker(\varphi_{\xi_{\mathscr{A}}^\beta})$ is a maximal isotropic subgroup for the commutator pairing and hence by Grothendieck descent (see [Rob10, Lemma 2.4.7]; the proof there is in characteristic 0, but it extends to ordinary abelian varieties in characteristic p via canonical lifts), it follows that $\xi_{\mathscr{A}}^\beta$ is a pullback of a principal polarisation $\xi_{\mathscr{B}}$ on $\mathscr{B}$. For uniqueness, note that φ^* defines a homomorphism between the Néron-Severi groups $\mathbf{NS}(\mathscr{B})$ and $\mathbf{NS}(\mathscr{A})$ (free abelian groups of the same rank), which becomes an isomorphism after tensoring with $\mathbf{Q}$, hence it is injective. □

We define the principally polarised, levelled, β-isogeny graph $(\mathscr{W}_\beta^{\mathrm{pp}}, v_\beta)$ as follows. Recall that two polarisations $\xi_{\mathscr{A}}$ and $\xi'_{\mathscr{A}}$ on $\mathscr{A}$ are isomorphic if and only if there is a unit $u \in \mathcal{O}(\mathscr{A})^\times$ such that $\xi'_{\mathscr{A}} = u^*\xi_{\mathscr{A}}$. A vertex of the graph is an isomorphism class of pairs $(\mathscr{A}, \xi_{\mathscr{A}})$, where $\mathscr{A}$ is a principally polarisable abelian variety occurring in $(\mathscr{W}_\beta, v_\beta)$, and $\xi_{\mathscr{A}}$ is a principal polarisation on $\mathscr{A}$. There is an edge of multiplicity m from the isomorphism class of $(\mathscr{A}, \xi_{\mathscr{A}})$ to the isomorphism class of $(\mathscr{B}, \xi_{\mathscr{B}})$ if there are m distinct subgroups of $\mathscr{A}$ that are kernels of β-isogenies $\varphi : \mathscr{A} \to \mathscr{B}$ such that $\varphi^*\xi'_{\mathscr{B}}$ is isomorphic to $\xi_{\mathscr{A}}^\beta$, for some polarisation $\xi'_{\mathscr{B}}$ isomorphic to $\xi_{\mathscr{B}}$. The graph $\mathscr{W}_\beta^{\mathrm{pp}}$ admits a forgetful map to $\mathscr{W}_\beta$, and in particular inherits the structure of a levelled graph $(\mathscr{W}_\beta^{\mathrm{pp}}, v_\beta)$.

Remark 5.29. It can be the case that there is no β-isogeny $\varphi : \mathscr{A} \to \mathscr{B}$ such that $\varphi^*\xi_{\mathscr{B}} \cong \xi_{\mathscr{A}}^\beta$, but that there is nonetheless an edge (because there is a map with this property for some other polarisation $\xi'_{\mathscr{B}}$, isomorphic to $\xi_{\mathscr{B}}$). This can happen because pullbacks of isomorphic polarisations are not necessarily isomorphic, when $\mathscr{A}$ and $\mathscr{B}$ have different automorphism groups.

We note that this graph is undirected:

Proposition 5.30. *If $\varphi : \mathscr{A} \to \mathscr{B}$ is a β-isogeny, then there is a unique β-isogeny $\tilde{\varphi} : \mathscr{B} \to \mathscr{A}$ satisfying $\tilde{\varphi}\varphi = \beta$, called the β-dual of φ.*

Proof. Let κ be the kernel of φ. The group $\mathscr{A}[\beta]$ is an $\mathcal{O}^+(\mathscr{A})/(\beta)$-vector space of dimension 2, of which the kernel κ is a vector subspace of dimension 1. Therefore there is another vector subspace κ' such that $\mathscr{A}[\beta] = \kappa \oplus \kappa'$, and $\varphi(\kappa')$ is the kernel of a β-isogeny $\psi : \mathscr{B} \to \mathscr{C}$. Then, the kernel of the composition $\psi \circ \varphi$ is $\mathscr{A}[\beta]$ so there is an isomorphism $u : \mathscr{C} \to \mathscr{A}$ such that $u \circ \psi \circ \varphi = \beta$. The isogeny $u \circ \psi$ is the β-dual of φ (which is trivially unique). □

5.5.2. Structure of the β-isogeny graph. Recall from Section 3.2 that if $\mathscr{A}$ is a simple ordinary principally polarisable abelian variety with endomorphism ring $\mathcal{O}$, then the set of isomorphism classes of principal polarisations on $\mathscr{A}$ is a torsor for the group $U(\mathcal{O}) = \mathrm{TP}(\mathcal{O})/N_{K/K^+}(\mathcal{O}^\times)$. Also, the Shimura class group $\mathfrak{C}(\mathcal{O})$ acts freely on the set of isomorphism classes of principally polarised abelian varieties whose endomorphism ring is $\mathcal{O}$. If β is coprime to the conductor of $\mathcal{O}$, then an element of $\mathfrak{C}(\mathcal{O})$ acts by a β-isogeny if and only if it is of the form $(\mathfrak{L}, \beta)$, for some prime ideal $\mathfrak{L}$ of $\mathcal{O}$ dividing (β).

Theorem 5.31. *Let $\mathscr{V}^{\mathrm{pp}}$ be any connected component of the levelled β-isogeny graph $(\mathscr{W}_\beta^{\mathrm{pp}}, v_\beta)$. For each $i \geq 0$, let $\mathscr{V}_i^{\mathrm{pp}}$ be the subgraph of $\mathscr{V}^{\mathrm{pp}}$ at level i. We have:*

(i) For each $i \geq 0$, the varieties in $\mathscr{V}_i^{\mathrm{pp}}$ share a common endomorphism ring $\mathcal{O}_i$. The order $\mathcal{O}_0$ can be any order with locally maximal real multiplication at ℓ, whose conductor is not divisible by β;

(ii) The level $\mathscr{V}_0^{\mathrm{pp}}$ is isomorphic to the Cayley graph of the subgroup of $\mathfrak{C}(\mathcal{O}_0)$ with generators $(\mathfrak{L}_i, \beta)$ where $\mathfrak{L}_i$ are the prime ideals in $\mathcal{O}_0$ above β;

(iii) For any $x \in \mathscr{V}_0^{\mathrm{pp}}$, there are

$$\frac{N(\mathfrak{l}) - \left(\frac{K}{\beta}\right)}{[\mathcal{O}_0^\times : \mathcal{O}_1^\times]} \cdot \frac{|U(\mathcal{O}_1)|}{|U(\mathcal{O}_0)|}$$

edges of multiplicity $[\mathcal{O}_0^\times : \mathcal{O}_1^\times]$ from x to distinct vertices of $\mathscr{V}_1^{\mathrm{pp}}$ (where $\left(\frac{K}{\beta}\right)$ is -1, 0 or 1 if β is inert, ramified, or split in K); these edges, plus the ones in $\mathscr{V}_0^{\mathrm{pp}}$, are all the edges from x;

(iv) For each $i > 0$, and any $x \in \mathscr{V}_i^{\mathrm{pp}}$, there is one simple edge from x to a vertex in $\mathscr{V}_{i-1}^{pp}$, and

$$\frac{N(\mathfrak{l})}{[\mathcal{O}_i^\times : \mathcal{O}_{i+1}^\times]} \cdot \frac{|U(\mathcal{O}_{i+1})|}{|U(\mathcal{O}_i)|}$$

edges of multiplicity $[\mathcal{O}_i^\times : \mathcal{O}_{i+1}^\times]$ to distinct vertices of $\mathscr{V}_{i+1}^{\mathrm{pp}}$; these are all the edges from x;

(v) For each edge $x \to y$, there is an edge $y \to x$.

In particular, the graph $\mathscr{V}^{\mathrm{pp}}$ is an $N(\beta)$-volcano if and only if $\mathcal{O}_0^\times \subset K^+$. Also, if $\mathscr{V}^{\mathrm{pp}}$ contains a variety defined over the finite field k, the subgraph containing only the varieties defined over k consists of the subgraph of the first v levels, where v is the valuation at β of the conductor of $\mathcal{O}_{K^+}[\pi] = \mathcal{O}_{K^+}[\pi, \pi^\dagger]$.

The proof relies on some preliminary results.

Lemma 5.32. *Let $\varphi : \mathscr{A} \to \mathscr{B}$ be a β-isogeny, and let $\xi_{\mathscr{A}}$ be a principal polarisation on $\mathscr{A}$. We have:*

(i) If φ is β-ascending, there is, up to isomorphism, a unique polarisation $\xi_{\mathscr{B}}$ on $\mathscr{B}$ such that $\varphi^*\xi_{\mathscr{B}}$ is isomorphic to $\xi_{\mathscr{A}}^\beta$;

(ii) If φ is β-descending, there are, up to isomorphism, exactly

$$\frac{|U(\mathcal{O}(\mathscr{B}))|}{|U(\mathcal{O}(\mathscr{A}))|}$$

distinct polarisations $\xi_{\mathscr{B}}$ on $\mathscr{B}$ such that $\varphi^*\xi_{\mathscr{B}}$ is isomorphic to $\xi_{\mathscr{A}}^\beta$.

Proof. Let us first prove (i). From Proposition 5.28, there exists a polarisation $\xi_{\mathscr{B}}$ on $\mathscr{B}$ such that $\varphi^*\xi_{\mathscr{B}} = \xi_{\mathscr{A}}^\beta$. Suppose $\xi'_{\mathscr{B}}$ is a polarisation such that $\varphi^*\xi'_{\mathscr{B}} \cong \xi_{\mathscr{A}}^\beta$. Then there

is a unit $u \in \mathcal{O}(\mathscr{A})^\times$ such that $\varphi^*\xi'_{\mathscr{B}} = u^*\xi^\beta_{\mathscr{A}}$. But φ is ascending, so $u \in \mathcal{O}(\mathscr{B})^\times$ and therefore

$$\varphi^*\xi'_{\mathscr{B}} = u^*\xi^\beta_{\mathscr{A}} = u^*(\varphi^*\xi_{\mathscr{B}}) = \varphi^*(u^*\xi_{\mathscr{B}}).$$

From the uniqueness in Proposition 5.28, we obtain $\xi'_{\mathscr{B}} = u^*\xi_{\mathscr{B}}$, so $\xi_{\mathscr{B}}$ and $\xi'_{\mathscr{B}}$ are two isomorphic polarisations.

For (ii), again apply Proposition 5.28, and observe that the kernel of the surjection $U(\mathcal{O}(\mathscr{B})) \to U(\mathcal{O}(\mathscr{A}))$ of Lemma 3.12 acts simply transitively on the set of isomorphism classes of polarisations $\xi_{\mathscr{B}}$ on $\mathscr{B}$ satisfying $\varphi^*\xi_{\mathscr{B}} \cong \xi^\beta_{\mathscr{A}}$. □

Proof of Theorem 5.31. First observe that (i) is immediate from Theorem 5.13(i), since the leveling on $\mathscr{V}^{\mathrm{pp}}$ is induced from that of $\mathscr{V}$. Also, (v) is a direct consequence of the existence of β-duals, established in Proposition 5.30. Now, let us prove that for any class $(\mathscr{A}, \xi_{\mathscr{A}})$ at a level $i > 0$, there is a unique edge to level $i-1$. From Theorem 5.13, there exists an ascending isogeny $\varphi : \mathscr{A} \to \mathscr{B}$ (unique up to isomorphism of $\mathscr{B}$), and from Lemma 5.32(i), there is a unique polarisation $\xi_{\mathscr{B}}$ on $\mathscr{B}$ (up to isomorphism) such that $(\mathscr{A}, \xi_{\mathscr{A}}) \to (\mathscr{B}, \xi_{\mathscr{B}})$ is an edge in $\mathscr{V}^{\mathrm{pp}}$.

These results, and the fact that $\mathscr{V}_0$ is connected, imply that $\mathscr{V}_0^{\mathrm{pp}}$ is connected. We can then deduce (ii) from the action of the Shimura class group $\mathfrak{C}(\mathcal{O}_0)$.

Now, (iii) (respectively, (iv)) is a consequence of Theorem 5.13(iii) (respectively, Theorem 5.13(iv)) together with Lemma 5.32. The statement on multiplicities of the edges also uses the fact that if $\varphi, \psi : \mathscr{A} \to \mathscr{B}$ are two β-isogenies with the same kernel, and $\xi_{\mathscr{A}}$ is a principal polarisation on $\mathscr{A}$, then the two principal polarisations on $\mathscr{B}$ induced via φ and ψ are isomorphic.

The volcano property follows from the corresponding phrase in the statement of Theorem 5.13, and the statement on fields of definition follows from Remark 5.9, which shows that the isomorphism from a principally polarised absolutely simple ordinary abelian variety to its dual, and hence the polarisation, is defined over the field of definition of the variety. □

5.5.3. Principally polarisable surfaces. The result of Theorem 5.31 for abelian surfaces (still absolutely simple, ordinary) is a bit simpler than the general case, thanks to the following lemma.

Lemma 5.33. *Suppose $g = 2$. With all notation as in Theorem 5.31, we have $U(\mathcal{O}_i) = U(\mathcal{O}_0)$ for any non-negative integer i.*

Proof. In these cases, one has $\mathcal{O}_K^\times = \mathcal{O}_{K^+}^\times$ except in the case $K = \mathbf{Q}(\zeta_5)$ (see Remark 5.25); but even when $K = \mathbf{Q}(\zeta_5)$ the equality is true up to units of norm 1. Therefore for any order $\mathcal{O}$ in K, one has $N_{K/K^+}(\mathcal{O}^\times) = N_{K/K^+}((\mathcal{O} \cap K^+)^\times)$. Thus, none of the groups $U(\mathcal{O}_i)$ actually depend on i. □

Therefore, the factors $|U(\mathcal{O}_{i+1})|/|U(\mathcal{O}_i)|$ disappear when $g = 2$. It follows that each component $\mathscr{W}^{\mathrm{pp}}$ is either isomorphic to its image in $(\mathscr{W}_\beta, v_\beta)$, or is isomorphic to the natural double cover of this image constructed by doubling the length of the cycle $\mathscr{V}_0$ (as illustrated in Figure 5.4). The first case occurs when (β) is inert in K/K^+, or when the order of $(\mathfrak{L}, \beta)$ in $\mathfrak{C}(\mathcal{O}_0)$ equals the order of $\mathfrak{L}$ in $\mathrm{Cl}(\mathcal{O}_0)$ (where $\mathfrak{L}$ is a prime ideal of $\mathcal{O}_0$ above (β)). The second case occurs when the order of $(\mathfrak{L}, \beta)$ is twice that of $\mathfrak{L}$.

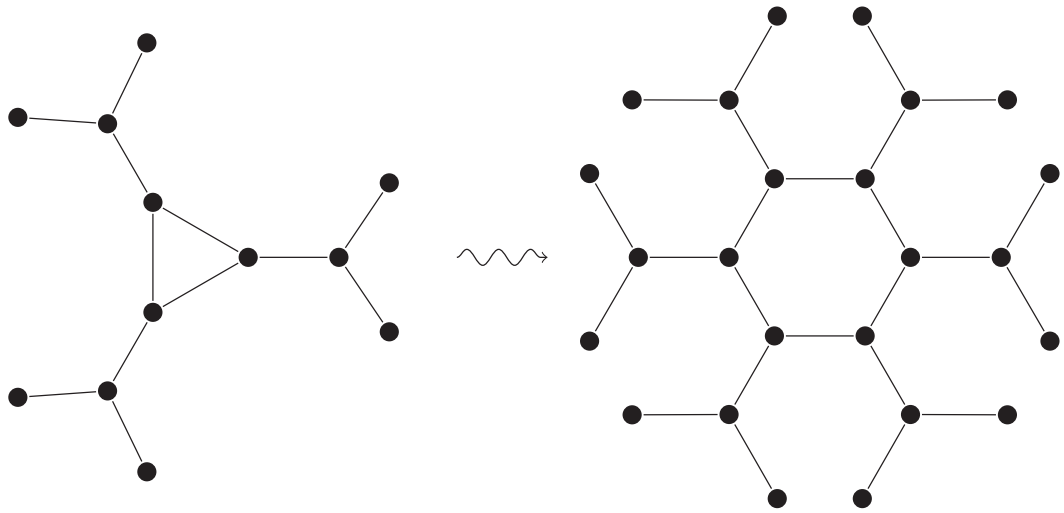


FIGURE 5.4. An example of how adding the polarisation data to a volcano of β-isogenies can double the length of the cycle. The volcanoes are depicted "from above".

5.6. Graphs of (ℓ,ℓ)-isogenies

We now specialise to the case $g = 2$, and the key family of (ℓ,ℓ)-isogenies. Then, $\mathscr{A}$ is an absolutely simple, ordinary, principally polarisable abelian variety of dimension 2, and K is a primitive quartic CM-field. The subfield K^+ is a real quadratic number field.

Definition 5.34 ((ℓ,ℓ)-isogeny)**.** Let $(\mathscr{A},\xi_{\mathscr{A}})$ be a principally polarised abelian surface. We call an isogeny $\varphi\colon \mathscr{A} \to \mathscr{B}$ an (ℓ,ℓ)-isogeny (with respect to $\xi_{\mathscr{A}}$) if $\ker(\varphi)$ is a maximal isotropic subgroup of $\mathscr{A}[\ell]$ with respect to the Weil pairing on $\mathscr{A}[\ell]$ induced by the polarisation isomorphism corresponding to $\xi_{\mathscr{A}}$.

First, note that since $g = 2$, even though the lattice of orders in K is much more intricate than in the quadratic case, there still is some linearity when looking at the suborders $\mathcal{O}^+(\mathscr{A}) = \mathcal{O}(\mathscr{A}) \cap K^+$, since K^+ is a quadratic number field. For any variety $\mathscr{A}$ in the fixed isogeny class, there is an integer f, the conductor of $\mathcal{O}^+(\mathscr{A})$, such that $\mathcal{O}^+(\mathscr{A}) = \mathbf{Z} + f\mathcal{O}_{K^+}$. The local order $\mathfrak{o}^+(\mathscr{A})$ is exactly the order $\mathfrak{o}_n = \mathbf{Z}_\ell + \ell^n \mathfrak{o}_{K^+}$ in K^+_ℓ, where $n = v_\ell(f)$ is the valuation of f at the prime ℓ. The next result describes how (ℓ,ℓ)-isogenies can navigate between these "levels" of real multiplication.

Definition 5.35. Let $\varphi : \mathscr{A} \to \mathscr{B}$ be an isogeny. If $\mathfrak{o}^+(\mathscr{A}) \subsetneq \mathfrak{o}^+(\mathscr{B})$ we say that φ is an *RM-ascending* isogeny, if $\mathfrak{o}^+(\mathscr{B}) \subsetneq \mathfrak{o}^+(\mathscr{A})$ we say it is *RM-descending*, otherwise $\mathfrak{o}^+(\mathscr{A}) = \mathfrak{o}^+(\mathscr{B})$ and it is *RM-horizontal*.

Theorem 5.36. *Suppose $\mathfrak{o}^+(\mathscr{A}) = \mathfrak{o}_n$ with $n > 0$. For any principal polarisation ξ on $\mathscr{A}$, the kernels of (ℓ,ℓ)-isogenies from $(\mathscr{A},\xi)$ are:*

- *(i) A unique RM-ascending one, whose target has local order $\mathfrak{o}_{n-1} \cdot \mathfrak{o}(\mathscr{A})$ (in particular, the local real order of the target is $\mathfrak{o}_{n-1}$, and the kernel is defined over the same field as $\mathscr{A}$);*
- *(ii) $\ell^2 + \ell$ RM-horizontal ones;*
- *(iii) ℓ^3 RM-descending isogenies, whose targets have local real order $\mathfrak{o}_{n+1}$.*

The above theorem is proven in Section 5.7. Note that we start by considering (ℓ,ℓ)-isogenies defined over the algebraic closure of the finite field k; in virtue of Remark 5.9, it is then easy to deduce the results on isogenies defined over k.

Second, we focus our attention to abelian surfaces with maximal real multiplication at ℓ (i.e., the case $n = 0$ above). The description of $\mathfrak{l}$-isogeny graphs provided by Theorem 5.13 leads to a complete understanding of graphs of (ℓ,ℓ)-isogenies preserving the maximal real order locally at ℓ, via the next theorem. More precisely, we study the structure of the graph $\mathscr{G}_{\ell,\ell}$ whose vertices are the isomorphism classes of principally polarisable surfaces $\mathscr{A}$ in the fixed isogeny class, which have maximal real multiplication locally at ℓ (i.e., $\mathfrak{o}_{K^+} \subset \mathfrak{o}(\mathscr{A})$), with an edge of multiplicity m from such a vertex $\mathscr{A}$ to a vertex $\mathscr{B}$ if there are m distinct subgroups $\kappa \subset \mathscr{A}$ that are kernels of (ℓ,ℓ)-isogenies such that $\mathscr{A}/\kappa \cong \mathscr{B}$. This definition will be justified by the fact that the kernels of (ℓ,ℓ)-isogenies preserving the maximal real multiplication locally at ℓ do not depend on the choice of a principal polarisation on the source (see Remark 5.58). The following theorem is proven in Section 5.8, where its consequences are discussed in detail.

Theorem 5.37. *Suppose that $\mathscr{A}$ has maximal real multiplication locally at ℓ. Let ξ be any principal polarisation on $\mathscr{A}$. There is a total of $\ell^3+\ell^2+\ell+1$ kernels of (ℓ,ℓ)-isogenies from $\mathscr{A}$ with respect to ξ. Among these, the kernels whose target also has maximal local real order do not depend on ξ, and are:*

(i) the ℓ^2+1 kernels of $\ell\mathcal{O}_{K^+}$-isogenies if ℓ is inert in K^+;
(ii) the $\ell^2+2\ell+1$ kernels of compositions of an $\mathfrak{l}_1$-isogeny with an $\mathfrak{l}_2$-isogeny if ℓ splits as $\mathfrak{l}_1\mathfrak{l}_2$ in K^+;
(iii) the $\ell^2+\ell+1$ kernels of compositions of two $\mathfrak{l}$-isogenies if ℓ ramifies as $\mathfrak{l}^2$ in K^+.

The other (ℓ,ℓ)-isogenies have targets with real multiplication by $\mathbf{Z}_\ell + \ell\mathfrak{o}_{K^+}$.

5.6.1. Polarisations and symplectic structures. One knows that if $\varphi\colon \mathscr{A} \to \mathscr{B}$ is an (ℓ,ℓ)-isogeny with respect to a principal polarisation $\xi_{\mathscr{A}}$ on $\mathscr{A}$, then there is a unique principal polarisation $\xi_{\mathscr{B}}$ on $\mathscr{B}$ such that $\varphi^*\xi_{\mathscr{B}} = \xi_{\mathscr{A}}^\ell$ (this is a consequence of Grothendieck descent [Mum66, pp. 290–291]; see also [Rob10, Proposition 2.4.7]). This allows us to view an isogeny of *a priori* non-polarised abelian varieties φ as an isogeny of polarised abelian varieties $\varphi\colon (\mathscr{A},\xi_{\mathscr{A}}^\ell) \to (\mathscr{B},\xi_{\mathscr{B}})$.

Let $T = T_\ell\mathscr{A}$, and $V = T \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$. As for $\mathfrak{l}$-isogenies, we are studying (ℓ,ℓ)-isogenies through the lens of lattices in V. The polarisation data, preserved by (ℓ,ℓ)-isogenies, translates nicely in the world of lattices by endowing V with a symplectic structure. Fix a polarisation $\xi_{\mathscr{A}}$ of $\mathscr{A}$. It induces a polarisation isogeny $\lambda : \mathscr{A} \to \mathscr{A}^\vee$, which in turn gives a map $T \to T_\ell(\mathscr{A}^\vee)$. Therefore the Weil pairing equips T with a natural $\mathbf{Z}_\ell$-linear pairing $\langle -,-\rangle$, which extends to a pairing on V. The pairing $\langle -,-\rangle$ is symplectic, and it satisfies $\langle \alpha x, y\rangle = \langle x, \alpha^\dagger y\rangle$ for any $\alpha \in K$ (see [Mil86b, Lemma 16.2e, and Section 167]). For Γ a lattice in V, write

$$\Gamma^* = \{\alpha \in V \mid \langle \alpha, \Gamma\rangle \subset \mathbf{Z}_\ell\}$$

for the dual lattice of Γ. Then $T \subset T^*$, and the quotient is isomorphic to $(\ker\lambda)[\ell^\infty]$. In particular, T is self-dual if and only if the degree of λ is coprime to ℓ. Therefore T is a self-dual lattice when $\xi_{\mathscr{A}}$ is a principal polarisation.

5.7. Levels for the real multiplication in dimension 2

Again, fix an absolutely simple, ordinary, principally polarisable abelian variety $\mathscr{A}$ of dimension 2. Then K is a primitive quartic CM-field, and the subfield K^+ is a real quadratic number field. The orders in K_ℓ^+ are linearly ordered, since they are all of the form $\mathfrak{o}_n = \mathbf{Z}_\ell + \ell^n \mathfrak{o}_{K^+}$. These integers n can be seen as "levels" of real multiplication. The goal of this section is to take advantage of this linear structure to prove Theorem 5.36.

5.7.1. Preliminaries on symplectic lattices. Let $\mathbf{F}_\ell$ be the finite field with ℓ elements.

Lemma 5.38. *Let W be a symplectic $\mathbf{F}_\ell$-vector space of dimension 4. It contains exactly $\ell^3 + \ell^2 + \ell + 1$ maximal isotropic subspaces.*

Proof. In the following, a *line* or a *plane* means a dimension 1 or 2 subspace of a vector space (i.e., they contain the origin of the vector space). Fix any line L in W. We will count the number of maximal isotropic subspaces of W containing L. The line L is itself isotropic (yet not maximal), so $L \subset L^\perp$. Also, $\dim L + \dim L^\perp = 4$, so $\dim L^\perp = 3$. Since any maximal isotropic subspace of W is of dimension 2, it is easy to see that those containing L are exactly the planes in $L^\perp$ containing L. There are $\ell + 1$ such planes, because they are in natural correspondence with the lines in the dimension 2 vector space $L^\perp/L$. It follows that there are $\ell + 1$ maximal isotropic subspaces of W containing L. Because there are $\ell^3 + \ell^2 + \ell + 1$ lines L in W, and each maximal isotropic subspace of W contains $\ell + 1$ lines, we conclude that there are $\ell^3 + \ell^2 + \ell + 1$ maximal isotropic subspaces. □

Lemma 5.39. *Let V be a symplectic $\mathbf{Q}_\ell$-vector space of dimension 4. Let $\Lambda \subset V$ be a lattice in V such that $\Lambda^* = \Lambda$. Then $\Lambda/\ell\Lambda$ is a symplectic $\mathbf{F}_\ell$-vector space of dimension 4 for the symplectic form*

$$\langle \lambda + \ell\Lambda, \mu + \ell\Lambda \rangle_\ell = \langle \lambda, \mu \rangle \mod \ell.$$

Proof. The fact that the form $\langle -, - \rangle_\ell$ is bilinear and alternating easily follows from the fact that the form $\langle -, - \rangle$ is symplectic. It only remains to prove that it is non-degenerate. Let $\lambda \in \Lambda$, and suppose that $\langle \lambda + \ell\Lambda, \mu + \ell\Lambda \rangle_\ell = 0$ for any $\mu \in \Lambda$. We now prove that $\lambda \in \ell\Lambda$. For any $\mu \in \Lambda$, we have $\langle \lambda, \mu \rangle \in \ell\mathbf{Z}_\ell$, and therefore $\langle \ell^{-1}\lambda, \mu \rangle \in \mathbf{Z}_\ell$. So $\ell^{-1}\lambda \in \Lambda^* = \Lambda$, whence $\lambda \in \ell\Lambda$, concluding the proof. □

Lemma 5.40. *Let V be a symplectic $\mathbf{Q}_\ell$-vector space of dimension 4, and Λ a self-dual lattice in V. Let $\ell\Lambda \subset \Gamma \subset \Lambda$ be an intermediate lattice. Then $\Gamma/\ell\Lambda$ is maximal isotropic in $\Lambda/\ell\Lambda$ if and only if $\Gamma^* = \ell^{-1}\Gamma$.*

Proof. First, suppose that $\Gamma/\ell\Lambda$ is maximal isotropic. Fix $\gamma \in \Gamma$. For any $\delta \in \Gamma$, since $\Gamma/\ell\Lambda$ is isotropic, we have $\langle \gamma, \delta \rangle \in \ell\mathbf{Z}_\ell$, so $\langle \ell^{-1}\gamma, \delta \rangle \in \mathbf{Z}_\ell$ and therefore $\ell^{-1}\gamma \in \Gamma^*$. This proves that $\ell^{-1}\Gamma \subset \Gamma^*$. Now, let $\alpha \in \Gamma^*$. Observe that $\langle \ell\alpha, \gamma \rangle = \ell\langle \alpha, \gamma \rangle \in \ell\mathbf{Z}_\ell$ for any $\gamma \in \Gamma$. This implies that $\ell^{-1}\alpha$ must be in Γ, because $\Gamma/\ell\Lambda$ is maximally isotropic. This proves that $\ell^{-1}\Gamma^* \subset \Gamma$.

Now, suppose that $\Gamma^* = \ell^{-1}\Gamma$. Then, $\langle \ell^{-1}\Gamma, \Gamma \rangle \subset \mathbf{Z}_\ell$, so $\langle \Gamma, \Gamma \rangle \in \ell\mathbf{Z}_\ell$, and $\Gamma/\ell\Lambda$ is isotropic. Let $\lambda \in \Lambda$ such that $\langle \lambda + \ell\Lambda, \Gamma/\ell\Lambda \rangle_\ell = \{0\}$. Then, $\langle \ell^{-1}\lambda, \Gamma \rangle \subset \ell\mathbf{Z}_\ell$, so $\ell^{-1}\lambda \in \Gamma^* = \ell^{-1}\Gamma$, which implies that $\lambda \in \Gamma$. So $\Gamma/\ell\Lambda$ is maximal isotropic. □

Definition 5.41 ((ℓ,ℓ)-neighbors)**.** The set $\mathscr{L}(\Lambda)$ of (ℓ,ℓ)-*neighbors* of Λ is the set of lattices Γ such that $\ell\Lambda \subset \Gamma \subset \Lambda$, and $\Gamma/\ell\Lambda$ is maximal isotropic in $\Lambda/\ell\Lambda$.

Again, using Proposition 5.7, we obtain:

Proposition 5.42. *With $T = T_\ell\mathscr{A}$, the (ℓ,ℓ)-isogenies $\mathscr{A} \to \mathscr{B}$ correspond, under Proposition 5.7, to the lattices Γ with $T \subset \Gamma \subset \frac{1}{\ell}T$ and Γ/T a maximal isotropic subspace of $\frac{1}{\ell}T/T$, i.e., to (ℓ,ℓ)-neighbors of T rescaled by a factor ℓ^{-1}.*

5.7.2. (ℓ,ℓ)-neighboring lattices. Throughout this section, V is a symplectic $\mathbf{Q}_\ell$-vector space of dimension 4. Again, we consider a prime number ℓ, a quartic CM-field K, with K^+ its quadratic real subfield. The algebra $K_\ell = K \otimes_{\mathbf{Q}} \mathbf{Q}_\ell$ is a $\mathbf{Q}_\ell$-algebra of dimension 4, with an involution $x \mapsto x^\dagger$ fixing K_ℓ^+ induced by the generator of $\mathrm{Gal}(K/K^+)$. Suppose that K_ℓ acts ($\mathbf{Q}_\ell$-linearly) on V, and that for any $x \in K_\ell$, $u, v \in V$, we have $\langle xu, v\rangle = \langle u, x^\dagger v\rangle$. For any lattice Λ in V, the *real order* of Λ is the order in $K_\ell^+ = K^+ \otimes_{\mathbf{Q}} \mathbf{Q}_\ell$ defined as

$$\mathfrak{o}^+(\Lambda) = \{x \in K_\ell^+ \mid x\Lambda \subset \Lambda\}.$$

Any order in K_ℓ^+ is of the form $\mathfrak{o}_n = \mathbf{Z}_\ell + \ell^n \mathfrak{o}_{K^+}$, for some non-negative integer n, with $\mathfrak{o}_{K^+}$ the maximal order of K_ℓ^+. We say that Λ is an $\mathfrak{o}_n$-lattice if $\mathfrak{o}(\Lambda) = \mathfrak{o}_n$. The goal of this section is to prove the following lattice counterpart of Theorem 5.36.

Proposition 5.43. *Let Λ be a self-dual $\mathfrak{o}_n$-lattice, with $n > 0$. The set $\mathscr{L}(\Lambda)$ of its (ℓ,ℓ)-neighbors contains exactly one $\mathfrak{o}_{n-1}$-lattice, namely $\ell\mathfrak{o}_{n-1}\Lambda$, as well as $\ell^2+\ell$ lattices of real order $\mathfrak{o}_n$, and ℓ^3 lattices of real order $\mathfrak{o}_{n+1}$.*

Lemma 5.44. *Let Λ be a self-dual $\mathfrak{o}_n$-lattice in V, for some non-negative integer n. Then, Λ is a free $\mathfrak{o}_n$-module of rank 2.*

Proof. By Lemma 5.14, the order $\mathfrak{o}_n$ is a Gorenstein ring of dimension 1, and it follows from [Bas63, Theorem 6.2] that Λ is a reflexive $\mathfrak{o}_n$-module. From [Bas63, Proposition 7.2], Λ has a projective direct summand, so $\Lambda = \mathfrak{o}_n e_1 \oplus M$ for some $e_1 \in \Lambda$, and M an $\mathfrak{o}_n$-submodule. This M is still reflexive (any direct summand of a reflexive module is reflexive). So applying [Bas63, Proposition 7.2] again to M, together with the fact that it has $\mathbf{Z}_\ell$-rank 2, there is a non-negative integer $m \le n$ and an element $e_2 \in \Lambda$ such that $M = \mathfrak{o}_m e_2$. We shall prove that $m = n$. By contradiction, assume $m < n$. We have $\Lambda/\ell\Lambda = (\mathfrak{o}_n e_1/\ell\mathfrak{o}_n) \oplus (\mathfrak{o}_m e_2/\ell\mathfrak{o}_m)$. Observe that $\mathfrak{o}_m e_2/\ell\mathfrak{o}_m$ is maximal isotropic. Indeed, it is of dimension 2, and for any $x, y \in \mathfrak{o}_m$, $\langle xe_2, ye_2\rangle = -\langle ye_2, xe_2\rangle$ because the form is alternating, and $\langle xe_2, ye_2\rangle = \langle ye_2, xe_2\rangle$ because it is K^+-bilinear, so $\langle xe_2, ye_2\rangle = 0$. Also, we have $\mathfrak{o}_{n-1} \subset \mathfrak{o}_m$, so

$$\langle \ell\mathfrak{o}_{n-1}e_1, \mathfrak{o}_m e_2\rangle = \langle \ell e_1, \mathfrak{o}_{n-1}\mathfrak{o}_m e_2\rangle = \ell\langle e_1, \mathfrak{o}_m e_2\rangle \subset \ell\mathbf{Z}_\ell.$$

This proves that $\ell\mathfrak{o}_{n-1}e_1/\ell\mathfrak{o}_n \subset (\mathfrak{o}_m e_2/\ell\mathfrak{o}_m)^\perp = \mathfrak{o}_m e_2/\ell\mathfrak{o}_m$, a contradiction. □

Using a standard abuse of notation, write $\mathbf{F}_\ell[\epsilon]$ for the ring of dual numbers, i.e., an $\mathbf{F}_\ell$-algebra isomorphic to $\mathbf{F}_\ell[X]/X^2$ via an isomorphism sending ϵ to X.

Lemma 5.45. *Let $R = \mathbf{F}_\ell[\epsilon]f_1 \oplus \mathbf{F}_\ell[\epsilon]f_2$ be a free $\mathbf{F}_\ell[\epsilon]$-module of rank 2. The $\mathbf{F}_\ell[\epsilon]$-submodules of R of $\mathbf{F}_\ell$-dimension 2 are exactly the $\ell^2+\ell+1$ modules ϵR, and $\mathbf{F}_\ell[\epsilon]\cdot g$ for any $g \notin \epsilon R$. A complete list of these orbits $\mathbf{F}_\ell[\epsilon]\cdot g$ is given by $\mathbf{F}_\ell[\epsilon]\cdot(b\epsilon f_1 + f_2)$ for any $b \in \mathbf{F}_\ell$, and $\mathbf{F}_\ell[\epsilon]\cdot(f_1 + \alpha f_2 + \beta\epsilon f_2)$, for any $\alpha, \beta \in \mathbf{F}_\ell$.*

Proof. Let $H \subset R$ be a subspace of dimension 2, stable under the action of $\mathbf{F}_\ell[\epsilon]$. For any $g \in H$, write $g = a_g f_1 + b_g\epsilon f_1 + c_g f_2 + d_g\epsilon f_2 \in H$ for $a_g, b_g, c_g, d_g \in \mathbf{F}_\ell$. Since H is $\mathbf{F}_\ell[\epsilon]$-stable, for any $g \in H$, the element $g\epsilon = a_g\epsilon f_1 + c_g\epsilon f_2$ is also in H.

First suppose $a_g = 0$ and $c_g = 0$ for any $g \in H$. Then, as $H = \epsilon R$, it is indeed an $\mathbf{F}_\ell[\epsilon]$-submodule and has $\mathbf{F}_\ell$-dimension 2. Now, suppose $a_g = 0$ for any $g \in H$, but H

contains an element g such that $c_g \neq 0$. Then, H contains both $b_g\epsilon f_1 + c_g f_2 + d_g\epsilon f_2$, and $c_g\epsilon f_2$, so H is the $\mathbf{F}_\ell$-vector space spanned by ϵf_2 and $b_g\epsilon f_1 + c_g f_2$. There are $\ell+1$ such subspaces H (one for each possible $(b_g : c_g) \in \mathbf{P}^1(\mathbf{F}_\ell)$), and all of them are of dimension 2 and R-stable.

Finally, suppose there exists $g \in H$ such that $a_g \neq 0$. Then, it is spanned as an $\mathbf{F}_\ell$-vector spaces by a pair $\{f_1 + \alpha f_2 + \beta\epsilon f_2, \epsilon f_1 + \alpha\epsilon f_2\}$, with $\alpha, \beta \in \mathbf{F}_\ell$, and any of the ℓ^2 subspaces of this form are $\mathbf{F}_\ell[\epsilon]$-submodules. □

Lemma 5.46. *Let Λ be an $\mathfrak{o}_n$-lattice, for some non-negative integer n. For any element $g \in \Lambda/\ell\Lambda$, the orbit $\mathfrak{o}_n \cdot g$ is an isotropic subspace of $\Lambda/\ell\Lambda$.*

Proof. Let $\lambda \in \Lambda$ such that $g = \lambda + \ell\Lambda$. For any $\alpha, \beta \in \mathfrak{o}_n$, we have $\langle\alpha\lambda, \beta\lambda\rangle = -\langle\beta\lambda, \alpha\lambda\rangle$ because the symplectic form on V is alternating, and $\langle\alpha\lambda, \beta\lambda\rangle = \langle\beta\lambda, \alpha\lambda\rangle$ because it is K^+-bilinear. So $\langle\alpha g, \beta g\rangle_\ell = 0$, and the orbit of g is isotropic. □

Proof of Proposition 5.43. From Lemma 5.44, Λ splits as $e_1\mathfrak{o}_n \oplus e_2\mathfrak{o}_n$, for some $e_1, e_2 \in \Lambda$. Observe that there is an element $\epsilon \in \mathfrak{o}_n$ such that $\mathfrak{o}_n/\ell\mathfrak{o}_n = \mathbf{F}_\ell[\epsilon] \cong \mathbf{F}_\ell[X]/(X^2)$, via the isomorphism sending ϵ to X. The quotient $R = \Lambda/\ell\Lambda$ is a free $\mathbf{F}_\ell[\epsilon]$-module of rank 2. Let $\pi : \Lambda \to R$ be the canonical projection. The set $\{f_1, \epsilon f_1, f_2, \epsilon f_2\}$ forms an $\mathbf{F}_\ell$-basis of R, where $f_i = \pi(e_i)$.

From Lemma 5.45, R contains $\ell^2+\ell+1$ subspaces of dimension 2 that are $\mathbf{F}_\ell[\epsilon]$-stable. The subspace $\epsilon R = \mathbf{F}_\ell\epsilon f_1 \oplus \mathbf{F}_\ell\epsilon f_2$ is isotropic because

$$\langle\epsilon f_1, \epsilon f_2\rangle_\ell = \langle f_1, \epsilon^2 f_2\rangle_\ell = 0.$$

Together with Lemma 5.46, we conclude that all $\ell^2 + \ell + 1$ of these $\mathbf{F}_\ell[\epsilon]$-stable subspaces are maximal isotropic. From Lemma 5.38, R contains a total of $\ell^3 + \ell^2 + \ell + 1$ maximal isotropic subspaces. Thus, the (ℓ, ℓ)-neighbors corresponding to the remaining ℓ^3 subspaces are not stable for the action of $\mathfrak{o}_n$. They are however stable for the action of $\mathfrak{o}_{n+1}$, so those are $\mathfrak{o}_{n+1}$-lattices.

It remains to prove that among the $\ell^2 + \ell + 1$ neighbors that are $\mathfrak{o}_n$-stable, only the lattice $\ell\mathfrak{o}_{n-1}\Lambda$ (which corresponds to the subspace ϵR) is $\mathfrak{o}_{n-1}$-stable, and that it is not $\mathfrak{o}_{n-2}$-stable. This would prove that $\ell\mathfrak{o}_{n-1}\Lambda$ is an $\mathfrak{o}_{n-1}$-lattice, and the $\ell^2 + \ell$ other lattices have order $\mathfrak{o}_n$.

Write $\Gamma = \ell\mathfrak{o}_{n-1}\Lambda$. Then $\pi(\Gamma) = \epsilon R$ is maximal isotropic and $\mathbf{F}_\ell[\epsilon]$-stable. Suppose by contradiction that we have $\mathfrak{o}_{n-2}\Gamma \subset \Gamma$. Then, $\ell\mathfrak{o}_{n-2}\Lambda \subset \mathfrak{o}_{n-2}\Gamma \subset \Gamma \subset \Lambda$, so $\ell\mathfrak{o}_{n-2}\Lambda \subset \Lambda$. But $\ell\mathfrak{o}_{n-2} \not\subset \mathfrak{o}_n$, which contradicts the fact that Λ is an $\mathfrak{o}_n$-lattice. Therefore Γ is an $\mathfrak{o}_{n-1}$-lattice.

Let $H \subset R$ be another maximal isotropic subspace, and suppose that $\pi^{-1}(H)$ is $\mathfrak{o}_{n-1}$-stable. Let $\lambda = e_1(a + \ell^n x) + e_2(b + \ell^n y) \in \pi^{-1}(H)$, with $a, b \in \mathbf{Z}_\ell$ and $x, y \in \mathfrak{o}_{K^+}$, and let $z \in \mathfrak{o}_{n-1}$. A simple computation yields

$$\Lambda = z\lambda + \Lambda = zae_1 + zbe_2 + \Lambda.$$

Therefore, both za and zb must be in $\mathfrak{o}_n$ for any $z \in \mathfrak{o}_{n-1}$. It follows that a and b must be in $\ell\mathbf{Z}_\ell$, whence $\lambda \in \Gamma$. So $\pi^{-1}(H) \subset \Gamma$, and we conclude that $H = \epsilon R$ from the fact that both are maximal isotropic. This proves that no (ℓ, ℓ)-neighbor other that Γ is $\mathfrak{o}_{n-1}$-stable. □

5.7.3. Changing the real multiplication with (ℓ, ℓ)-isogenies. The results for lattices are now ready to be applied to analyse how (ℓ, ℓ)-isogenies can change the real multiplication. Fix a principally polarisable absolutely simple ordinary abelian surface $\mathscr{A}$ over $k = \mathbf{F}_q$. As usual, K is its endomorphism algebra, and K^+ the maximal real

subfield of K. The local real order $\mathfrak{o}^+(\mathscr{A})$ of $\mathscr{A}$ is of the form $\mathfrak{o}_n = \mathbf{Z}_\ell + \ell^n \mathfrak{o}_{K^+}$ for some non-negative integer n.

Proof of Theorem 5.36. It follows from Proposition 5.43 together with Proposition 5.42, and the observation that the $\mathfrak{o}_{n-1}$-lattice $\ell\mathfrak{o}_{n-1}\Lambda$ has order $\mathfrak{o}_{n-1} \cdot \mathfrak{o}(\Lambda)$. □

In the following, we show that some structure of the graphs of horizontal isogenies at any level (of real multiplication) can be inferred from the structure at the maximal level: indeed, there is a graph homomorphism from any non-maximal level to the level above.

Definition 5.47 (RM-predecessor)**.** Suppose $\mathfrak{o}^+(\mathscr{A}) = \mathfrak{o}_n$ with $n > 0$. Note that the kernel κ of the unique RM-ascending isogeny of Proposition 5.36 is given by the quotient $(\mathfrak{o}_{n-1}T_\ell\mathscr{A})/T_\ell\mathscr{A}$ (via Proposition 5.7) and does not depend on the polarisation. The *RM-predecessor* of $\mathscr{A}$ is the variety $\mathrm{pr}(\mathscr{A}) = \mathscr{A}/\kappa$, and we denote by $\mathrm{up}_\mathscr{A} : \mathscr{A} \to \mathscr{A}/\kappa$ the canonical projection. If ξ is a principal polarisation on $\mathscr{A}$, let $\mathrm{pr}(\xi)$ be the unique principal polarisation induced by ξ via $\mathrm{up}_\mathscr{A}$.

Proposition 5.48. *Suppose $n > 0$. For any principal polarisation ξ on $\mathscr{A}$, and any RM-horizontal (ℓ,ℓ)-isogeny $\varphi : \mathscr{A} \to \mathscr{B}$ with respect to ξ, there is an (ℓ,ℓ)-isogeny $\tilde{\varphi} : \mathrm{pr}(\mathscr{A}) \to \mathrm{pr}(\mathscr{B})$ with respect to $\mathrm{pr}(\xi)$ such that the following diagram commutes:*

$$\begin{array}{ccc} \mathrm{pr}(\mathscr{A}) & \xrightarrow{\tilde{\varphi}} & \mathrm{pr}(\mathscr{B}) \\ {\scriptstyle \mathrm{up}_\mathscr{A}}\uparrow & & \uparrow{\scriptstyle \mathrm{up}_\mathscr{B}} \\ \mathscr{A} & \xrightarrow{\varphi} & \mathscr{B}. \end{array}$$

Proof. This follows from the fact that if Λ is an $\mathfrak{o}_n$-lattice and $\Gamma \in \mathscr{L}(\Lambda)$ is an (ℓ,ℓ)-neighbor of Λ, then $\ell\mathfrak{o}_{n-1}\Gamma \in \mathscr{L}(\ell\mathfrak{o}_{n-1}\Lambda)$. □

5.8. (ℓ,ℓ)-isogenies preserving the real multiplication

In this section, we prove Theorem 5.37 by analysing the relationship between $\mathfrak{l}$-isogenies and (ℓ,ℓ)-isogenies preserving the maximal real multiplication.

5.8.1. (ℓ,ℓ)-neighbors and $\mathfrak{l}$-neighbors. Let $\mathscr{L}^+(\Lambda)$ be the set of (ℓ,ℓ)-neighbors of the lattice Λ with maximal real multiplication. These neighbors will be analysed through $\mathfrak{l}$-neighbors, for $\mathfrak{l}$ a prime ideal in $\mathfrak{o}_{K^+}$. This will allow us to account for the possible splitting behaviors of ℓ. The relation between the set $\mathscr{L}^+(\Lambda)$ and the sets $\mathscr{L}_\mathfrak{l}(\Lambda)$ is given by the following proposition proved case-by-case in the following three sections, as Propositions 5.50, 5.54 and 5.56:

Proposition 5.49. *Let Λ be a lattice with maximal real multiplication. The set of (ℓ,ℓ)-neighbors with maximal real multiplication is*

$$\mathscr{L}^+(\Lambda) = \begin{cases} \mathscr{L}_{\ell\mathfrak{o}_{K^+}}(\Lambda) & \text{if } \ell \text{ is inert in } K^+, \\ \mathscr{L}_{\mathfrak{l}_1}[\mathscr{L}_{\mathfrak{l}_2}(\Lambda)] = \mathscr{L}_{\mathfrak{l}_2}[\mathscr{L}_{\mathfrak{l}_1}(\Lambda)] & \text{if } \ell \text{ splits as } \mathfrak{l}_1\mathfrak{l}_2 \text{ in } K^+, \\ \mathscr{L}_\mathfrak{l}[\mathscr{L}_\mathfrak{l}(\Lambda)] & \text{if } \ell \text{ ramifies as } \mathfrak{l}^2 \text{ in } K^+. \end{cases}$$

5.8.1.1. *The inert case.* Suppose that ℓ is inert in K^+. Then, $\ell\mathcal{O}_{K^+}$ is the unique prime ideal of K^+ above ℓ. The orders in K_ℓ with maximal real multiplication are exactly the orders $\mathfrak{o}_\mathfrak{f}$ with $\mathfrak{f} = \ell^n\mathfrak{o}_{K^+}$, i.e., the orders $\mathfrak{o}_{K^+} + \ell^n\mathfrak{o}_K$ with $n \geq 0$.

Proposition 5.50. *Let Λ be a lattice with maximal real multiplication. If ℓ is inert in K^+, the set of (ℓ,ℓ)-neighbors with maximal real multiplication is*

$$\mathscr{L}^+(\Lambda) = \mathscr{L}_{\ell\mathfrak{o}_{K^+}}(\Lambda).$$

Proof. Since $\mathfrak{o}_{K^+}/\ell\mathfrak{o}_{K^+} \cong \mathbf{F}_{\ell^2}$, $\Lambda/\ell\Lambda$ is a free $\mathfrak{o}(\Lambda)/\ell\mathfrak{o}(\Lambda)$-module of rank 1. In particular, it is a vector space over $\mathbf{F}_{\ell^2}$ of dimension 2, and thereby the $\mathfrak{o}_{K^+}$-stable maximal isotropic subspaces of $\Lambda/\ell\Lambda$ are $\mathbf{F}_{\ell^2}$-lines. Since any $\mathbf{F}_{\ell^2}$-line is isotropic, $\mathscr{L}_{\ell\mathfrak{o}_{K^+}}(\Lambda)$ is precisely the set of (ℓ,ℓ)-neighbors preserving the maximal real multiplication. □

Remark 5.51. The structure of $\mathscr{L}^+(\Lambda)$ is then fully described by Proposition 5.18, with $\mathfrak{l} = \ell\mathfrak{o}_{K^+}$, and $N\mathfrak{l} = \ell^2$. In particular, $\mathscr{L}(\Lambda)$ consists of ℓ^2+1 neighbors with maximal real multiplication, and $\ell^3+\ell$ with real multiplication by $\mathfrak{o}_1 = \mathbf{Z} + \ell\mathfrak{o}_{K^+}$.

The split case. Suppose that ℓ splits in K^+ as $\ell\mathcal{O}_{K^+} = \mathfrak{l}_1\mathfrak{l}_2$. The orders in K_ℓ with maximal real multiplication are exactly the orders $\mathfrak{o}_\mathfrak{f} = \mathfrak{o}_{K^+} + \mathfrak{f}\mathfrak{o}_K$, where $\mathfrak{f} = \mathfrak{l}_1^m\mathfrak{l}_2^n$ for any non-negative integers m and n.

Lemma 5.52. *Suppose Λ has maximal real multiplication. Then, we have the orthogonal decomposition $\Lambda/\ell\Lambda = (\mathfrak{l}_1\Lambda/\ell\Lambda) \perp (\mathfrak{l}_2\Lambda/\ell\Lambda)$.*

Proof. Let $\mathfrak{o} = \mathfrak{o}(\Lambda)$. Since $\mathfrak{l}_1$ and $\mathfrak{l}_2$ are coprime and $\mathfrak{l}_1\mathfrak{l}_2 = \ell\mathfrak{o}_{K^+}$, the quotient $\mathfrak{o}/\ell\mathfrak{o}$ splits as $\mathfrak{l}_1\mathfrak{o}/\ell\mathfrak{o} \oplus \mathfrak{l}_2\mathfrak{o}/\ell\mathfrak{o}$. It follows that $\Lambda/\ell\Lambda = (\mathfrak{l}_1\Lambda/\ell\Lambda) \oplus (\mathfrak{l}_2\Lambda/\ell\Lambda)$. Furthermore, $\langle \mathfrak{l}_1\Lambda, \mathfrak{l}_2\Lambda\rangle = \langle \Lambda, \mathfrak{l}_1\mathfrak{l}_2\Lambda\rangle = \langle \Lambda, \ell\Lambda\rangle \subset \ell\mathbf{Z}_\ell$, so $\mathfrak{l}_1\Lambda/\ell\Lambda \subset (\mathfrak{l}_2\Lambda/\ell\Lambda)^\perp$. The last inclusion is also an equality because both $\mathfrak{l}_1\Lambda/\ell\Lambda$ and $\mathfrak{l}_2\Lambda/\ell\Lambda$ have dimension 2. □

Lemma 5.53. *Suppose Λ has maximal real multiplication. An (ℓ,ℓ)-neighbor $\Gamma \in \mathscr{L}(\Lambda)$ has maximal real multiplication if and only if there exist $\Gamma_1 \in \mathscr{L}_{\mathfrak{l}_1}(\Lambda)$ and $\Gamma_2 \in \mathscr{L}_{\mathfrak{l}_2}(\Lambda)$ such that $\Gamma = \mathfrak{l}_2\Gamma_1 + \mathfrak{l}_1\Gamma_2$.*

Proof. First, let $\Gamma \in \mathscr{L}(\Lambda)$ be an (ℓ,ℓ)-neighbor with maximal real multiplication. Defining $\Gamma_i = \Gamma + \mathfrak{l}_i\Lambda$, we then have

$$\mathfrak{l}_2\Gamma_1 + \mathfrak{l}_1\Gamma_2 = (\mathfrak{l}_1+\mathfrak{l}_2)\Gamma + \ell\Lambda = \mathfrak{o}_{K^+}\Gamma + \ell\Lambda = \Gamma.$$

By contradiction, suppose $\Gamma_i \notin \mathscr{L}_i(\Lambda)$. Then, Γ_i is either Λ or $\mathfrak{l}_i\Lambda$. Suppose first that $\Gamma_i = \Lambda$. Then $\Gamma \subset \mathfrak{l}_i\Lambda$, and even $\Gamma = \mathfrak{l}_i\Lambda$ since $[\Lambda:\Gamma] = [\Lambda:\mathfrak{l}_i\Lambda] = \ell^2$. But the orthogonal decomposition of Lemma 5.52 implies that $\mathfrak{l}_i\Lambda/\Lambda$ is not isotropic, contradicting the fact that $\Gamma \in \mathscr{L}(\Lambda)$.

For the converse, suppose $\Gamma = \mathfrak{l}_2\Gamma_1 + \mathfrak{l}_1\Gamma_2$ for some $\Gamma_1 \in \mathscr{L}_{\mathfrak{l}_1}(\Lambda)$ and $\Gamma_2 \in \mathscr{L}_{\mathfrak{l}_2}(\Lambda)$. Then $\Gamma/\ell\Lambda$ is of dimension 2, so it suffices to prove that it is isotropic. Each summand $\mathfrak{l}_i\Gamma_j$ is isotropic, because it is of dimension 1, and Lemma 5.52 implies that $\mathfrak{l}_2\Gamma_1$ and $\mathfrak{l}_1\Gamma_2$ are orthogonal, so their sum Γ is isotropic. □

Proposition 5.54. *Suppose Λ has maximal real multiplication. If ℓ splits in K^+ as $\ell\mathfrak{o}_{K^+} = \mathfrak{l}_1\mathfrak{l}_2$, the set of (ℓ,ℓ)-neighbors of Λ with maximal real multiplication is*

$$\mathscr{L}^+(\Lambda) = \mathscr{L}_{\mathfrak{l}_1}[\mathscr{L}_{\mathfrak{l}_2}(\Lambda)] = \mathscr{L}_{\mathfrak{l}_2}[\mathscr{L}_{\mathfrak{l}_1}(\Lambda)].$$

Proof. For any $\Gamma_1 \in \mathscr{L}_{\mathfrak{l}_1}(\Lambda)$ and $\Gamma_2 \in \mathscr{L}_{\mathfrak{l}_2}(\Lambda)$, we have that $\mathfrak{l}_2\Gamma_1 + \mathfrak{l}_1\Gamma_2 \in \mathscr{L}_{\mathfrak{l}_2}(\Gamma_1)$ and $\mathfrak{l}_2\Gamma_1 + \mathfrak{l}_1\Gamma_2 \in \mathscr{L}_{\mathfrak{l}_1}(\Gamma_2)$. This proposition is thus a consequence of Lemma 5.53. □

Remark 5.55. When ℓ splits in K^+, $\mathscr{L}^+(\Lambda)$ is then of size $\ell^2+2\ell+1$, and the $\ell^3-\ell$ other (ℓ,ℓ)-neighbors have real order $\mathfrak{o}_1$.

The ramified case. Suppose that ℓ ramifies in K^+ as $\ell\mathcal{O}_{K^+} = \mathfrak{l}^2$. Then, the quotient $\mathfrak{o}_{K^+}/\ell\mathfrak{o}_{K^+}$ is isomorphic to $\mathbf{F}_\ell[\epsilon]$ with $\epsilon^2 = 0$. The orders in K_ℓ with maximal real multiplication are exactly the orders $\mathfrak{o}_{\mathfrak{l}^n} = \mathfrak{o}_{K^+} + \mathfrak{l}^n\mathfrak{o}_K$, with $n \geq 0$.

Proposition 5.56. *Suppose Λ has maximal real multiplication. If ℓ splits in K^+ as $\ell\mathfrak{o}_{K^+} = \mathfrak{l}^2$, the set of (ℓ,ℓ)-neighbors of Λ with maximal real multiplication is*

$$\mathscr{L}^+(\Lambda) = \mathscr{L}_\mathfrak{l}[\mathscr{L}_\mathfrak{l}(\Lambda)].$$

Proof. Let $\Gamma \in \mathscr{L}^+(\Lambda)$. First, if $\Gamma = \mathfrak{l}\Lambda$, observe that for any $\Pi \in \mathscr{L}_\mathfrak{l}(\Lambda)$, we have $\mathfrak{l}\Lambda \in \mathscr{L}_\mathfrak{l}(\Lambda)$, and therefore $\Gamma \in \mathscr{L}_\mathfrak{l}[\mathscr{L}_\mathfrak{l}(\Lambda)]$. We can now safely suppose $\Gamma \neq \mathfrak{l}\Lambda$. Let $\Pi = \Gamma + \mathfrak{l}\Lambda$. We have the sequence of inclusions

$$\ell\Lambda \subset \mathfrak{l}\Pi \subset \Gamma \subsetneq \Pi \subset \Lambda.$$

By contradiction, suppose $\Pi = \Lambda$. Then, $\Gamma \cap \mathfrak{l}\Lambda = \ell\Lambda$. Since $\mathfrak{l}\Gamma \subset \Gamma \cap \mathfrak{l}\Lambda = \ell\Lambda$, it follows that $\mathfrak{l}\Lambda = \mathfrak{l}\Pi = \mathfrak{l}\Gamma + \ell\Lambda \subset \ell\Lambda$, a contradiction. Therefore $\Gamma \subsetneq \Pi \subsetneq \Lambda$, and each inclusion must be of index ℓ. Then, $\Gamma \in \mathscr{L}_\mathfrak{l}(\Pi) \subset \mathscr{L}_\mathfrak{l}[\mathscr{L}_\mathfrak{l}(\Lambda)]$.

Let us now prove that $\mathscr{L}_\mathfrak{l}[\mathscr{L}_\mathfrak{l}(\Lambda)] \subset \mathscr{L}^+(\Lambda)$. Let $\Pi \in \mathscr{L}_\mathfrak{l}(\Lambda)$ and $\Gamma \in \mathscr{L}_\mathfrak{l}(\Pi)$. We have the sequence of inclusions

$$\ell\Lambda = \mathfrak{l}(\mathfrak{l}\Lambda) \subset_\ell \mathfrak{l}\Pi \subset_\ell \Gamma \subset_\ell \Pi \subset_\ell \Lambda,$$

where $\subset_\ell$ means that the first lattice is of index ℓ in the second. Therefore $\ell\Lambda \subset \Gamma \subset \Lambda$, and $\Gamma/\ell\Lambda$ is of dimension 2 over $\mathbf{F}_\ell$. Since $\Gamma/\mathfrak{l}\Lambda$ is a line, there is an element $\pi \in \Pi$ such that $\Pi = \mathbf{Z}_\ell\pi + \mathfrak{l}\Lambda$. Similarly, $\Pi/\mathfrak{l}\Gamma$ is a line, so there is an element $\gamma \in \Gamma$ such that $\Gamma = \mathbf{Z}_\ell\gamma + \mathfrak{l}\pi + \ell\Lambda$. Therefore, writing $x = \gamma + \ell\Lambda$ and $y = \pi + \ell\Lambda$, the quotient $\Gamma/\ell\Lambda$ is generated as an $\mathbf{F}_\ell$-vector space by x and ϵy. Since $\gamma \in \Gamma \subset \Pi = \mathbf{Z}_\ell\pi + \mathfrak{l}\Lambda$, there exist $a \in \mathbf{Z}_\ell$ and $z \in \Lambda/\ell\Lambda$ such that $x = ay + \epsilon z$. Then,

$$\langle x, \epsilon y\rangle_\ell = \langle ay, \epsilon y\rangle_\ell + \langle \epsilon z, \epsilon y\rangle_\ell = a\langle y, \epsilon y\rangle_\ell + \langle z, \epsilon^2 y\rangle_\ell = 0,$$

where the last equality uses Lemma 5.46, and the fact that $\epsilon^2 = 0$. So $\Gamma/\ell\Lambda$ is maximal isotropic, and $\Gamma \in \mathscr{L}(\Lambda)$. Furthermore $\epsilon x = a\epsilon y$, and $\epsilon y = 0$ are both in $\Gamma/\ell\Lambda$, so the latter is $\mathbf{F}_\ell[\epsilon]$-stable, so Γ is $\mathfrak{o}_{K^+}$-stable. This proves that $\Gamma \in \mathscr{L}^+(\Lambda)$. □

Remark 5.57. For any two distinct lattices $\Pi_1, \Pi_2 \in \mathscr{L}_\mathfrak{l}(\Lambda)$, we have a non-empty intersection $\mathscr{L}_\mathfrak{l}(\Pi_1) \cap \mathscr{L}_\mathfrak{l}(\Pi_2) = \{\mathfrak{l}\Lambda\}$.

5.8.2. Locally maximal real multiplication and (ℓ,ℓ)-isogenies. Fix again a principally polarisable, absolutely simple, ordinary abelian surface $\mathscr{A}$ over $k = \mathbf{F}_q$, with endomorphism algebra K, and K^+ the maximal real subfield of K. Now suppose that $\mathscr{A}$ has locally maximal real multiplication at ℓ. Recall from Theorem 5.2 that any such locally maximal real order is of the form $\mathfrak{o}_\mathfrak{f} = \mathfrak{o}_{K^+} + \mathfrak{f}\mathfrak{o}_K$, for some $\mathfrak{o}_{K^+}$-ideal $\mathfrak{f}$. The structure of $\mathfrak{l}$-isogeny graphs as described by Theorem 5.13 can be used to describe graphs of (ℓ,ℓ)-isogenies preserving the real multiplication, via Theorem 5.37.

Proof of Theorem 5.37. This theorem is a direct consequence of Proposition 5.49 translated to the world of isogenies via Proposition 5.42. □

Remark 5.58. Note that in particular, Theorem 5.37 implies that the kernels of the (ℓ,ℓ)-isogenies $\mathscr{A} \to \mathscr{B}$ preserving the real multiplication do not depend on the choice of a polarisation ξ on $\mathscr{A}$.

To describe graphs of (ℓ,ℓ)-isogenies with maximal local real multiplication, we combine Theorem 5.13 and Theorem 5.37. To do so, the following notation is useful.

Notation 5.59. Let $\mathcal{O}$ be any order in K with locally maximal real multiplication at ℓ, whose conductor is not divisible by $\mathfrak{l}$. We denote by $\mathscr{V}_\mathfrak{l}(\mathcal{O})$ the connected graph $\mathscr{V}$ described in Theorem 5.13. If $\mathfrak{l}$ does divide the conductor of $\mathcal{O}$, let $\mathcal{O}'$ be the smallest order containing $\mathcal{O}$, whose conductor is not divisible by $\mathfrak{l}$. Then, we also write $\mathscr{V}_\mathfrak{l}(\mathcal{O})$ for the graph $\mathscr{V}_\mathfrak{l}(\mathcal{O}')$.

The inert and ramified cases. Combining Theorem 5.13 and Theorem 5.37 allows us to describe the graph of (ℓ,ℓ)-isogenies with maximal local real multiplication at ℓ. To simplify the exposition, we assume from now on that the primitive quartic CM-field K is different from $\mathbf{Q}(\zeta_5)$, but the structure for $\mathbf{Q}(\zeta_5)$ can be deduced in the same way (bearing in mind that in that case, $\mathcal{O}_{K^+}^\times$ is of index 5 in $\mathcal{O}_K^\times$). Let $\mathscr{A}$ be any principally polarisable abelian variety with order $\mathcal{O}$, with maximal real multiplication locally at ℓ. When ℓ is inert in K^+, the connected component of $\mathscr{A}$ in the (ℓ,ℓ)-isogeny graph (again, for maximal local real multiplication) is exactly the volcano $\mathscr{V}_\mathfrak{l}(\mathcal{O})$ (see Notation 5.59). When ℓ ramifies as $\mathfrak{l}^2$ in K^+, the connected component of $\mathscr{A}$ in the graph of $\mathfrak{l}$-isogenies is isomorphic to the graph $\mathscr{V}_\mathfrak{l}(\mathcal{O})$, and the graph of (ℓ,ℓ)-isogenies can be constructed from it as follows: to the same set of vertices, add an edge in the (ℓ,ℓ)-graph between $\mathscr{B}$ and $\mathscr{C}$ for each path of length 2 between $\mathscr{B}$ and $\mathscr{C}$ in the $\mathfrak{l}$-volcano; each vertex $\mathscr{B}$ has now $\ell^2+2\ell+1$ outgoing edges, while there are only $\ell^2+\ell+1$ possible kernels of RM-preserving (ℓ,ℓ)-isogenies (see Remark 5.57). This is because the edge corresponding to the canonical projection $\mathscr{B}\to\mathscr{B}/\mathscr{B}[\mathfrak{l}]$ has been accounted for $\ell+1$ times. Remove ℓ of these copies, and the result is exactly the graph of (ℓ,ℓ)-isogenies.

Example 5.60. Suppose $\ell=2$ ramifies in K^+ as $\mathfrak{l}^2$, and $\mathfrak{l}$ is principal in $\mathcal{O}_{K^+}$. Suppose further that $\mathfrak{l}$ splits in K into two prime ideals of order 4 in $\mathrm{Cl}(\mathcal{O}_K)$. Then, the first four levels of any connected component of the (ℓ,ℓ)-isogeny graph for which the largest order is $\mathcal{O}_K$ are isomorphic to the graph of Figure 5.5. The underlying $\mathfrak{l}$-isogeny volcano is represented with dotted nodes and edges. Since $\mathfrak{l}$ is principal in $\mathcal{O}_{K^+}$, it is an undirected graph, and we represent it as such. The level 0, i.e., the surface of the volcano, is the dotted cycle of length 4 at the center. The circles have order $\mathcal{O}_K$, the squares have order $\mathcal{O}_{K^+}+\mathfrak{l}\mathcal{O}_K$, the diamonds $\mathcal{O}_{K^+}+\ell\mathcal{O}_K$, and the triangles $\mathcal{O}_{K^+}+\mathfrak{l}^3\mathcal{O}_K$.

The split case. For simplicity, suppose again that the primitive quartic CM-field K is different from $\mathbf{Q}(\zeta_5)$. Let $\mathscr{A}$ be any principally polarisable abelian variety with order $\mathcal{O}$, with maximal real multiplication locally at ℓ. The situation when ℓ splits as $\mathfrak{l}_1\mathfrak{l}_2$ in K^+ (with $\mathfrak{l}_1$ and $\mathfrak{l}_2$ principal in $\mathcal{O}\cap K^+$) is a bit more delicate because the $\mathfrak{l}_1$ and $\mathfrak{l}_2$-isogeny graphs need to be carefully pasted together. Let $\mathscr{G}_{\mathfrak{l}_1,\mathfrak{l}_2}(\mathscr{A})$ be the connected component of $\mathscr{A}$ in the labelled isogeny graphs whose edges are $\mathfrak{l}_1$-isogenies (labelled $\mathfrak{l}_1$) and $\mathfrak{l}_2$-isogenies (labelled $\mathfrak{l}_2$). The graph of (ℓ,ℓ)-isogenies is the graph on the same set of vertices, such that the number of edges between two vertices $\mathscr{B}$ and $\mathscr{C}$ is exactly the number of paths of length 2 from $\mathscr{B}$ to $\mathscr{C}$, whose first edge is labelled $\mathfrak{l}_1$ and second edge is labelled $\mathfrak{l}_2$. It remains to fully understand the structure of the graph $\mathscr{G}_{\mathfrak{l}_1,\mathfrak{l}_2}(\mathscr{A})$. Similar to the cases where ℓ is inert or ramified in K^+, we would like a complete characterization of the structure of the isogeny graph, i.e., a description that is sufficient to construct an explicit model of the abstract graph.

Without loss of generality, suppose $\mathcal{O}$ is locally maximal at ℓ. Then, the endomorphism ring of any variety in $\mathscr{G}_{\mathfrak{l}_1,\mathfrak{l}_2}(\mathscr{A})$ is characterized by the conductor $\mathfrak{l}_1^m\mathfrak{l}_2^n$ at ℓ, and we denote by $\mathcal{O}_{m,n}$ the corresponding order. The graph $\mathscr{G}_{\mathfrak{l}_1,\mathfrak{l}_2}(\mathscr{A})$ only depends on the order, so we also denote it by $\mathscr{G}_{\mathfrak{l}_1,\mathfrak{l}_2}(\mathcal{O})$. For simplicity of exposition, let us assume that $\mathfrak{l}_1$ and $\mathfrak{l}_2$ are principal in $\mathcal{O}\cap K^+$, so that the $\mathfrak{l}_i$-isogeny graphs are volcanoes.

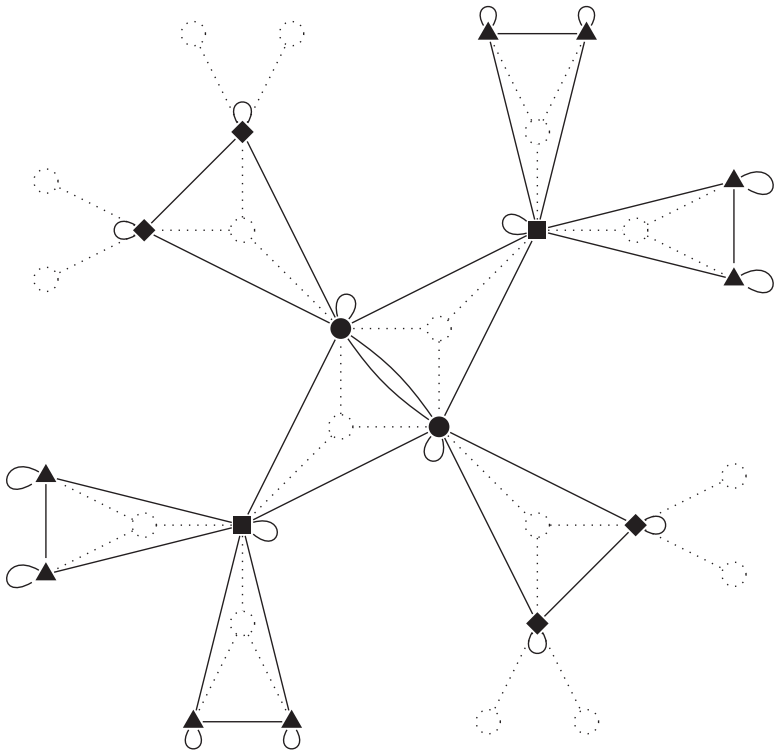


FIGURE 5.5. An example of an (ℓ, ℓ)-isogeny graph, when ℓ ramifies in K^+.

Definition 5.61 (Cyclic homomorphism)**.** Let $\mathscr{X}$ and $\mathscr{Y}$ be two graphs. A graph homomorphism $\psi : \mathscr{X} \to \mathscr{Y}$ is a *cyclic homomorphism* if each edge of $\mathscr{X}$ and $\mathscr{Y}$ can be directed in such a way that ψ becomes a homomorphism of directed graphs, and each undirected cycle in $\mathscr{X}$ becomes a directed cycle.

Lemma 5.62. *Let $\mathscr{X}$, $\mathscr{Y}$ and $\mathscr{Y}'$ be connected, d-regular graphs, with $d \leq 2$, such that $\mathscr{Y}$ and $\mathscr{Y}'$ are isomorphic. If $\varphi : \mathscr{Y} \to \mathscr{X}$ and $\varphi' : \mathscr{Y}' \to \mathscr{X}$ are two cyclic homomorphisms, there is an isomorphism $\psi : \mathscr{Y} \to \mathscr{Y}'$ such that $\varphi = \varphi' \circ \psi$.*

Proof. The statement is trivial if d is 0 or 1. Suppose $d = 2$, i.e., $\mathscr{X}$, $\mathscr{Y}$ and $\mathscr{Y}'$ are cycles. Let $\mathscr{X}$ be the cycle $x_0 - x_1 - \cdots - x_m$, with $x_m = x_0$. Similarly, $\mathscr{Y}$ is the cycle $y_0 - y_1 - \cdots - y_n$, with $y_n = y_0$. Without loss of generality, $\varphi(y_0) = x_0$ and $\varphi(y_1) = x_1$. There is a direction on the edges of $\mathscr{X}$ and $\mathscr{Y}$ such that φ becomes a homomorphism of directed graphs, and $\mathscr{Y}$ becomes a directed cycle. Without loss of generality, the direction of $\mathscr{Y}$ is given by $y_i \to y_{i+1}$. Since $y_0 \to y_1$, we have $\varphi(y_0) \to \varphi(y_1)$, hence $x_0 \to x_1$. Since $y_1 \to y_2$, we must also have $x_1 \to \varphi(y_2)$, so $\varphi(y_2) \neq x_0$ and therefore $\varphi(y_2) = x_2$, and as a consequence $x_1 \to x_2$. Repeating inductively, we obtain $x_i \to x_{i+1}$ for all $i \leq m$, and $\varphi(y_i) = x_{i \bmod m}$ for all $i \leq n$.

Similarly, any direction on $\mathscr{X}$ and $\mathscr{Y}'$ such that $\mathscr{Y}'$ is a directed cycle and φ' becomes a homomorphism of directed graphs turns $\mathscr{X}$ into a directed cycle. Without loss of generality, it is exactly the directed cycle $x_0 \to x_1 \to \cdots \to x_m$ (if it is the other direction, simply invert the directions of $\mathscr{Y}'$). There is then an enumeration $\{y'_i\}_{i=0}^n$ of $\mathscr{Y}'$ such that $\varphi'(y'_i) = x_i$, and $y'_i \to y'_{i+1}$ for each i. The isomorphism ψ is then simply given by $\psi(y_i) = y'_i$. □

Proposition 5.63. *The graph $\mathscr{G}_{\mathfrak{l}_1,\mathfrak{l}_2}(\mathcal{O})$, with edges labelled by $\mathfrak{l}_1$ and $\mathfrak{l}_2$, and bi-levelled by $(v_{\mathfrak{l}_1}, v_{\mathfrak{l}_2})$, is isomorphic to the unique (up to isomorphism) graph $\mathscr{G}$ with edges labelled by $\mathfrak{l}_1$ and $\mathfrak{l}_2$, and bi-levelled by a pair (v_1, v_2), satisfying:*

- *(i) For $i = 1, 2$, the subgraph of $\mathscr{G}$ containing only the edges labelled by $\mathfrak{l}_i$ is a disjoint union of ℓ-volcanoes, levelled by v_i;*
- *(ii) For $i \neq j$, if u and v are connected by an $\mathfrak{l}_i$-edge, then $v_j(u) = v_j(v)$;*
- *(iii) For any non-negative integers m, and n, let $\mathscr{G}_{m,n}$ be the subgraph induced by the vertices v such that $(v_1(v), v_2(v)) = (m, n)$. Then,*
  - *(i) $\mathscr{G}_{0,0}$ is isomorphic to the Cayley graph $\mathscr{C}_{0,0}$ of the subgroup of $\mathrm{Cl}(\mathcal{O})$ with generators the invertible ideals of the order $\mathcal{O}$ above ℓ, naturally labelled by $\mathfrak{l}_1$ and $\mathfrak{l}_2$;*
  - *(ii) each connected component of $\mathscr{G}_{m,n}$ is isomorphic to the Cayley graph $\mathscr{C}_{m,n}$ of the subgroup of $\mathrm{Cl}(\mathcal{O}_{m,n})$ with generators the invertible ideals of the order $\mathcal{O}_{m,n}$ above ℓ, naturally labelled by $\mathfrak{l}_1$ and $\mathfrak{l}_2$.*
- *(iv) For any two vertices u and v in $\mathscr{G}$, there is a path of the form $u \overset{\mathfrak{l}_1}{-} w \overset{\mathfrak{l}_2}{-} v$ if and only if there is a path of the form $u \overset{\mathfrak{l}_2}{-} w' \overset{\mathfrak{l}_1}{-} v$ (where $\overset{\mathfrak{l}_i}{-}$ denotes an edge labelled by $\mathfrak{l}_i$).*

Proof. First, it is not hard to see that $\mathscr{G}_{\mathfrak{l}_1,\mathfrak{l}_2}(\mathcal{O})$ satisfies all these properties. Properties (i) and (ii) follow from Proposition 5.20 and Theorem 5.13. Property (iii) follows from the free CM-action of $\mathrm{Cl}(\mathcal{O}_{m,n})$ on the corresponding isomorphism classes. Property (iv) follows from the fact that $\mathscr{A}[\mathfrak{l}_1] \oplus \mathscr{A}[\mathfrak{l}_2]$ is a direct sum.

Let $\mathscr{G}$ and $\mathscr{G}'$ be two graphs with these properties. For $i = 1, 2$, let pr_i (respectively, pr'_i) be the predecessor map induced by the volcano structure of the $\mathfrak{l}_i$-edges on $\mathscr{G}$ (respectively, on $\mathscr{G}'$). We will construct an isomorphism $\Psi : \mathscr{G} \to \mathscr{G}'$ by starting with the isomorphism between $\mathscr{G}_{0,0}$ and $\mathscr{G}'_{0,0}$ and extending it on the blocks $\mathscr{G}_{m,n}$ and $\mathscr{G}'_{m,n}$ one at a time. Let $n > 0$, and suppose, by induction, that Ψ has been defined exactly on the blocks $\mathscr{G}_{i,j}$ for $i + j < n$. Let us extend Ψ to the blocks $\mathscr{G}_{m,n-m}$ for $m = 0, \ldots, n$ in succession.

Both $\mathscr{G}_{0,n}$ and $\mathscr{G}'_{0,n}$ have the same number of vertices, and their connected components are all isomorphic $\mathscr{C}_{0,n}$, which are of degree d at most 2. We have the graph homomorphism $\mathrm{pr}_2 : \mathscr{G}_{0,n} \to \mathscr{G}_{0,n-1}$. Let S be the set of connected components of $\mathscr{G}_{0,n}$. Define the equivalence relation on S

$$A \sim B \iff \mathrm{pr}_2(A) = \mathrm{pr}_2(B).$$

Similarly define the equivalence relation $\sim'$ on the set S' of connected components of $\mathscr{G}'_{0,n}$. Observe that each equivalence class for either $\sim$ or $\sim'$ has same cardinality, so one can choose a bijection $\Theta : S \to S'$ such that for any $A \in S$, we have $\Psi(\mathrm{pr}_2(A)) = \mathrm{pr}'_2(\Theta(A))$. It is not hard to check that pr_2 and pr'_2 are cyclic homomorphisms, using Property (iv). From Lemma 5.62, for each $A \in S$, there is a graph isomorphism $\psi_A : A \to \Theta(A)$ such that for any $x \in A$, it is the case that $\mathrm{pr}'_2(\psi_A(x)) = \Psi(\mathrm{pr}_2(x))$. Let $\hat{\Psi}$ be the map extending Ψ by sending any $x \in \mathscr{G}_{0,n}$ to $\psi_A(x)$, where A is the connected component of x in $\mathscr{G}_{0,n}$. We need to show that it is a graph isomorphism. Write $\mathscr{D}$ and $\mathscr{D}'$ for the domain and codomain of Ψ. The map $\hat{\Psi}$, restricted and corestricted to $\mathscr{D}$ and $\mathscr{D}'$ is exactly Ψ, so is an isomorphism. Also, the restriction and corestriction to $\mathscr{G}_{0,n}$ and $\mathscr{G}'_{0,n}$ is an isomorphism, by construction. Only the edges between $\mathscr{G}_{0,n}$ and $\mathscr{D}$ (respectively $\mathscr{G}'_{0,n}$ and $\mathscr{D}'$) might cause trouble. The only edges between $\mathscr{G}_{0,n}$ and $\mathscr{D}$ are actually between $\mathscr{G}_{0,n}$ and $\mathscr{G}_{0,n-1}$, and are of the form $(x, \mathrm{pr}_2(x))$. But Ψ was precisely constructed so that $\Psi(\mathrm{pr}_2(x)) = \mathrm{pr}'_2(\Psi(x))$, so $\hat{\Psi}$ is indeed an isomorphism.

Now, let $0 < m < n$ and suppose that Ψ has been extended to the components $\mathscr{G}_{i,n-i}$ for each $i < m$. Let us extend it to $\mathscr{G}_{m,n-m}$. Since $m > 0$ and $n - m > 0$, the graph $\mathscr{C}_{m,n-m}$ is a single point, with no edge. Let us now prove that for any pair (x_1, x_2), where x_1 is a vertex in $\mathscr{G}_{m-1,n-m}$ and x_2 in $\mathscr{G}_{m,n-m-1}$ such that $\mathrm{pr}_2(x_1) = \mathrm{pr}_1(x_2)$, there is a unique vertex x in $\mathscr{G}_{m,n-m}$ such that $(x_1, x_2) = (\mathrm{pr}_1(x), \mathrm{pr}_2(x))$. First, we show that for any vertex $x \in \mathscr{G}_{m,n-m}$, we have

$$\mathrm{pr}_1^{-1}(\mathrm{pr}_1(x)) \cap \mathrm{pr}_2^{-1}(\mathrm{pr}_2(x)) = \{x\}.$$

Let $z = \mathrm{pr}_1(\mathrm{pr}_2(x))$. Let $X = \mathrm{pr}_1^{-1}(\mathrm{pr}_1(x))$ and $Y = \mathrm{pr}_1^{-1}(z)$. From Property (ii), z and $\mathrm{pr}_1(x)$ are at the same v_1-level, so from Property (i), we have $|X| = |Y|$. For any $y \in Y$, we have $\mathrm{pr}_1(x) \overset{\mathfrak{l}_2}{-} z \overset{\mathfrak{l}_1}{-} y$, so there is a vertex x' such that $\mathrm{pr}_1(x) \overset{\mathfrak{l}_1}{-} x' \overset{\mathfrak{l}_2}{-} y$. Then, $v_1(x') = v_1(y) = v_1(\mathrm{pr}_1(x)) - 1$, and therefore $x' \in X$. This implies that pr_2 induces a surjection $\widetilde{\mathrm{pr}}_2 : X \to Y$ (this is pr_2 restricted to X and corestricted to Y), which is a bijection since $|X| = |Y|$. So

$$X \cap \mathrm{pr}_2^{-1}(\mathrm{pr}_2(x)) = X \cap \widetilde{\mathrm{pr}}_2^{-1}(\mathrm{pr}_2(x)) = \{x\}.$$

Now, an elementary counting argument shows that $x \mapsto (\mathrm{pr}_1(x), \mathrm{pr}_2(x))$ is a bijection between the vertices of $\mathscr{G}_{m,n-m}$ and the pairs (x_1, x_2), where x_1 is a vertex in $\mathscr{G}_{m-1,n-m}$ and x_2 in $\mathscr{G}_{m,n-m-1}$ such that $\mathrm{pr}_2(x_1) = \mathrm{pr}_1(x_2)$. This property also holds in $\mathscr{G}'$, and we can thereby define $\psi : \mathscr{G}_{m,n-m} \to \mathscr{G}'_{m,n-m}$ as the bijection sending any vertex x in $\mathscr{G}_{m,n-m}$ to the unique vertex x' in $\mathscr{G}'_{m,n-m}$ such that

$$(\mathrm{pr}'_1(x'), \mathrm{pr}'_2(x')) = (\Psi(\mathrm{pr}_1(x)), \Psi(\mathrm{pr}_2(x))).$$

It is then easy to check that the extension of Ψ induced by ψ is an isomorphism. The final step, extending on $\mathscr{G}_{n,0}$, is similar to the case of $\mathscr{G}_{0,n}$. This concludes the induction, and proves that $\mathscr{G}$ and $\mathscr{G}'$ are isomorphic. □

5.9. Applications to "going up" algorithms

5.9.1. Motivation for a "going up" algorithm. Although our Theorem 5.36 does not determine the global structure of the graph of (ℓ, ℓ)-isogenies, it is enough to prove our final result: a "going up" algorithm. This algorithm, given as input a principally polarised abelian surface, finds a path of computable isogenies leading to an abelian surface with maximal endomorphism ring, when this is possible.

A first application of the "going up" algorithm is in generating (hyperelliptic) curves of genus 2 over finite fields with suitable security parameters via the CM method. The method is based on first computing invariants for the curve (Igusa invariants) and then using a method of Mestre [Mes91] (see also [CQ05]) to construct the equation of the curve. There are three different ways to compute the minimal polynomials of these invariants (the Igusa class polynomials):

(1) Complex analytic techniques [vW99, Wen03, Str10, ET14];
(2) p-adic lifting techniques [CKL08, GHK$^+$06];
(3) A technique based on the Chinese remainder theorem [EL10, FL08, BGL11] (the *CRT method*).

Although 3), which requires a "going up" algorithm, is currently the least efficient method, it is also the least understood and deserves more attention: its analogue for elliptic curves holds the records for time and space complexity and for the size of the computed examples [ES10, Sut11]. The work of [LR12a] aims at generalising (to genus 2) the method of Sutherland [Sut11] for elliptic curves. Based on (ℓ, ℓ)-isogenies that do not require the endomorphism ring to be maximal, it yields a probabilistic algorithm for

"going up" to an abelian surface with maximal endomorphism ring, and, although the authors cannot prove that the "going up" algorithm succeeds with any fixed probability, the improvement is practical and, heuristically, it significantly reduces the running time of the previous results (the CRT method of [BGL11]) in genus 2.

Our Algorithm 5.1 answers a question of [LR12a] by providing a deterministic method and removing the heuristics from the complexity analysis.

A second application is in the computation of an explicit isogeny between any two given principally polarised abelian surfaces in the same isogeny class. We explored in Chapter 3 how to find an isogeny between two such surfaces with the same endomorphism ring. This can be extended to other pairs of isogenous principally polarised abelian surfaces, by first computing paths of isogenies to reach the maximal endomorphism ring, then applying the method of Section 3.7.

Similarly, the "going up" algorithm can also extend results about the random self-reducibility of the discrete logarithm problem in genus 2 cryptography. The results of Chapter 3 imply that if the discrete logarithm problem is efficiently solvable on a non-negligible proportion of the Jacobians with maximal endomorphism ring within an isogeny class, then it is efficiently solvable for all isogenous Jacobians with maximal endomorphism ring. For this to hold on any other Jacobian in the isogeny class, it only remains to compute a path of isogenies reaching the level of the maximal endomorphism ring.

5.9.2. Largest reachable orders. The results from Section 5.7.3 and Section 5.8.2 on the structure of the graph of (ℓ,ℓ)-isogenies allow us to determine exactly when there exists a sequence of (ℓ,ℓ)-isogenies leading to a surface with maximal local order at ℓ. When there is no such path, one can still determine the largest reachable orders. Recall the notation $\mathfrak{o}_{\mathfrak{f}} = \mathfrak{o}_{K^+} + \mathfrak{f}\mathfrak{o}_K$ where $\mathfrak{f}$ is an ideal of $\mathfrak{o}_{K^+}$.

Proposition 5.64. *Suppose $\mathscr{A}$ has maximal local real order, and $\mathfrak{o}(\mathscr{A}) = \mathfrak{o}_{\mathfrak{f}}$.*

(i) If ℓ divides $\mathfrak{f}$, there is a unique (ℓ,ℓ)-isogeny to a surface with order $\mathfrak{o}_{\ell^{-1}\mathfrak{f}}$.

(ii) If ℓ ramifies in K^+ as $\mathfrak{l}^2$ and $\mathfrak{f} = \mathfrak{l}$, then there exists an (ℓ,ℓ)-isogeny to a surface with maximal local order if and only if $\mathfrak{l}$ is not inert in K. It is unique if $\mathfrak{l}$ is ramified, and there are two if it splits.

(iii) If ℓ splits in K^+ as $\mathfrak{l}_1\mathfrak{l}_2$, and $\mathfrak{f} = \mathfrak{l}_1^i$ for some $i > 0$, then there exists an (ℓ,ℓ)-isogeny to a surface with local order $\mathfrak{o}_{\mathfrak{l}_1^{i-1}}$ if and only if $\mathfrak{l}_2$ is not inert in K. It is unique if $\mathfrak{l}_2$ is ramified, and there are two if it splits. Also, there always exists an (ℓ,ℓ)-isogeny to a surface with local order $\mathfrak{o}_{\mathfrak{l}_1^{i-1}\mathfrak{l}_2}$.

Proof. This is a straightforward case-by-case analysis of Proposition 5.20 and Theorem 5.37. □

Definition 5.65 (Parity of $\mathscr{A}$)**.** Suppose $\mathscr{A}$ has real order $\mathfrak{o}^+(\mathscr{A}) = \mathbf{Z}_\ell + \ell^n\mathfrak{o}_{K^+}$. Construct an isogenous $\mathscr{B}$ by taking the RM-predecessor n times starting from $\mathscr{A}$, i.e., $\mathscr{B} = \mathrm{pr}(\mathrm{pr}(\ldots \mathrm{pr}(\mathscr{A})\ldots))$ is the (iterated) RM-predecessor of $\mathscr{A}$ that has maximal real local order. Let $\mathfrak{f}$ be the conductor of $\mathfrak{o}(\mathscr{B})$. The *parity* of $\mathscr{A}$ is 0 if $N(\mathfrak{f} \cap \mathfrak{o}_{K^+})$ is a square, and 1 otherwise.

Remark 5.66. The parity is always 0 if ℓ is inert in K^+.

Theorem 5.67. *For any $\mathscr{A}$, there exists a sequence of (ℓ,ℓ)-isogenies starting from $\mathscr{A}$ and ending at a variety with maximal local order, except in the following two cases:*

(i) $\mathscr{A}$ has parity 1, the prime ℓ splits in K^+ as $\mathfrak{l}_1\mathfrak{l}_2$, and both $\mathfrak{l}_1$ and $\mathfrak{l}_2$ are inert in K, in which case the largest reachable local orders are $\mathfrak{o}_{K^+} + \mathfrak{l}_1\mathfrak{o}_K$ and $\mathfrak{o}_{K^+} + \mathfrak{l}_2\mathfrak{o}_K$;

(ii) $\mathscr{A}$ has parity 1, the prime ℓ ramifies in K^+ as $\mathfrak{l}^2$, and $\mathfrak{l}$ is inert in K, in which case the largest reachable local order is $\mathfrak{o}_{K^+} + \mathfrak{l}\mathfrak{o}_K$.

Proof. First, from Propositon 5.48, there is a sequence of (ℓ,ℓ)-isogenies starting from $\mathscr{A}$ and ending at a variety with maximal local order if and only if there is such a path that starts by a sequence of isogenies up to $\mathscr{B} = \mathrm{pr}(\mathrm{pr}(\dots \mathrm{pr}(\mathscr{A})\dots))$, and then only consists of (ℓ,ℓ)-isogenies preserving the maximality of the local real order. It is therefore sufficient to look at sequences of RM-preserving (ℓ,ℓ)-isogenies from $\mathscr{B}$, which has by construction the same parity s as $\mathscr{A}$.

From Proposition 5.64, there is a path from $\mathscr{B}$ to a surface $\mathscr{C}$ with local order $\mathfrak{o}(\mathscr{C}) = \mathfrak{o}_{\mathfrak{l}^s}$ where $\mathfrak{l}$ is a prime ideal of $\mathfrak{o}_{K^+}$ above ℓ, and s is the parity of $\mathscr{A}$. We are done if the parity is 0. Suppose the parity is 1. From Propositions 5.20 and Theorem 5.37, one can see that there exists a sequence of RM-preserving (ℓ,ℓ)-isogenies from $\mathscr{C}$ which changes the parity to 0 if and only if ℓ ramifies in K^+ as $\mathfrak{l}^2$ and $\mathfrak{l}$ is not inert in K, or ℓ splits in K^+ as $\mathfrak{l}_1\mathfrak{l}_2$ and either $\mathfrak{l}_1$ or $\mathfrak{l}_2$ is not inert in K. This concludes the proof. □

5.9.3. A "going up" algorithm. In many applications (in particular, the CM method in genus 2 based on the CRT) it is useful to find a chain of isogenies to a principally polarised abelian surface with maximal endomorphism ring starting from any curve whose Jacobian is in the given isogeny class. Lauter and Robert [LR12a, Section 5] propose a probabilistic algorithm to construct a principally polarised abelian variety whose endomorphism ring is maximal. That algorithm is heuristic, and the probability of failure is difficult to analyse. We now apply our structural results from Subsection 5.8.2 to some of their ideas to give a provable algorithm.

5.9.3.1. *Prior work of Lauter–Robert.* Given a prime ℓ for which we would like to find an isogenous abelian surface over $k = \mathbf{F}_q$ with maximal local endomorphism ring at ℓ, suppose that $\alpha = \ell^e\alpha'$ for some $\alpha' \in \mathcal{O}_K$ and some $e > 0$. To find a surface $\mathscr{A}'/k$ for which $\alpha/\ell^e \in \mathrm{End}(\mathscr{A}')$, Lauter and Robert [LR12a, Section 5] use (ℓ,ℓ)-isogenies and a way to test whether $\alpha/\ell^e \in \mathrm{End}(\mathscr{A}')$. In fact, $\alpha/\ell^e \in \mathrm{End}(\mathscr{A}')$ is equivalent to testing that $\alpha(\mathscr{A}'[\ell^e]) = 0$, i.e., α is trivial on the ℓ^e-torsion of $\mathscr{A}$. To guarantee that, one defines an "obstruction" $N_e = \#\alpha(\mathscr{A}[\ell^e])$ that measures the failure of α/ℓ^e to be an endomorphism of $\mathscr{A}'$. To construct an abelian surface that contains the element α/ℓ^e as endomorphism, one uses (ℓ,ℓ)-isogenies iteratively in order to decrease the associated obstruction N_e (this is in essence the idea of [LR12a, Algorithm 21]).

To reach an abelian surface with maximal local endomorphism ring at ℓ, Lauter and Robert look at the structure of $\mathrm{End}(\mathscr{A}) \otimes_{\mathbf{Z}} \mathbf{Z}_\ell$ as a $\mathbf{Z}_\ell$-module and define an obstruction via a particular choice of a $\mathbf{Z}_\ell$-basis [LR12a, Algorithm 23].

5.9.3.2. *Refined obstructions and provable algorithm.* Theorem 5.67 above gives a provable "going up" algorithm that runs in three main steps: 1) it uses (ℓ,ℓ)-isogenies to reach a surface with maximal local real endomorphism ring at ℓ; 2) it reaches the largest possible order via (ℓ,ℓ)-isogenies as in Theorem 5.67; 3) if needed, it makes a last step to reach the maximal local endomorphism ring via a cyclic isogeny. To implement 1) and 2), one uses refined obstructions, which we now describe in detail.

5.9.3.3. *"Going up" to maximal real multiplication.* Considering the local orders $\mathfrak{o}_{K^+} = \mathcal{O}_{K^+} \otimes_{\mathbf{Z}} \mathbf{Z}_\ell$ and $\mathbf{Z}_\ell[\pi + \pi^\dagger]$, choose a $\mathbf{Z}_\ell$-basis $\{1, \beta/\ell^e\}$ for $\mathfrak{o}_{K^+}$ such that $\beta \in \mathbf{Z}[\pi + \pi^\dagger]$ and apply a "real-multiplication" modification of [LR12a, Algorithm 21] to β. Thus, given an abelian surface $\mathscr{A}$ with endomorphism algebra isomorphic to K, define the

obstruction for $\mathscr{A}$ to have maximal real multiplication at ℓ as

$$N^+(\mathscr{A}) = e - \max\{\epsilon\colon \beta(\mathscr{A}[\ell^\epsilon]) = 0\}.$$

Clearly, $\mathscr{A}$ will have maximal real endomorphism ring at ℓ if and only if $N^+(\mathscr{A}) = 0$. The following simple lemma characterizes the obstruction:

Lemma 5.68. *The obstruction $N^+(\mathscr{A})$ is equal to the valuation at ℓ of the conductor of the real multiplication $\mathcal{O}^+(\mathscr{A}) \subset \mathcal{O}_{K^+}$.*

Proof. Using the definition of $N^+(\mathscr{A})$ and the fact that $\beta/\ell^\epsilon \in \mathcal{O}(\mathscr{A})$ if and only if $\beta(\mathscr{A}[\ell^\epsilon]) = 0$, it follows that

$$\mathbf{Z}_\ell + \beta/\ell^{e-N^+(\mathscr{A})}\mathbf{Z}_\ell \subseteq \mathfrak{o}^+(\mathscr{A}) \subsetneq \mathbf{Z}_\ell + \beta/\ell^{e-N^+(\mathscr{A})+1}\mathbf{Z}_\ell.$$

Since all orders of $\mathcal{O}_{K^+}$ are of the form $\mathbf{Z} + c\mathcal{O}_{K^+}$ for some $c \in \mathbf{Z}_{>0}$, by localisation at ℓ one sees that

$$\mathfrak{o}^+(\mathscr{A}) = \mathbf{Z}_\ell + \beta/\ell^{e-N^+(\mathscr{A})}\mathbf{Z}_\ell = \mathbf{Z}_\ell + \ell^{N^+(\mathscr{A})}\mathfrak{o}_{K^+},$$

i.e., the valuation at ℓ of the conductor of $\mathcal{O}^+(\mathscr{A})$ is $N^+(\mathscr{A})$. □

The lemma proves that the following algorithm works (i.e., that there always exists a neighbor decreasing the obstruction N^+):

Algorithm 5.1 Going up to the maximal real endomorphism ring

Require: An abelian surface $\mathscr{A}/k$ with endomorphism algebra $K = \mathrm{End}(\mathscr{A}) \otimes \mathbf{Q}$, and a prime number ℓ.
Ensure: An isogenous abelian surface $\mathscr{A}'/k$ with $\mathfrak{o}^+(\mathscr{A}') = \mathfrak{o}_{K^+}$.
1: $\beta \leftarrow$ an element $\beta \in \mathbf{Z}[\pi + \overline{\pi}]$ such that $\{1, \beta/\ell^e\}$ is a $\mathbf{Z}_\ell$-basis for $\mathfrak{o}_{K^+}$.
2: Compute $N^+(\mathscr{A}) = e - \max\{\epsilon\colon \beta(\mathscr{A}[\ell^\epsilon]) = 0\}$
3: **if** $N^+(\mathscr{A}) = 0$ **then**
4: **return** $\mathscr{A}$
5: **end if**
6: $\mathcal{L} \leftarrow$ list of maximal isotropic $\kappa \subset \mathscr{A}[\ell]$ with $\kappa \cap \beta(\mathscr{A}[\ell^{e-N^+(\mathscr{A})+1}]) \neq \emptyset$
7: **for** $\kappa \in \mathcal{L}$ **do**
8: Compute $N^+(\mathscr{A}/\kappa) = e - \max\{\epsilon\colon \beta((A/\kappa)[\ell^\epsilon]) = 0\}$
9: **if** $N^+(\mathscr{A}/\kappa, \epsilon) < N^+(\mathscr{A}, \epsilon)$ **then**
10: $\mathscr{A} \leftarrow \mathscr{A}/\kappa$ and **go to** Step 3
11: **end if**
12: **end for**

5.9.3.4. *Almost maximal order with (ℓ, ℓ)-isogenies.* For each prime ℓ, use the "going up" algorithm (Algorithm 5.1), until $\mathcal{O}^+(\mathscr{A}) = \mathcal{O}_{K^+}$. Let ℓ be any prime and let $\mathfrak{l} \subset \mathcal{O}_{K^+}$ be a prime ideal above ℓ. Let $\mathfrak{o}_{+,\mathfrak{l}} = \mathcal{O}_{K^+,\mathfrak{l}}$ be the completion at $\mathfrak{l}$ of $\mathcal{O}_{K^+}$. Consider the suborder $\mathfrak{o}_{+,\mathfrak{l}}[\pi + \pi^\dagger]$ of the maximal local (at $\mathfrak{l}$) order $\mathcal{O}_K \otimes_{\mathcal{O}_{K^+}} \mathfrak{o}_{+,\mathfrak{l}}$. Now write

$$\mathfrak{o}_{+,\mathfrak{l}}[\pi + \pi^\dagger] = \mathfrak{o}_{+,\mathfrak{l}} + \gamma\mathfrak{o}_{+,\mathfrak{l}}, \text{ and}$$
$$\mathcal{O}_K \otimes_{\mathcal{O}_{K^+}} \mathfrak{o}_{+,\mathfrak{l}} = \mathfrak{o}_{+,\mathfrak{l}} + \gamma/\varpi^{f_\mathfrak{l}}\mathfrak{o}_{+,\mathfrak{l}},$$

for some endomorphism γ. Here, ϖ is a uniformiser for the local order $\mathfrak{o}_{+,\mathfrak{l}}$ and $f_\mathfrak{l} \geq 0$ is some integer. To define a similar obstruction to $N^+(\mathscr{A}, \epsilon)$, but at $\mathfrak{l}$, let

$$N_\mathfrak{l}(\mathscr{A}) = f_\mathfrak{l} - \max\{\delta\colon \gamma(\mathscr{A}[\mathfrak{l}^\delta]) = 0\}.$$

To compute these obstructions, we compute γ on the $\mathfrak{l}$-power torsion of $\mathscr{A}$. The idea is similar to Algorithm 5.1, except that in the split case, one must test the obstructions $N_{\mathfrak{l}}(\mathscr{A}, \epsilon)$ for both prime ideals $\mathfrak{l} \subset \mathcal{O}_{K^+}$ above ℓ at the same time. We now show that one can reach the maximal possible "reachable" (in the sense of Theorem 5.67) local order at ℓ starting from $\mathscr{A}$ and using only (ℓ, ℓ)-isogenies. When ℓ is either inert or ramified in K^+, there is only one obstruction $N_{\mathfrak{l}}(\mathscr{A})$, and one can ensure that it decreases at each step via the obvious modification of Algorithm 5.1.

Suppose now that $\ell\mathcal{O}_{K^+} = \mathfrak{l}_1\mathfrak{l}_2$ is split. Let $\mathfrak{f} = \mathfrak{l}_1^{i_1}\mathfrak{l}_2^{i_2}$ be the conductor of $\mathscr{A}$ and suppose, without loss of generality, that $i_1 \geq i_2$. To first ensure that one can reach an abelian surface $\mathscr{A}$ for which $0 \leq i_1 - i_2 \leq 1$, we relate the conductor $\mathfrak{f}$ to the two obstructions at $\mathfrak{l}_1$ and $\mathfrak{l}_2$.

Lemma 5.69. *Let $\mathscr{A}$ be an abelian surface with maximal local real endomorphism ring at ℓ and let $\mathfrak{o}(\mathscr{A}) = \mathfrak{o}_{K^+} + \mathfrak{f}\mathfrak{o}_K$ where $\mathfrak{f}$ is the conductor. Then*

$$v_{\mathfrak{l}_1}(\mathfrak{f}) = N_{\mathfrak{l}_1}(\mathscr{A}) \qquad \text{and} \qquad v_{\mathfrak{l}_2}(\mathfrak{f}) = N_{\mathfrak{l}_2}(\mathscr{A}).$$

Proof. The proof is the same as the one of Lemma 5.68. □

Using the lemma, and assuming $N_{\mathfrak{l}_1}(\mathscr{A}) - N_{\mathfrak{l}_2}(\mathscr{A}) > 1$, one repeatedly looks for an (ℓ, ℓ)-isogeny at each step that will decrease $N_{\mathfrak{l}_1}(\mathscr{A})$ by 1 and increase $N_{\mathfrak{l}_2}(\mathscr{A})$ by 1. Such an isogeny exists by Proposition 5.64(iii). One repeats this process until

$$0 \leq N_{\mathfrak{l}_1}(\mathscr{A}) - N_{\mathfrak{l}_2}(\mathscr{A}) \leq 1.$$

If at this stage $N_{\mathfrak{l}_2}(\mathscr{A}) > 0$, this means that $\ell \mid \mathfrak{f}$ and hence, by Proposition 5.64(i), there exists a unique (ℓ, ℓ)-isogeny decreasing both obstructions. One searches for that (ℓ, ℓ)-isogeny by testing whether the two obstructions decrease simultaneously, and repeats until $N_{\mathfrak{l}_2}(\mathscr{A}) = 0$.

If $N_{\mathfrak{l}_1}(\mathscr{A}) = 0$, then the maximal local order at ℓ has been reached. If $N_{\mathfrak{l}_1}(\mathscr{A}) = 1$ then Proposition 5.64(iii) implies that, if $\mathfrak{l}_2$ is not inert in K, then there exists an (ℓ, ℓ)-isogeny that decreases $N_{\mathfrak{l}_1}(\mathscr{A})$ to 0 and keeps $N_{\mathfrak{l}_2}(\mathscr{A})$ at zero.

5.9.3.5. *Final step via a cyclic isogeny.* In the exceptional cases of Theorem 5.67, it may happen that one needs to do an extra step via a cyclic isogeny to reach the maximal local endomorphism ring at ℓ. Whenever this cyclic $\mathfrak{l}$-isogeny is computable via the DJRV algorithm, one can always reach maximal local endomorphism ring at ℓ. But $\mathfrak{l}$-isogenies are computable if and only if $\mathfrak{l}$ is trivial in the narrow class group of K^+. We thus distinguish the following two cases:

(1) If $\mathfrak{l}$-isogenies are computable by the DJRV algorithm then one can always reach maximal local endomorphism ring at ℓ.
(2) If $\mathfrak{l}$-isogenies are not computable by the DJRV algorithm, one can only use (ℓ, ℓ)-isogenies, so Theorem 5.67 tells us what the largest order that we can reach is.

PART III

IDEAL LATTICES IN CYCLOTOMIC FIELDS

6

Finding short generators of principal ideals

Abstract. This chapter and the next are based on an ongoing project with Ronald Cramer and Léo Ducas, which is essentially an extension of our collaboration presented at EUROCRYPT 2017 and published as

[CDW17] R. Cramer, L. Ducas, and B. Wesolowski, *Short Stickelberger class relations and application to Ideal-SVP*, Advances in Cryptology – EUROCRYPT 2017 (J. Coron and J. B. Nielsen, eds.), Lecture Notes in Computer Science, vol. 10210, Springer, 2017, pp. 324–348.

The first part of this project, presented in this chapter, is mostly concerned with extending the results of [CDPR16], notably by providing a full proof of the numerical stability of their method to find short generators of principal ideals in cyclotomic fields, and by extending the results to cyclotomic fields of arbitrary conductor (rather than prime powers). The core of [CDW17] is the object of Chapter 7, yet relevant pieces of that article are already introduced in the present chapter.

Fix an integer $m > 2$ and a primitive m-th root of unity $\zeta_m \in \mathbf{C}$. Let $K = \mathbf{Q}(\zeta_m)$ be the cyclotomic field of conductor m. By the cyclotomic ring of conductor m, we shall mean $\mathcal{O}_K = \mathbf{Z}[\zeta_m]$, the ring of integers of K. The trace $\mathrm{Tr} : K \to \mathbf{Q}$ induces an inner product on K as $\langle a, b\rangle = \mathrm{Tr}(ab^\tau)$, where τ is complex conjugation. The field K is then a Hermitian vector space of dimension $\varphi(m)$ (where φ is Euler's totient function), and ideals in $\mathcal{O}_K$ are Euclidean lattices, which are referred to as *cyclotomic ideal lattices*. This chapter and the next explore the following question: what is the shortest vector that we can find in such a lattice, in polynomial time, given the help of a quantum computer?

The problem of finding short vectors of a Euclidean lattice (the shortest vector problem, SVP, or its approximated version, approx-SVP) is a central hard problem in complexity theory. It has become the theoretical foundation for many cryptographic constructions thanks to the average-case to worst-case reductions of Ajtai [Ajt99] and Regev [Reg09]: the resulting cryptosystems are secure as long as there *exists* a lattice where finding short vectors is hard. Instantiations of these problems over ideal lattices have attracted particular attention, as they allow very efficient implementations, and much smaller keys than generic lattices. The Ring-SIS [Mic07, LM06, PR06] and Ring-LWE [SSTX09, LPR13] problems were introduced, and shown to be at least as hard as worst-case instances of Ideal-SVP (the specialisation of approx-SVP to ideal lattices). Both problems Ring-SIS and Ring-LWE have shown very versatile problems for

building efficient cryptographic schemes. Typically, Ring-SIS, Ring-LWE and Ideal-SVP are instantiated over cyclotomic rings — a choice which further ensures the hardness of the decisional version of Ring-LWE under the same worst-case Ideal-SVP hardness assumption [LPR13].

For some time, it seemed plausible that the ideal versions of lattice problems should be just as hard to solve as the unstructured ones: only some (almost) linear-time advantages were known. This was challenged by a series of works, initiated by Campbell *et al.* [CGS14], and followed by [BS16] and [CDPR16]. They show that in a cyclotomic ring of prime-power conductor, given a principal ideal that is guaranteed to have a "very short" generator, one can retrieve such a "very short" generator in quantum polynomial time. As a consequence, some cryptographic schemes were broken, but it had a very limited impact on the more general Ideal-SVP since ideals with a "very short" generator are rare. A step towards the general case is already taken in [CDPR16]: they show that, still in a cyclotomic ring of prime-power conductor, one can find a short generator of any given principal ideal in quantum polynomial time. While not "very short", this generator does provide an unexpectedly good approximation of the shortest vector of the ideal.

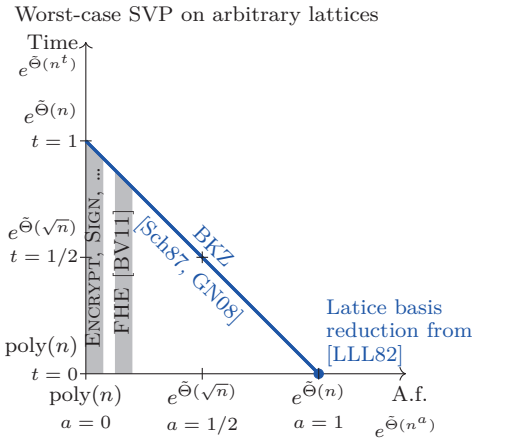
In this chapter and the next, we are interested in the general case of Ideal-SVP, for arbitrary ideal lattices in any cyclotomic ring. Studying the geometry of units and ideals of cyclotomic rings, we devise a quantum algorithm that given an ideal lattice of the cyclotomic ring of conductor m, finds an approximation of the shortest vector by a factor $\exp(\tilde{O}(\sqrt{m}))$. Under some plausible (and carefully justified) number-theoretic assumptions, the algorithm runs in polynomial time. This is the main result of this part of the manuscript, formalised as Theorem 7.10. In contrast, the best known polynomial time generic lattice algorithms can only reach an approximation factor $\exp(\tilde{O}(m))$. This unexpected hardness gap between approx-SVP in generic lattices and in cyclotomic ideal lattices is illustrated in Figure 6.1.

To the best of our knowledge, this result does not immediately lead to an attack on any proposed scheme based on Ring-LWE, for two reasons. First, the approximation factor $\gamma = \exp(\tilde{O}(\sqrt{m}))$ in the worst-case is asymptotically too large to affect any actual Ring-LWE based schemes even for advanced cryptosystems such as the state of the art fully homomorphic encryption schemes (see [BV11, DM15]). Second, Ring-LWE is known to be at least as hard as Ideal-SVP but not known to be equivalent.

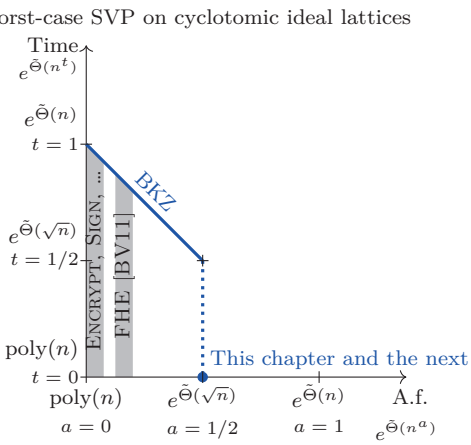
Despite those two serious obstacles, it seems a reasonable precaution to consider weaker structured lattice assumptions, such as Module-LWE [LS15] (i.e., an "unusually-Short Vector Problem" in a module of larger rank over a smaller ring), which provides an intermediate problem between Ring-LWE and general LWE.

Approx-SVP for principal ideals. Our method is divided into two main steps. First, in this chapter, we show how to find a short vector in the case where the ideal is principal; then, in the next chapter, we show how to reduce the general case to the principal case.

The principal case is dealt with via a study of the geometry of cyclotomic units. The methods involved were introduced in [CDPR16], and we extend their results by providing a full analysis of the numerical stability, and generalising the methods to cyclotomic fields of arbitrary conductor. Let $\mathfrak{a}$ be a principal ideal in $\mathcal{O}_K$. The idea is to find a short *generator* of $\mathfrak{a}$ (rather than just a short element). First, the algorithms of [BS16] allow to find an arbitrary generator g of $\mathfrak{a}$ in quantum polynomial time. Then, $g\mathcal{O}_K^\times$ is the set of all generators of $\mathfrak{a}$. We are looking for a short element of $g\mathcal{O}_K^\times$. The logarithmic embedding (see Definition 6.10) allows to transform this into a lattice problem: the



In the general case, the best known algorithms (BKZ [Sch87] and Slide [GN08]) run in time $\exp(\tilde{\Theta}(n^t))$ for an approximation factor $\exp(\tilde{\Theta}(n^a))$, where $t + a = 1$.



For ideal lattices of cyclotomic fields, the results of the present chapter and the next give a quantum polynomial runtime (i.e., $t = 0$) for any $a \geq 1/2$.

FIGURE 6.1. Best known (quantum) time–approximation factor tradeoffs to solve approx-SVP in arbitrary lattices (on the left) and in cyclotomic ideal lattices (on the right), in the worst case. The integer n is the dimension of the lattice; for a cyclotomic field of conductor m, this dimension is $n = \varphi(m)$. The approximation factors upon which the security of cryptographic schemes relies are typically between polynomial poly(n) and quasi-polynomial $\exp(\text{polylog}(n))$ (represented as the grey area).

image $\text{Log}(\mathcal{O}_K^\times)$ is a lattice of dimension $\varphi(m) - 1$, and the logarithmic embedding of $g\mathcal{O}_K^\times$ is the translation

$$\text{Log}(g) + \text{Log}(\mathcal{O}_K^\times)$$

of this lattice. We exhibit a full-rank set of short elements in $\text{Log}(\mathcal{O}_K^\times)$, which can be used to find a short vector in $\text{Log}(g) + \text{Log}(\mathcal{O}_K^\times)$, giving rise to a short element of $g\mathcal{O}_K^\times$, i.e., a short generator. We show in Theorem 6.18 that this method allows to find in quantum polynomial time an approximation of the shortest vector of $\mathfrak{a}$ for the subexponential approximation factor $\exp(\tilde{O}(\sqrt{m}))$.

6.1. Computational problems in lattices

Recall that a Euclidean lattice is a discrete subgroup of the vector space $\mathbf{R}^n$, with the canonical Euclidean norm denoted $\|\cdot\|$. The length of the shortest non-zero vector of a lattice Λ is called the minimal distance, and denoted $\lambda_1(\Lambda)$. The main problem we are trying to solve is the following.

Definition 6.1 (approx-SVP)**.** The *short vector problem* with approximation factor α (or α-SVP) is the following: given a basis of a lattice $\Lambda \subset \mathbf{R}^n$, find a vector $v \in \Lambda \setminus \{0\}$ such that $\|v\| \leq \alpha\lambda_1(\Lambda)$.

This problem is closely related to the close vector problem.

Definition 6.2 (approx-CVP)**.** The *close vector problem* up to distance δ (or δ-CVP) is the following: given a basis of a lattice $\Lambda \subset \mathbf{R}^n$ and a target $t \in \mathbf{R}^n$, find a vector $v \in \Lambda$ such that $\|v - t\| \leq \delta$.

Given a *short* basis of the lattice Λ (i.e., a basis consisting of short vectors), one can find good solutions of the close vector problem, as exposed in the rest of this section. However, if only a "bad" basis is known (i.e., with long vectors), then both above problems are believed to be hard. This gap between what is feasible with a good or a bad basis is at the heart of lattice-based public key cryptography: a bad basis can serve as a public key (and enables a few simple tasks, like generating random lattice points), while a good basis of the same lattice can serve as secret key (and allows to solve otherwise difficult problems, like finding lattice points close to a given target).

In the rest of this section, we present algorithms to solve approx-CVP given a short basis (which will prove very useful in the design of algorithms to solve approx-SVP in ideal lattices). If $B = [b_1, \ldots, b_k] \in \mathbf{R}^{n \times k}$ is a matrix composed of linearly independent column vectors $b_i \in \mathbf{R}^n$, we denote by $\widetilde{B} = [\widetilde{b}_1, \ldots, \widetilde{b}_k] \in \mathbf{R}^{n \times k}$ its Gram-Schmidt orthogonalisation. Moreover, we denote by $\mathcal{P}(B)$ the centered parallelepiped spanned by B, defined as

$$\mathcal{P}(B) = B \cdot [-1/2, 1/2)^k = \left\{ \sum x_i b_i \middle| x_i \in [-1/2, 1/2) \right\}.$$

If B is the basis of a full-rank lattice $\Lambda \subset \mathbf{R}^n$, both $\mathcal{P}(B)$ and $\mathcal{P}(\widetilde{B})$ are fundamental domains for Λ on $\mathbf{R}^n$. These fundamental domains admit polynomial-time reduction algorithms. For the latter fundamental domain $\mathcal{P}(\widetilde{B})$, this algorithm is referred to as *size-reduction* or as the *nearest-plane algorithm* [LLL82, Bab86].

Lemma 6.3. *There is a classical deterministic polynomial time algorithm* $\mathrm{NP}(B, t)$*, that given the basis* $B \in \mathbf{Q}^{n \times k}$ *of a lattice* $\Lambda \subset \mathbf{R}^n$*, and a target* $t \in \Lambda \otimes \mathbf{Q}$*, outputs a pair* (v, d) *where* $v \in \mathbf{Z}^k$*,* $d \in \mathcal{P}(\widetilde{B})$ *and* $t = Bv + d$*.*

Given a short basis B of a lattice Λ, the above algorithm can be used to find a lattice point v close to any target t. In fact, and this will prove very convenient, it is even sufficient to know a set of short vectors of Λ that span $\Lambda \otimes \mathbf{R}$.

Corollary 6.4. *There is a classical deterministic polynomial time algorithm* $\mathrm{CV}(W, t)$*, that given a set* W *of* k *vectors of a lattice* $\Lambda \subset \mathbf{Q}^n$ *that spans* $\Lambda \otimes \mathbf{Q}$*, and a target* $t \in \Lambda \otimes \mathbf{Q}$*, outputs a vector* $v \in \mathbf{Z}^k$ *such that both*

$$\|W \cdot v - t\| \leq 1/2 \cdot \sqrt{n} \cdot \max_{w \in W} \|w\|, \text{ and,} \tag{6.1}$$

$$\|W \cdot v - t\|_1 \leq 1/2 \cdot n \cdot \max_{w \in W} \|w\|. \tag{6.2}$$

Proof. First, we construct a set of linearly independent vectors $C \subset W$, which can be done in deterministic polynomial time in a greedy manner. The set C generates a full-rank sub-lattice of Λ, in particular setting $(v', d) = \mathrm{NP}(C, t)$ it holds that $Cv' - t = d \in \mathcal{P}(\widetilde{C})$, and by Euclidean additivity

$$\begin{aligned} \|d\|^2 &\leq 1/4 \cdot \textstyle\sum_i \|\widetilde{c}_i\|^2 \\ &\leq 1/4 \cdot n \cdot \max_i \|\widetilde{c}_i\|^2 \\ &\leq 1/4 \cdot n \cdot \max_{w \in W} \|w\|^2. \end{aligned}$$

It remains to pad the vectors v' to v with appropriately placed zeros to conclude the proof of (6.1). The proof of (6.2) is simply derived from (6.1) by Cauchy-Schwartz inequality. □

We also require an algorithm to find a close vector with respect to the ℓ_∞-norm, yet in the worst-case the algorithm may not provide a close enough vector. This can be improved by resorting to a probabilistic approach, thanks to the following proposition.

Proposition 6.5. *If $\widetilde{B} \in \mathbf{R}^{n\times k}$ has orthogonal columns, and if x is uniformly distributed over $\mathcal{P}(\widetilde{B})$, then*

$$\|x\|_\infty \leq \tau \cdot \max_i \|\widetilde{b}_i\|$$

holds except with probability at most $2n \cdot \exp(-2\tau^2)$.

Proof. First, let us write $(\widetilde{B}, 0) = QD$ where D is a diagonal matrix with coefficients $(\|\widetilde{b}_1\|, \ldots, \|\widetilde{b}_k\|, 0, \ldots, 0)$ and Q is an orthogonal matrix (i.e., $QQ^t = Q^tQ = I$).

We write $x = QDy$ where y is uniform in $[-1/2, 1/2)$. In particular, for each j we have $x_j = \sum_i Q_{j,i}D_{i,i}y_i$. Hoeffding's bound states that the probability that $|x_j| \geq s$ is less than $2\exp(-2s^2/\sum(Q_{j,i}D_{i,i})^2)$. Note that $\sum_i(Q_{j,i}D_{i,i})^2 \leq \max_i\|\widetilde{b}_i\|^2$. Taking $s = \tau \cdot \max_i \|\widetilde{b}_i\|$, one concludes by the union bound over all j's. □

Lemma 6.6. *There is a classical randomized polynomial time algorithm $\mathrm{CV}_\infty(W, t)$ that given a set W of k vectors of a lattice $\Lambda \subset \mathbf{R}^n$ that spans $\Lambda \otimes \mathbf{Q}$, and a target $t \in \Lambda \otimes \mathbf{Q}$, outputs a vector $v \in \mathbf{Z}^k$ such that*

$$\|W \cdot v - t\|_\infty \leq \sqrt{2 \cdot \log(8n)} \cdot \max_{w\in W} \|w\| \tag{6.3}$$

with probability at least $1/2$.

Proof. First, construct a set of linearly independent vectors $C \subset W$, and consider the lattice Λ' generated by C. Sample a uniform $p \in \mathcal{P}(\widetilde{C})$, compute $(v, d) = \mathrm{NP}(C, t + p)$. Note that $\|W \cdot v - t\|_\infty \leq \|W \cdot v - (t + p))\|_\infty + \|p\|_\infty$. Because p is uniform over a fundamental domain of Λ', it is the case that $t + p \bmod \Lambda'$ is uniform, therefore $(W \cdot v - (t + p))$ is uniform over $\mathcal{P}(\widetilde{C})$.

Apply Proposition 6.5 to both p (respectively $W \cdot v - (t+p)$) with $\tau = \sqrt{1/2 \cdot \log(8n)}$: $\|p\|_\infty$ (respectively $\|W \cdot v - (t + p)\|_\infty$) is less than $\sqrt{1/2 \cdot \log(8n)} \cdot \max_{w\in W} \|w\|$ except with probability at most $1/4$. A union bound allows to conclude. □

6.2. Computing in number fields and their class groups

To find short vectors in ideal lattices, we need to perform computations in a number field K, in its ring of integers $\mathcal{O}_K$, and in its class group Cl_K.

6.2.1. Representation of elements of $\mathcal{O}_K$. The standard representation of an element $\alpha \in \mathcal{O}_K$ is the vector $\vec{\alpha} = (\alpha_0, \ldots, \alpha_{n-1})$ in the standard power $\mathbf{Z}$-basis of $\mathcal{O}_K$, i.e., the sequence of coefficients of the polynomial $\alpha = \sum \alpha_i X^i \mod \Phi_m(X)$ where Φ_m denotes the m-th cyclotomic polynomial. A fractional element $\alpha \in K$ is uniquely represented as $\frac{1}{q} \cdot \vec{\alpha}'$ where q is a positive integer coprime to the greatest common divisor of the coefficients of α'.

Often, algorithms for $\mathcal{O}_K$ have to manipulate very large elements, so large that a standard representation would have an exponential length. It is the case for instance for the quantum polynomial time algorithms of [BS16]. This issue is resolved by using a *compact representation*: a compact representation of an element $\alpha \in K$ is a sequence of

elements in $\gamma_1, \ldots, \gamma_\ell \in \mathcal{O}_K$ in the standard representation and integers $k_1, \ldots, k_\ell$ such that $\alpha = \prod_{i=1}^{\ell} \gamma_i^{k_i}$.

If it is guaranteed that $\alpha \in K$ is short, one can efficiently recover a standard representation from a compact one. In [CDPR16], this is dealt with by resorting to floating-point approximations, yet Biasse [Bia18] suggested to instead perform fast modular exponentiation.

Lemma 6.7 (Formalised from [Bia18])**.** *Given elements $\gamma_1, \ldots, \gamma_\ell \in K$ in standard representation and integers $k_1, \ldots, k_\ell, q, B \in \mathbf{Z}$, assuming that $\alpha = \prod_{i=1}^{\ell} \gamma_i^{k_i}$ satisfies $q\alpha \in \mathcal{O}_K$, and the standard representation of α has coefficients with absolute value at most B, one can compute α in standard representation in polynomial time in the size of the input.*

Proof. Choose $Q \geq 2qB$, and compute $q\alpha = q \prod_{i=1}^{\ell} \gamma_i^{k_i} \bmod Q$ using fast modular exponentiation. Recover $q\alpha$ as a representative of $q\alpha \bmod Q$ with coefficients in the interval $[-Q/2, Q/2]$. □

6.2.2. Quantum algorithms for class groups. Classically, problems related to class group computations remain difficult, and the best known classical algorithms for class group computations run in sub-exponential time (for example, see [BF14, BEF+17]). Yet, building on the recent advances on quantum algorithms for the hidden subgroup problem in large dimensions [EHKS14], Biasse and Song [BS16] introduced a quantum algorithm to perform S-unit group computations. It allows to compute class groups, and to solve the principal ideal problem (PIP) in quantum polynomial time.

Theorem 6.8 ([BS16, Theorem 1.3])**.** *There is a quantum algorithm for deciding if an ideal $\mathfrak{a} \subseteq \mathcal{O}$ of an order $\mathcal{O}$ in a number field K is principal, and for computing $\alpha \in \mathcal{O}$ in compact representation such that $\mathfrak{a} = (\alpha)$, in polynomial time in the parameters $[K : \mathbf{Q}]$, $\log(N(\mathfrak{a}))$ and $\log(\Delta)$, where Δ is the absolute value of the discriminant of $\mathcal{O}$.*

The Biasse-Song [BS16] algorithm for S-unit group computation also allows to solve the class group discrete logarithm problem[1]: given a basis $\mathfrak{B}$ of ideals generating a subgroup of the class group Cl_K containing the class of $\mathfrak{a}$, express the class of $\mathfrak{a}$ as a product of ideals in $\mathfrak{B}$.

Proposition 6.9 ([BS16])**.** *Let $\mathfrak{B}$ be a set of prime ideals generating a subgroup H of Cl_K. There exists a quantum algorithm $\mathrm{ClDL}_{\mathfrak{B}}$ which, when given as input any ideal $\mathfrak{a}$ in $\mathcal{O}_K$ such that $[\mathfrak{a}] \in H$, outputs a vector $y \in \mathbf{Z}^{\mathfrak{B}}$ such that $\prod \mathfrak{p}^{y_\mathfrak{p}} \sim \mathfrak{a}$, and runs in polynomial time in $n = \deg(K)$, $\max_{\mathfrak{p} \in \mathfrak{B}} \log(N\mathfrak{p})$, $\log(N\mathfrak{a})$, $|\mathfrak{B}|$ and $\log(\Delta_K)$, where Δ_K is the absolute value of the discriminant of K.*

Proof. Given Theorem 1.1 of [BS16] the proof of this corollary is standard, and recognisable as the linear algebra step of index calculus methods.

The prime factorization $\mathfrak{a} = \mathfrak{q}_1^{a_1} \ldots \mathfrak{q}_k^{a_k}$ can be obtained in polynomial time in n, $\log(\Delta_K)$ and $\log(N\mathfrak{a})$, by Shor's algorithm [Sho97, EH10]. Let $\mathfrak{C} = \mathfrak{B} \cup \{\mathfrak{q}_1, \ldots, \mathfrak{q}_k\}$, and one can assume without loss of generality that this union is disjoint. Let $r = n_1 + n_2 - 1$,

[1] In fact, Proposition 6.9 is a corollary of [BS16, Theorem 1.1]. Even though it is not stated explicitly in that paper, it must be attributed to that paper nevertheless. Indeed, the implication is straightforward and its authors have already sketched it in public talks. Our purpose here is merely to include technical details for completeness.

where n_1 is the number of real embeddings of K, and n_2 is the number of pairs of complex embeddings. Consider the homomorphism

$$\psi : \mathbf{Z}^{\mathfrak{B}} \times \mathbf{Z}^k \longrightarrow \mathrm{Cl}_K$$
$$((e_{\mathfrak{p}})_{\mathfrak{p}\in\mathfrak{B}}, (f_1, \ldots, f_k)) \longmapsto \left[\prod_{\mathfrak{p}\in\mathfrak{B}} \mathfrak{p}^{e_{\mathfrak{p}}}\right] \cdot \left[\prod_{i=1}^{k} \mathfrak{q}_i^{f_i}\right].$$

As described in [BS16, Section 4], solving the $\mathfrak{C}$-unit problem provides a generating set of size $c = r + |\mathfrak{B}| + k$ for the kernel L of ψ. From [BS16, Theorem 1.1] such a generating set $\{v_i\}_{i=1}^c$ can be found by a quantum algorithm in time polynomial in n, $\max_{\mathfrak{p}\in\mathfrak{C}}\{\log(N\mathfrak{p})\}$, $\log(d_K)$ and $|\mathfrak{C}| = O(|\mathfrak{B}| + \log(N\mathfrak{a}))$. For each i, write $v_i = ((w_{i,\mathfrak{p}})_{\mathfrak{p}\in\mathfrak{B}}, (v_{i,1}, \ldots, v_{i,k}))$. Since $[\mathfrak{a}] \in H$ and $\mathfrak{B}$ generates H, the system of equations $\{\sum_{j=1}^c x_j v_{j,i} = a_i\}_{i=1}^k$ has a solution $x \in \mathbf{Z}^c$ which can be computed in polynomial time. We obtain

$$0 = \psi\left(\sum_{i=1}^{c} x_i v_i\right) = \left[\prod_{\mathfrak{p}\in\mathfrak{B}} \mathfrak{p}^{\sum_j x_j w_{j,\mathfrak{p}}}\right] \cdot \left[\prod_{i=1}^{k} \mathfrak{q}_i^{\sum_j x_j v_{j,i}}\right] = \left[\prod_{\mathfrak{p}\in\mathfrak{B}} \mathfrak{p}^{\sum_j x_j w_{j,\mathfrak{p}}}\right] \cdot [\mathfrak{a}].$$

Then, the output of $\mathrm{ClDL}_{\mathfrak{B}}$ is $y = \left(-\sum_j x_j w_{j,\mathfrak{p}}\right)_{\mathfrak{p}\in\mathfrak{B}}$. □

6.3. Preliminaries on cyclotomic ideal lattices

An integer $m > 2$ is fixed for this chapter and the next, as well as a primitive m-th root of unity $\zeta_m \in \mathbf{C}$. The cyclotomic field of conductor m is $K = \mathbf{Q}(\zeta_m)$, and the cyclotomic ring of conductor m is $\mathcal{O}_K = \mathbf{Z}[\zeta_m]$, the ring of integers of K. The integer Δ_K is the absolute value of the discriminant of K. The field $K^+ = \mathbf{Q}(\zeta_m + \zeta_m^{-1})$ is the maximal real subfield of K. As usual, the algebraic norm of an ideal $\mathfrak{h}$ is denoted $N(\mathfrak{h})$. We denote by $\tau \in \mathrm{Gal}(K/\mathbf{Q})$ the complex conjugation of K.

Class groups. Let Cl_K be the class group of $\mathcal{O}_K$. The class of an ideal $\mathfrak{h}$ is denoted $[\mathfrak{h}]$, and if two ideals $\mathfrak{h}$ and $\mathfrak{h}'$ are in the same class, we write $\mathfrak{h} \sim \mathfrak{h}'$. Let Cl_{K^+} be the class group of K^+. The relative norm map $N_{K/K^+} : \mathrm{Cl}_K \to \mathrm{Cl}_{K^+}$ on ideal classes (which sends the class of $\mathfrak{h}$ to the class of $\mathfrak{h}^{1+\tau}$) is a surjection, and its kernel is the relative class group Cl_K^-.

The Galois group and its group ring. Let G denote the Galois group of the extension $K/\mathbf{Q}$. It is canonically isomorphic to $(\mathbf{Z}/m\mathbf{Z})^\times$ via the isomorphism $a \mapsto \sigma_a$, where σ_a is the automorphism sending ζ_m to ζ_m^a. Naturally, we have $\tau = \sigma_{-1}$. Given an automorphism $\sigma \in G$, and an element $a \in K$ or an ideal $\mathfrak{h}$ of $\mathcal{O}_K$, we denote the action of σ by a^σ or $\mathfrak{h}^\sigma$. This notation extends to the action of the group ring $\mathbf{Z}[G]$: for any $\alpha = \sum_{\sigma\in G} \alpha_\sigma \sigma \in \mathbf{Z}[G]$, we write

$$\mathfrak{h}^\alpha = \prod_{\sigma\in G} (\mathfrak{h}^\sigma)^{\alpha_\sigma}.$$

Ideals as lattices. The field K is a Hermitian vector space over $\mathbf{Q}$ for the inner product $\langle a, b\rangle = \mathrm{Tr}(ab^\tau)$. The corresponding Euclidean norm is denoted $\|a\|$, and coincides with the ℓ_2-norm induced by the Minkowski embedding

$$K \longrightarrow \mathbf{C}^{\varphi(m)} : a \longmapsto (a^\sigma)_{\sigma\in G}.$$

We also denote the ℓ_1-norm and ℓ_∞-norm by $\|a\|_1$ and $\|a\|_\infty$. The volume of an ideal $\mathfrak{h}$ as a lattice relates to its algebraic norm by $\mathrm{Vol}(\mathfrak{h}) = \sqrt{\Delta_K} N(\mathfrak{h})$. The length $\lambda_1(\mathfrak{h})$ of

the shortest non-zero vector of $\mathfrak{h}$ is determined by its algebraic norm up to a polynomial factor:

$$\frac{1}{\text{poly}(n)} N(\mathfrak{h})^{1/n} \leq \lambda_1(\mathfrak{h}) \leq \text{poly}(n) N(\mathfrak{h})^{1/n}. \tag{6.4}$$

The right inequality is an application of Minkowsky's second theorem, whereas the left one follows from the fact that the ideal $v\mathcal{O}_K$ generated by the shortest vector v of $\mathfrak{h}$ is a multiple (a sub-ideal) of $\mathfrak{h}$, and that $\text{Vol}(v\mathcal{O}_K) \leq \|v\|^n$.

6.4. The geometry of cyclotomic units

In this section and the next, we study the geometry of cyclotomic units, and as an application, we provide a quantum algorithm for approx-SVP in principal ideals, Algorithm 6.2. Suppose g is a generator of some principal ideal $\mathfrak{a}$. Then, $g\mathcal{O}_K^\times$ is the set of all generators of $\mathfrak{a}$. Generators of short Euclidian norm can be studied and found by investigating the geometry of the unit group $\mathcal{O}_K^\times$, and more specifically of the lattice $\text{Log}(\mathcal{O}_K^\times)$ obtained via the logarithmic embedding. The main results exploit the subgroup $C \subset \mathcal{O}_K^\times$ of cyclotomic units, whose corresponding lattice $\text{Log}(C)$ admits an efficiently computable set of short generators.

6.4.1. The logarithmic embedding and cyclotomic units. Recall that G denotes the Galois group $\text{Gal}(K/\mathbf{Q})$, and $\tau \in G$ is complex conjugation.

Definition 6.10 (Logarithmic embedding)**.** The *logarithmic embedding* of K is

$$\begin{aligned} \text{Log} : K^\times &\longrightarrow \mathbf{R}[G]/(1-\tau) \\ a &\longmapsto \sum_{\sigma \in G} \log(|a^\sigma|) \cdot \sigma^{-1}. \end{aligned}$$

It is easy to check that this is a morphism of $\mathbf{Z}[G]$-modules. The ring $\mathbf{R}[G]/(1-\tau)$ also has a geometric structure: given any set $B \subset G$ of representatives of $G/\langle\tau\rangle$, the projection of B to $\mathbf{R}[G]/(1-\tau)$ forms a basis (which does not actually depend on the choice of B) and we consider the norms on $\mathbf{R}[G]/(1-\tau)$ coming from the induced isomorphism with $\mathbf{R}^{\varphi(m)/2}$.

The kernel of the logarithmic embedding restricted to $\mathcal{O}_K^\times$ is the subgroup generated by -1 and ζ_m. Dirichlet's unit theorem implies that $\text{Log}(\mathcal{O}_K^\times)$ is a full-rank lattice in the linear subspace of $\mathbf{R}[G]/(1-\tau)$ orthogonal to $s(G) = \sum_{\sigma \in G} \sigma$.

Definition 6.11 (Cyclotomic units)**.** Let V be the multiplicative group generated by

$$\{\pm\zeta_m\} \cup \{1 - \zeta_m^j \mid j = 1, \ldots, m-1\}.$$

The *group of cyclotomic units* of K is the intersection $C = V \cap \mathcal{O}_K^\times$.

Theorem 6.12. *The lattice* $\text{Log}(C)$ *has full rank in* $\text{Log}(\mathcal{O}_K^\times)$.

Proof. From [Sin78], the group $C^+ = C \cap K^+$ has finite index in the group of real units $E^+ = \mathcal{O}_K^\times \cap K^+$. Let W be the multiplicative group generated by -1 and ζ_m. From [Was12, Theorem 4.12], the group WE^+ has index 1 or 2 in $\mathcal{O}_K^\times$. Since W is the kernel of $\text{Log} : \mathcal{O}_K^\times \to \mathbf{R}[G]/(1-\tau)$, we get

$$\begin{aligned} [\text{Log}(\mathcal{O}_K^\times) : \text{Log}(C^+)] &= [\text{Log}(\mathcal{O}_K^\times) : \text{Log}(E^+)][\text{Log}(E^+) : \text{Log}(C^+)] \\ &= [\mathcal{O}_K^\times : WE^+][E^+ : C^+], \end{aligned}$$

which is finite. Therefore $[\text{Log}(\mathcal{O}_K^\times) : \text{Log}(C)]$ is also finite. □

6.4.2. Short generating vectors of the cyclotomic units. We are interested in finding short generators of the lattice $\mathrm{Log}(C)$. Let $m = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ be the prime factorization of m, and for any index i let $m_i = m p_i^{-\alpha_i}$. For $0 < j < m$, let

$$v_j = \begin{cases} 1 - \zeta_m^j & \text{if for all indices } i, \text{ we have } m_i \nmid j, \\ \dfrac{1-\zeta_m^j}{1-\zeta_m^{m_i}} & \text{otherwise, for the unique } i \text{ such that } m_i \mid j. \end{cases}$$

Theorem 6.13 ([Kuč92, Theorem 4.2])**.** *The lattice* $\mathrm{Log}(C)$ *is generated by the set of vectors* $\{\mathrm{Log}(v_j) \mid 0 < j < m\}$.

Lemma 6.14. *For any integer* j *not divisible by* m*, we have* $\| \mathrm{Log}(1-\zeta_m^j)\| = O(\sqrt{m})$.

Proof. Write $j = ab$, where a divides m and $(b, m/a) = 1$.

$$\| \mathrm{Log}(1-\zeta_m^j)\|^2 = \sum_{i \in (\mathbf{Z}/m\mathbf{Z})^\times/\{\pm 1\}} \left(2 \log|1-\zeta_m^{ij}|\right)^2 = 4 \sum_{i \in (\mathbf{Z}/m\mathbf{Z})^\times/\{\pm 1\}} \left(\log|1-\zeta_{m/a}^{i}|\right)^2.$$

The natural group homomorphism $(\mathbf{Z}/m\mathbf{Z})^\times \to (\mathbf{Z}/(m/a)\mathbf{Z})^\times$ is a surjection, so its kernel has cardinality $\varphi(m)/\varphi(m/a)$, and we obtain

$$\begin{aligned} \| \mathrm{Log}(1-\zeta_m^j)\|^2 &= 4\frac{\varphi(m)}{\varphi(m/a)} \sum_{i \in (\mathbf{Z}/(m/a)\mathbf{Z})^\times/\{\pm 1\}} \left(\log|1-\zeta_{m/a}^{i}|\right)^2 \\ &= 4\frac{\varphi(m)}{\varphi(m/a)} \sum_{i \in (\mathbf{Z}/(m/a)\mathbf{Z})^\times/\{\pm 1\}} \left(\log|2\sin(\pi i a/m)|\right)^2 \\ &\le 8a \sum_{i=1}^{\lfloor m/2a \rfloor} \left(\log(2\sin(\pi i a/m))\right)^2 \\ &= 8a \sum_{i=1}^{\lfloor m/2a \rfloor} f(ia/m), \end{aligned} \tag{6.5}$$

where $f : [0, 1/2] \to \mathbf{R}$ is defined as $f(x) = (\log(2\sin(\pi x)))^2$. Since $f(x) \le \log 2$ for $1/6 \le x \le 1/2$, the terms in Equation (6.5) coming from $i > \lfloor m/6a \rfloor$ sum to at most $O(m)$. It remains to estimate the contribution of the remaining terms. Since $\sin(\pi x) \ge 2x$ for $0 \le x \le 1/2$, we have

$$8a \sum_{i=1}^{\lfloor m/6a \rfloor} f(ia/m) \le 8a \sum_{i=1}^{\lfloor m/6a \rfloor} (\log(4ia/m))^2 \le 8a\frac{m}{a}\int_0^{1/6} (\log(4x))^2 dx = O(m),$$

where the last equality follows from $\int_0^y (\log x)^2 dx = y((\log y)^2 - 2\log(y) + 2)$. □

6.5. Short vectors in principal ideals

The results from Section 6.4 on the geometry of cyclotomic units can be exploited to find short vectors in principal ideals.

6.5.1. Short generators in principal ideals.

Theorem 6.15. *There is a randomized algorithm* ShortGenerator *(Algorithm 6.1) that for any* $g \in \mathcal{O}_K$ *(in compact representation), finds an element* $h \in \mathcal{O}_K$ *(in compact representation) such that* $g\mathcal{O}_K = h\mathcal{O}_K$ *and*

$$\|h\| = \exp\left(O\left(\sqrt{m \log m}\right)\right) \cdot N(g)^{1/\varphi(m)},$$

and runs in polynomial time in the size of the input.

Algorithm 6.1 SHORTGENERATOR(g): finds a short generator of $g\mathcal{O}_K$.

Require: An element $g \in \mathcal{O}_K$ in compact representation $(\gamma_i, k_i)_{i=1}^{\ell}$.
Ensure: The compact representation of a short element generating $g\mathcal{O}_K$.
1: $W = (w_1, \ldots, w_{m-1})$ where $w_i = \mathrm{Log}(v_i)$; $s(G) = \sum_{\sigma \in G} \sigma \in \mathbf{R}[G]/(1-\tau)$;
2: $t' \leftarrow \sum_{i=1}^{\ell} k_i \mathrm{Log}(\gamma_i)$;
3: $t'' \leftarrow {}^{1}/_{\varphi(m)} \cdot \log(N(g)) \cdot s(G)$;
4: $t \leftarrow t' - t'' \in \mathrm{Log}(\mathcal{O}_K^{\times}) \otimes \mathbf{R}$;
5: **repeat**
6: $\quad x \leftarrow \mathrm{CV}_{\infty}(W, t)$; {randomized, see Lemma 6.6}
7: **until** $\|W \cdot x - t\|_{\infty} \leq \sqrt{2 \cdot \log(4\varphi(m))} \cdot \max_{w \in W} \|w\|$
8: **return** concatenation of $(\gamma_i, k_i)_{i=1}^{\ell}$ and $(v_i, -x_i)_{i=1}^{m-1}$.

Proof. A technical hurdle for this algorithm is the need to resort to approximate computations. We sketch here the proof ignoring this issue, by assuming that all operations on $\mathbf{R}$ can be performed in polynomial time. The full proof accounting for precision issues is deferred to Section 6.5.2.

Recall that g is given in compact representation $(\gamma_i, k_i)_{i=1}^{\ell}$, where $g = \prod_{i=1}^{\ell} \gamma_i^{k_i}$. The element t is the orthogonal projection of t' on the subspace $\mathrm{Log}(\mathcal{O}_K^{\times}) \otimes \mathbf{R}$. Let $W = (w_1, \ldots, w_{m-1})$ where $w_i = \mathrm{Log}(v_i)$. From Theorem 6.13, W is a set of generators of $\mathrm{Log}(C)$, and by Lemma 6.14, we have $\max_{w \in W} \|w\| = O(\sqrt{m})$. Calls to the randomized algorithm $\mathrm{CV}_{\infty}(W, t)$ are repeated until the output x satisfies

$$\|W \cdot x - t\|_{\infty} \leq \sqrt{2 \cdot \log(4\varphi(m))} \cdot \max_{w \in W} \|w\|.$$

According to Lemma 6.6, this procedure terminates in average polynomial time. Let h be the element with compact representation $(\gamma_i, k_i)_{i=1}^{\ell} \frown (v_i, -x_i)_{i=1}^{m-1}$ (where $\frown$ denotes the concatenation of sequences). We have

$$\begin{aligned}
\|h\|_{\infty} &\leq \exp(\|\mathrm{Log}(g) - W \cdot x\|_{\infty}) \\
&\leq \exp(\|t + t'' - W \cdot x\|_{\infty}) \\
&\leq \exp(\|t''\|_{\infty}) \cdot \exp(\|t - W \cdot x\|_{\infty}) \\
&\leq \exp\left(\|{}^{1}/_{\varphi(m)} \cdot \log(N(g)) \cdot s(G)\|_{\infty}\right) \cdot \exp\left(\sqrt{2 \cdot \log(4\varphi(m))} \cdot \max_{w \in W} \|w\|\right) \\
&\leq N(g)^{1/\varphi(m)} \cdot \exp\left(O\left(\sqrt{m \log m}\right)\right).
\end{aligned}$$

We conclude from the inequality $\|h\| \leq \sqrt{\varphi(m)} \|h\|_{\infty}$. □

6.5.2. Numerical stability. In this section, we prove that we can round all the logarithms $\mathrm{Log}(\gamma_i)$ and $\mathrm{Log}(v_i)$ to $\mathbf{Q}$ with polynomially many bits of precision and still obtain a small generator h. Set $p = \log_2(\max_{i=1}^{k} k_i \lceil \|\gamma_i\|_{\infty} \rceil)$ and note that p is polynomial in the size of the input. Let $n = \varphi(m)/2$ and suppose without loss of generality that the first $n-1$ vectors $w_1, \ldots, w_{n-1}$ are linearly independent.

The algorithm. Fix a set of n representatives of the cosets $G/\langle\tau\rangle$; they form a basis for $\mathbf{Z}[G]/(1-\tau)$. In this basis, consider the matrices

$$L = (\mathrm{Log}(\gamma_i))_{i=1}^{\ell}, \text{ and}$$
$$W = (w_i)_{i=1}^{n-1} = (\mathrm{Log}(v_i))_{i=1}^{n-1}.$$

Let $\varepsilon = 2^{-(p+m^2)}$, and compute an approximation $\overline{L}$ with coefficients in $\varepsilon\mathbf{Z}$ such that $\|L - \overline{L}\|_\infty \leq \varepsilon$. Now, we want an approximation $\overline{W}$ of W with coefficients in $\varepsilon\mathbf{Z}$ such that $\|W - \overline{W}\|_\infty \leq \varepsilon$ and each vector $\overline{w}_i$ still lies in $\mathrm{Log}(\mathcal{O}_K^\times) \otimes \mathbf{R}$. To do so, find some approximation $\widetilde{W}$ such that $\|W - \widetilde{W}\|_\infty \leq \varepsilon/2$, and let

$$\overline{w}_i = \widetilde{w}_i - \frac{1}{\varphi(m)} \sum_{j=1}^{n} \widetilde{w}_{i,j} s(G) \in \mathrm{Log}(\mathcal{O}_K^\times) \otimes \mathbf{R},$$

which satisfies $\|\overline{W} - \widetilde{W}\|_\infty \leq \varepsilon/2$.

We proceed with the same computation as in the proof of Theorem 6.15, using these approximate values. Compute $\overline{t}' = \overline{L} \cdot k$, and project $\overline{t}'$ orthogonally to $s(G)$, that is decompose $\overline{t}' = \overline{t} + \overline{t}''$ such that $\overline{t} \in \mathrm{Log}(\mathcal{O}_K^\times) \otimes \mathbf{R}$ and $\overline{t}' \in s(G) \cdot \mathbf{R}$. Repeatedly call the randomized algorithm $\overline{x} \leftarrow \mathrm{CV}_\infty(\overline{W}, \overline{t})$ until the output $\overline{x}$ satisfies

$$\|\overline{W} \cdot \overline{x} - \overline{t}\|_\infty \leq \sqrt{2 \cdot \log(8n)} \cdot \max_{w \in W} \|\overline{w}\|. \tag{6.6}$$

According to Lemma 6.6, this procedure terminates in average polynomial time. We output the compact representation $(\gamma_i, k_i)_{i=1}^{\ell} \frown (v_i, -\overline{x}_i)_{i=1}^{n-1}$ of h.

Analysis. We now prove that the output h is short. We have

$$\begin{aligned}\|h\|_\infty &\leq \exp(\|L \cdot k - W \cdot \overline{x}\|_\infty) \\ &\leq \exp(\|\overline{t}' - \overline{W} \cdot \overline{x}\|_\infty) \cdot \exp(\|(L - \overline{L}) \cdot k\|_\infty + \|(W - \overline{W}) \cdot \overline{x}\|_\infty)\end{aligned}$$

From Lemma 6.14, we have $\max_{w \in W} \|\overline{w}\| \leq O(\sqrt{m}) + \sqrt{n}\varepsilon \leq O(\sqrt{m})$, and together with (6.6) we can bound the first factor as

$$\exp(\|\overline{t}' - \overline{W} \cdot \overline{x}\|_\infty) \leq \exp(\|\overline{t}''\|_\infty) \cdot \exp(O(\sqrt{m \log m})).$$

Secondly, since $t'', \overline{t}''$ are respectively the projection of $t' = Lk$ and $\overline{t}'' = \overline{L}k$, it holds that $\|t'' - \overline{t}''\|_\infty \leq n\|t' - \overline{t}'\|_\infty$. So we get that $\|h\|_\infty$ is at most

$$N(g)^{1/\varphi(m)} \cdot \exp(O(\sqrt{m \log m})) \cdot \exp((n+1)\|(L - \overline{L}) \cdot k\|_\infty + \|(W - \overline{W}) \cdot \overline{x}\|_\infty).$$

Next, note that we have $\|(L - \overline{L}) \cdot k\|_\infty \leq n \cdot \|k\|_\infty \cdot \varepsilon \leq 2^{-m^2 + o(m)}$, so:

$$\|h\|_\infty \leq N(g)^{1/\varphi(n)} \cdot \exp(O(\sqrt{m \log m})) \cdot \exp(2^{-m^2+o(m)} + \|(W - \overline{W}) \cdot \overline{x}\|_\infty). \tag{6.7}$$

It remains to bound $\|\overline{x}\|$. For any matrix A, write A^+ for its pseudoinverse. We have that

$$\|\overline{x}\| \leq \|\overline{W}^+\| \|\overline{W} \cdot \overline{x}\| \leq \|\overline{W}^+\| \left(\|\overline{W} \cdot \overline{x} - \overline{t}\| + \|\overline{t}\|\right). \tag{6.8}$$

Lemma 6.16. *We have* $\|W^+\| \leq 5 \cdot \|W\|^{\varphi(m)-3}$.

Proof. The elements $w_1, \ldots, w_{n-1}$ generate a sublattice of $\mathrm{Log}(\mathcal{O}_K^\times)$, so

$$\det(W^t W) \geq \det(\mathrm{Log}(\mathcal{O}_K^\times)) = R_K \sqrt{n},$$

where R_K denotes the regulator of the field K. Writing $\lambda_1 \leq \cdots \leq \lambda_{n-1}$ the eigenvalues of W^tW, we have

$$\|(W^tW)^{-1}\| = \frac{1}{\lambda_1} = \frac{\prod_{i=2}^{n-1}\lambda_i}{\det(W^tW)} \leq \frac{\|W\|^{2(n-2)}}{R_K\sqrt{n}}.$$

From [Fri89, Theorem B], we have $R_K > \mathrm{lcm}(2,m)/10$ (except for $m = 10$, for which we have $R_K > 0.96$). Since W has full column rank, $W^+ = (W^tW)^{-1}W^t$. We conclude that

$$\|W^+\| \leq \|W\|\|(W^tW)^{-1}\| \leq \frac{5\|W\|^{2n-3}}{\sqrt{n}} \leq 5 \cdot \|W\|^{2n-3}.$$

□

Lemma 6.17. *We have* $\|\overline{W}^+\| \leq 4\|W^+\|$.

Proof. Let $E = \overline{W} - W$. First observe that $\overline{W}^+ = (I + EW^+)^+W^+$. Let $A = I + EW^+$. Since $\|I - A^tA\| < 1/2$, the generalisation of the Neumann series for the Moore-Penrose inverse gives

$$A^+ = \sum_{i=0}^{\infty}(I - A^tA)^iA^t.$$

Therefore,

$$\|\overline{W}^+\| \leq \|A^+\|\|W^+\| \leq 2\|A\|\|W^+\| \leq 4\|W^+\|.$$

□

It follows from the two above lemmata that $\|W^+\| \leq 2^{O(m)}$. Since we have that $\|\overline{W} \cdot \overline{x} - \overline{t}\| \leq 2^{o(m)}$ and $\|\overline{t}\| \leq 2^{p+o(m)}$, we deduce from (6.8) that $\|\overline{x}\| \leq 2^{p+O(m)}$, and therefore $\|(W - \overline{W}) \cdot \overline{x}\|_\infty \leq 2^{-m^2+O(m)}$. Applying this inequality to (6.7), we conclude that

$$\begin{aligned}\|h\|_\infty &\leq N(g)^{1/\varphi(m)} \cdot \exp(O(\sqrt{m\log m})) \cdot \exp(2^{-m^2+O(m)}) \\ &\leq N(g)^{1/\varphi(m)} \cdot \exp(O(\sqrt{m\log m})).\end{aligned}$$

6.5.3. The approximate short vector problem in principal ideals.

Theorem 6.18 (Approx-SVP for cyclotomic, principal ideals)**.** *There is a quantum algorithm* PrincipalIdealSVP *(Algorithm 6.2) that, when given a principal ideal* $\mathfrak{a}$ *in the cyclotomic ring of conductor* m*, finds a generator of Euclidean norm*

$$\exp(O\left(\sqrt{m\log m}\right)) \cdot N(\mathfrak{a})^{1/\varphi(m)},$$

in expected polynomial time in m *and* $\log N(\mathfrak{a})$*. This generator approximates SVP in the lattice* $\mathfrak{a}$ *with an approximation factor* $\exp(O\left(\sqrt{m\log m}\right))$*.*

Algorithm 6.2 PrincipalIdealSVP($\mathfrak{a}$): solves Approx-SVP in a principal ideal $\mathfrak{a}$.

Require: A principal ideal $\mathfrak{a}$ of $\mathcal{O}_K$.
Ensure: The compact representation of a short generator of $\mathfrak{a}$.
1: $g \leftarrow \mathrm{PIP}(\mathfrak{a})$; {PIP algorithm [BS16, Theorem 1.3]}
2: $h \leftarrow$ ShortGenerator(g); {Algorithm 6.1}
3: **return** h.

Proof. First apply the quantum algorithm of [BS16, Theorem 1.3] on $\mathfrak{a}$. Since $\mathfrak{a}$ is principal, it returns an element $g \in \mathcal{O}_K$ in compact representation such that $\mathfrak{a} = g\mathcal{O}_K$, in polynomial time in $\log(N(\mathfrak{a}))$ and m. From Theorem 6.15, Algorithm 6.1 returns another generator h of $\mathfrak{a}$ such that

$$\|h\| = \exp\left(O\left(\sqrt{m \log m}\right)\right) \cdot N(\mathfrak{a})^{1/\varphi(m)},$$

also in polynomial time. It follows from (6.4) that h approximates SVP in $\mathfrak{a}$ with an approximation factor $\exp(O\left(\sqrt{m \log m}\right))$. □

7

Mildly short vectors in cyclotomic ideal lattices

Abstract. This chapter is primarily based on a joint work with Ronald Cramer and Léo Ducas, presented at EUROCRYPT 2017 and published as

[CDW17] R. Cramer, L. Ducas, and B. Wesolowski, *Short Stickelberger class relations and application to Ideal-SVP*, Advances in Cryptology – EUROCRYPT 2017 (J. Coron and J. B. Nielsen, eds.), Lecture Notes in Computer Science, vol. 10210, Springer, 2017, pp. 324–348.

This chapter actually extends this work: it is, as the previous chapter, part of an ongoing collaboration with Ronald Cramer and Léo Ducas. Notably, this second part of the project extends the results of [CDW17] to cyclotomic fields of arbitrary conductor.

In the previous chapter, we have seen how to find a (mildly) short vector in a principal ideal of a cyclotomic ring in quantum polynomial time. In this chapter, we show how to deal with non-principal ideals, by reducing to the principal case. We keep the notation introduced in Section 6.3.

The close principal multiple problem. To reduce the problem from arbitrary ideals to principal ideals, we introduce the *close principal multiple problem* (or CPM): given an arbitrary ideal $\mathfrak{a}$, find an integral ideal $\mathfrak{b}$ such that $\mathfrak{ab}$ is principal, and $N(\mathfrak{b})$ is small. Suppose one can solve CPM with $N(\mathfrak{b}) \leq \exp(\tilde{O}(m^{1+c}))$, for some constant $c > 0$. Then, one can apply the results from the previous chapter, Theorem 6.18, to find a generator g of the principal ideal $\mathfrak{ab}$ such that

$$\|g\| \leq N(\mathfrak{ab})^{1/\varphi(m)} \exp\left(\tilde{O}\left(\sqrt{m}\right)\right) \leq N(\mathfrak{a})^{1/\varphi(m)} \exp\left(\tilde{O}\left(m^{\max(1/2,c)}\right)\right).$$

Since $g \in \mathfrak{ab} \subset \mathfrak{a}$, one has found an approximation of the shortest vector of $\mathfrak{a}$ for an approximation factor $\exp(\tilde{O}(m^{\max(1/2,c)}))$. This is asymptotically as good as the principal case when $c = 1/2$, and better than can be guaranteed by LLL, the basis reduction algorithm from [LLL82], for any $c < 1$.

Using the Stickelberger ideal. We study in Section 7.1 the geometry of the Stickelberger ideal (see Definition 7.1), and show how it can be used to solve some version of CPM. The Stickelberger ideal is an ideal S in the group ring $\mathbf{Z}[G]$ that annihilates the class group: for any ideal $\mathfrak{h}$ in $\mathcal{O}_K$ and any $s \in S$, the ideal $\mathfrak{h}^s$ is principal. Notice that the group ring $\mathbf{Z}[G]$ is naturally isomorphic to $\mathbf{Z}^{\varphi(m)}$, so it can be seen as a lattice in $\mathbf{R}^{\varphi(m)}$. The norms $\|\cdot\|$ and $\|\cdot\|_1$ denote the usual ℓ_2 (Euclidean) and ℓ_1 norms over $\mathbf{R}^{\varphi(m)}$.

The ℓ_1-norm is particularly interesting since for any ideal $\mathfrak{h}$ and any $\alpha \in \mathbf{Z}[G]$, we have $N(\mathfrak{h}^\alpha) = N(\mathfrak{h})^{\|\alpha\|_1}$.

For the moment, suppose that $\mathfrak{a}$ is an ideal of the form $\mathfrak{p}^\alpha$ for some $\alpha \in \mathbf{Z}[G]$. Now, suppose we can find a vector γ in the sub-lattice S that is close to α for the ℓ_1-norm. This means that $\|\gamma - \alpha\|_1$ is small, and so is $N(\mathfrak{p}^{\gamma-\alpha})$. Choosing $\mathfrak{b} = \mathfrak{p}^{\gamma-\alpha}$, we have that $\mathfrak{ab}$ is principal. Up to some technicalities ($\mathfrak{b}$ is not necessarily integral), this solves CPM for $\mathfrak{a}$.

As in the principal case, we have reduced the original problem to a lattice problem: given a vector $\alpha \in \mathbf{Z}[G]$, find a close vector in the sub-lattice S. However, the lattice S does not have full rank in $\mathbf{Z}[G]$, so we cannot directly solve the close vector problem here. Instead, we work with a quotient of $\mathbf{Z}[G]$, and solve CPM for ideals in the relative class group Cl_K^- (i.e., when $\mathfrak{a}\mathfrak{a}^\tau$ is principal). This is the object of Theorem 7.8: we show that given an element $\alpha \in \mathbf{Z}[G]$, and an ideal $\mathfrak{p}$ whose class is in the relative class group, one can solve CPM for $\mathfrak{a} = \mathfrak{p}^\alpha$ with $N(\mathfrak{b}) \leq N(\mathfrak{p})^{\tilde{O}(m^{1+1/2})}$ in classical polynomial time.

Approx-SVP for any cyclotomic ideal. These conditions on the above algorithm to solve CPM seem rather restrictive, but we show in Section 7.2 that under some plausible number-theoretic assumptions, they do not cause any trouble. This leads us to a more general CPM algorithm for arbitrary ideals $\mathfrak{a}$, Theorem 7.16. It is not straightforward to formally derive the best c-value that can be achieved by the general CPM algorithm, as it relies on the structure of the class group Cl_K as a $\mathbf{Z}[G]$-module. Based on computations of the class group structure by Schoof [Sch98] and a heuristic argument, we strongly believe it is plausible that $c = 1/2$ is reachable at least for a dense family of conductors m, if not all. This leads to the main result of this chapter: Approx-SVP in arbitrary ideals, Theorem 7.10.

7.1. The geometry of the Stickelberger ideal

In this section, we study the geometry of the Stickelberger ideal, and as an application, we provide a quantum algorithm for the close principal multiple problem in any $\mathbf{Z}[G]$-cycle of the relative class group Cl_K^-, Theorem 7.8.

For any ideals $\mathfrak{a}, \mathfrak{b}$ of $\mathcal{O}_K$ and any element $\alpha \in \mathbf{Z}[G]$, if $\mathfrak{a} \sim \mathfrak{b}$, then $\mathfrak{a}^\alpha \sim \mathfrak{b}^\alpha$, so the action of $\mathbf{Z}[G]$ on ideals induces an action of $\mathbf{Z}[G]$ on the class group Cl_K. As sketched above, we are interested in building a lattice Λ of full rank in $\mathbf{Z}[G]$ with a good basis, such that for any ideal $\mathfrak{h}$, and any $\lambda \in \Lambda$, the ideal $\mathfrak{h}^\lambda$ is principal (we say that Λ is a lattice of class relations).

7.1.1. The Stickelberger ideal. Recall that the Galois group G is canonically isomorphic to $(\mathbf{Z}/m\mathbf{Z})^\times$ via $a \mapsto \sigma_a$, where σ_a is the automorphism sending ζ_m to ζ_m^a. The fractional part of a rational $x \in \mathbf{Q}$ is denoted $\{x\}$, and is defined as the unique rational in the interval $[0, 1)$ such that $\{x\} = x \mod \mathbf{Z}$; equivalently, $\{x\} = x - \lfloor x \rfloor$.

Definition 7.1 (The Stickelberger ideal)**.** For any integer $a \in \mathbf{Z}$, let

$$\theta(a) = \sum_{b \in (\mathbf{Z}/m\mathbf{Z})^\times} \left\{ -\frac{ab}{m} \right\} \sigma_b^{-1} \in \mathbf{Q}[G].$$

Let S' be the $\mathbf{Z}$-module generated by $\{\theta(a) \mid a \in \mathbf{Z}\}$ in $\mathbf{Q}[G]$. The *Stickelberger ideal* is defined as $S = \mathbf{Z}[G] \cap S'$. It is an ideal in $\mathbf{Z}[G]$, and we will refer to the *Stickelberger lattice* when S is considered as a $\mathbf{Z}$-module.

This is the definition from [Sin78], while some references (such as [Was12]) use the term *Stickelberger ideal* to refer to the smaller ideal $\mathbf{Z}[G] \cap \theta(1)\mathbf{Z}[G]$. Note that the definitions coincide when m is a power of a prime number. The Stickelberger ideal provides some class relations, thanks to the following theorem. A proof can be found in [Wei74].

Theorem 7.2 (Stickelberger's theorem)**.** *The Stickelberger ideal annihilates the ideal class group of K. In other words, for any ideal $\mathfrak{h}$ of $\mathcal{O}_K$ and any $s \in S$, the ideal $\mathfrak{h}^s$ is principal.*

7.1.2. Short generating vectors of the Stickelberger lattice. For any integer a, let $v_a = a\theta(1) - \theta(a) \in \mathbf{Q}[G]$.

Lemma 7.3. *The set $\{v_a \mid a = 2, \dots, m\}$ generates the Stickelberger lattice.*

Proof. Let L be the lattice generated by $\{v_a \mid a = 2, \dots, m\}$ in $\mathbf{Q}[G]$. A simple calculation shows that $v_a \in \mathbf{Z}[G]$ for any integer a, so $L \subseteq S$. Let γ be an arbitrary element of S. Since $\theta(0) = 0$, and $\theta(a) = \theta(b)$ for any integers a and b such that $a \equiv b \mod m$, we can write $\gamma = \sum_{a=1}^{m-1} x_a \theta(a)$ where the x_a's are integers. Now,

$$\begin{aligned}\gamma = \sum_{a=1}^{m-1} x_a \theta(a) &= \sum_{a=1}^{m-1} x_a \left(\sum_{b \in (\mathbf{Z}/m\mathbf{Z})^\times} \left\{ -\frac{ab}{m} \right\} \right) \sigma_b^{-1} \\ &= \sum_{b \in (\mathbf{Z}/m\mathbf{Z})^\times} \left(\sum_{a=1}^{m-1} x_a \left\{ -\frac{ab}{m} \right\} \right) \sigma_b^{-1}.\end{aligned}$$

Therefore, the coefficient of σ_b^{-1} in γ is $\sum_{a=1}^{m-1} x_a \left\{ -\frac{ab}{m} \right\}$, and it is an integer since γ is in the group ring $\mathbf{Z}[G]$, so the sum $\sum_{a=1}^{m-1} x_a a$ is divisible by m. Let q be the integer such that $\sum_{a=1}^{m-1} x_a a = qm$. We obtain

$$\gamma = \sum_{a=1}^{m-1} x_a \theta(a) = \sum_{a=1}^{m-1} x_a a\theta(1) + \sum_{a=1}^{m-1} x_a(\theta(a) - a\theta(1)) = qv_m - \sum_{a=2}^{m-1} x_a v_a \in L,$$

which concludes the proof. □

We are now ready to construct our set of short generators for S. Let $w_a = v_a - v_{a-1}$ for $a \in \{2, \dots, m\}$, and let

$$W = \{w_2, \dots, w_m\}.$$

Lemma 7.4. *The set W is a set of short generators of S. More precisely,*

(1) W generates the Stickelberger lattice S;
(2) For any $a \in \{2, \dots, m\}$, $w_a = \sum_{b \in (\mathbf{Z}/m\mathbf{Z})^\times} \epsilon_{a,b} \cdot \sigma_b^{-1}$, with $\epsilon_{a,b} \in \{0, 1\}$;
(3) For any $w \in W$, we have $\|w\| \leq \sqrt{\varphi(m)}$.

The second item essentially generalises [Sch10, Proposition 9.4] from prime conductors to arbitrary conductors.

Proof. Point 1 is a direct consequence of Lemma 7.3 and the construction of W. Point 3 follows from Point 2, so we focus on proving Point 2. Similarly to the proof of [Was12,

Lemma 6.9], we have

$$v_a = a\theta(1) - \theta(a) = \sum_{b\in(\mathbf{Z}/m\mathbf{Z})^\times} \left(a\left\{-\frac{b}{m}\right\} - \left\{-\frac{ab}{m}\right\}\right)\sigma_b^{-1} = \sum_{b\in(\mathbf{Z}/m\mathbf{Z})^\times} \left\lfloor a\left\{-\frac{b}{m}\right\}\right\rfloor \sigma_b^{-1},$$

using the identity $x\{y\} - \{xy\} = \lfloor x\{y\}\rfloor$ for any integer x and real number y, since this difference is an integer and the term $\{xy\}$ is in the range $[0, 1)$. It remains to rewrite $w_a = \sum_{b\in(\mathbf{Z}/m\mathbf{Z})^\times} \epsilon_{a,b}\sigma_b^{-1}$, where

$$\epsilon_{a,b} = \left\lfloor a\left\{-\frac{b}{m}\right\}\right\rfloor - \left\lfloor (a-1)\left\{-\frac{b}{m}\right\}\right\rfloor \leq \left\{-\frac{b}{m}\right\} + 1 < 2.$$

Therefore $\epsilon_{a,b} \in \{0, 1\}$ for all indices a and b. □

7.1.3. Class relations for the relative class group. We cannot directly use the Stickelberger ideal $S \subset \mathbf{Z}[G]$ as a lattice of class relations since it does not have full rank in $\mathbf{Z}[G]$ as a $\mathbf{Z}$-module (precisely, its $\mathbf{Z}$-rank is $\varphi(m)/2 + 1$ when $m \geq 2$). Indeed, if the lattice is not full rank, a given vector does not necessarily have a short representative modulo the lattice. To resolve this issue, we restrict our attention to the subgroup Cl_K^-.

Recall that $K^+ = \mathbf{Q}(\zeta_m + \zeta_m^{-1})$ is the maximal real subfield of K, with class group Cl_{K^+}, and Cl_K^- is the relative class group (the kernel of the relative norm map $N_{K/K^+} : \mathrm{Cl}_K \to \mathrm{Cl}_{K^+}$). By construction, the element $1+\tau \in \mathbf{Z}[G]$ annihilates Cl_K^-, so the action of $\mathbf{Z}[G]$ on Cl_K^- factors through the quotient ring

$$R = \mathbf{Z}[G]/(1 + \tau).$$

The ring R also has a geometric structure. Let $\pi : \mathbf{Z}[G] \to R$ be the natural projection. Let $B \subset G$ be any set of representatives of $G/\langle\tau\rangle$. Then, the projection $\pi(B)$ forms a $\mathbf{Z}$-basis of R. The induced isomorphism $R \cong \mathbf{Z}^{\varphi(m)/2}$ naturally induces an ℓ_1 and ℓ_2-norm on R, and these norms do not actually depend on the choice of B.

Lemma 7.5. *The projected Stickelberger lattice $\pi(S)$ has full rank $\varphi(m)/2$ in R.*

Proof. A generalisation due to Sinnott [Sin78] of a theorem from Iwasawa states that $(1 - \tau)S$ is of full rank in $(1 - \tau)\mathbf{Z}[G]$. We conclude by noting that the projection of $(1 - \tau)\mathbf{Z}[G]$ into R is itself of full rank. □

The set of elements $\pi(W)$ has full rank in R. One can easily deduce from Lemma 7.4 that $\|\pi(w)\| \leq 2\sqrt{\varphi(m)}$ for any $w \in W$, but we can show the following slightly stronger bound.

Lemma 7.6. *For any $w \in W$, we have $\|\pi(w)\| \leq \sqrt{\varphi(m)}$.*

Proof. Using the notation of Lemma 7.4, it is sufficient to show that for any $a \in \{2, \ldots, m\}$ and $b \in (\mathbf{Z}/m\mathbf{Z})^\times$, we have $\epsilon_{a,b} - \epsilon_{a,-b} \in \{-1, 1\}$. For $a = m$, we have $\epsilon_{a,b} = \epsilon_{a,-b} = 1$, so $\pi(w_m) = 0$. Suppose $a \neq m$. Then, since $ab/m \notin \mathbf{Z}$,

$$\left\lfloor a\left\{-\frac{b}{m}\right\}\right\rfloor = \left\lfloor a\left(1 - \left\{\frac{b}{m}\right\}\right)\right\rfloor = a + \left\lfloor -a\left\{\frac{b}{m}\right\}\right\rfloor = a - \left\lfloor a\left\{\frac{b}{m}\right\}\right\rfloor,$$

Then, $\epsilon_{a,b} - \epsilon_{a,-b} = 1 - 2\epsilon_{a,-b} \in \{-1, 1\}$. □

7.1.4. The close principal multiple problem in a $\mathbf{Z}[G]$-cycle of Cl_K^-. We now show how to exploit the previously constructed set W of short relations to reduce class representations. More precisely, for any large $\alpha \in \mathbf{Z}[G]$ we will find a short $\beta \in \mathbf{Z}[G]$ such that $C^\beta = C^\alpha$, for any class $C \in \mathrm{Cl}_K^-$. We rely on the following close vector algorithm.

Theorem 7.7. *There is an algorithm* Reduce *(Algorithm 7.1), that given $\alpha \in \mathbf{Z}[G]$, finds an element $\beta \in \mathbf{Z}[G]$ such that $\|\beta\|_1 \leq 0.5 \cdot \varphi(m)^{3/2}$, and $C^\alpha = C^\beta$ for any $C \in \mathrm{Cl}_K^-$, and runs in polynomial time in m and $\log(\|\alpha\|)$.*

Algorithm 7.1 Reduce(α): finds a reduction of α.

Require: An element $\alpha \in \mathbf{Z}[G]$.

Ensure: An element $\beta \in \mathbf{Z}[G]$ such that $\|\beta\|_1 \leq 0.5 \cdot \varphi(m)^{3/2}$, and $C^\alpha = C^\beta$ for any $C \in \mathrm{Cl}_K^-$.

1: Let W be the generating set of S as in Lemma 7.4;
2: $v \leftarrow \mathrm{CV}(\pi(\alpha), \pi(W))$; {close vector algorithm of Corollary 6.4}
3: $\gamma \leftarrow \pi(W) \cdot v$;
4: Write $\pi(\alpha) - \gamma = \sum_{\sigma \in B} a_\sigma \pi(\sigma)$ using the basis $\pi(B)$ of R;
5: $\beta \leftarrow \sum_{\sigma \in B} a_\sigma \sigma$;
6: **return** β.

Proof. Recall that $\pi : \mathbf{Z}[G] \to R$ is the canonical projection, W is the generating set of S as in Lemma 7.4, and $B \subset G$ is any set of representatives of $G/\langle\tau\rangle$. From Lemma 7.5, $\pi(W)$ has full rank in R. So the close vector algorithm from Corollary 6.4 finds an element $\gamma \in \pi(S)$ such that

$$\|\pi(\alpha) - \gamma\|_1 \leq \frac{\varphi(m)}{2} \cdot \max_{w \in W} \|\pi(w)\| \leq 0.5 \cdot \varphi(m)^{3/2}.$$

Then, the element β returned by Algorithm 7.1 satisfies

$$\|\beta\|_1 = \|\pi(\alpha) - \gamma\|_1 \leq 0.5 \cdot \varphi(m)^{3/2}.$$

Furthermore, for any $C \in \mathrm{Cl}_K^-$, Stickelberger's theorem implies that $C^\gamma = [\mathcal{O}_K]$, and therefore $C^\alpha = C^\beta$. □

Theorem 7.8 (Close principal multiple algorithm for $\mathbf{Z}[G]$-cycles of Cl_K^-)**.** *Let $\mathfrak{p}$ be an ideal such that $[\mathfrak{p}] \in \mathrm{Cl}_K^-$. There is an algorithm* ClosePrincipalMultiple$^-$ *(Algorithm 7.2) that given an element $\alpha \in \mathbf{Z}[G]$, finds an integral ideal $\mathfrak{b}$ such that $\mathfrak{p}^\alpha \mathfrak{b}$ is principal and*

$$N(\mathfrak{b}) = N(\mathfrak{p})^{O\left(\varphi(m)^{3/2}\right)},$$

and runs in polynomial time in m, $\log(N(\mathfrak{p}))$ and $\log(\|\alpha\|)$.

Remark 7.9. If one is given the ideal $\mathfrak{a} = \mathfrak{p}^\alpha \in \mathfrak{p}^{\mathbf{Z}[G]}$ instead of the element α, one could try to recover α by solving a discrete logarithm problem in the relative class group. This is doable in quantum polynomial time (see Proposition 6.9), but we choose to have α given in Theorem 7.8 to obtain a classical algorithm.

Algorithm 7.2 ClosePrincipalMultiple$^-(\mathfrak{p}, \alpha)$: solves CPM for the ideal $\mathfrak{p}^\alpha$.

Require: An ideal $\mathfrak{p}$ such that $[\mathfrak{p}] \in \mathrm{Cl}_K^-$, and an element $\alpha \in \mathbf{Z}[G]$.

Ensure: An integral ideal $\mathfrak{b}$ such that $\mathfrak{p}^\alpha\mathfrak{b}$ is principal and $N(\mathfrak{b}) = N(\mathfrak{p})^{O\left(\varphi(m)^{3/2}\right)}$.

1: $\beta \leftarrow \textsc{Reduce}(\alpha)$; {Algorithm 7.1}
2: Write $\beta = \sum_{\sigma\in G} b_\sigma \sigma$;
3: **for all** $\sigma \in G$ **do**
4: $\quad (b_\sigma^+, b_\sigma^-) \leftarrow \begin{cases} (b_\sigma, 0) \textbf{ if } b_\sigma \geq 0, \\ (0, -b_\sigma) \textbf{ otherwise}; \end{cases}$
5: **end for**
6: $\gamma \leftarrow \sum_{\sigma\in G}(\tau b_\sigma^+ + b_\sigma^-)\sigma$;
7: **return** $\mathfrak{b} = \mathfrak{p}^\gamma$.

Proof. Consider β, γ and $\mathfrak{b}$ as in Algorithm 7.2. From Theorem 7.7, we have the bound $\|\beta\|_1 \leq 0.5 \cdot \varphi(m)^{3/2}$, and $\mathfrak{p}^\alpha \sim \mathfrak{p}^\beta$. Since $[\mathfrak{p}] \in \mathrm{Cl}_K^-$, we have $\mathfrak{p}^{-1} \sim \mathfrak{p}^\tau$, so

$$\mathfrak{p}^\gamma \sim \mathfrak{p}^{\sum_{\sigma\in G}(\tau b_\sigma^+ + b_\sigma^-)\sigma} \sim \mathfrak{p}^{\sum_{\sigma\in G}(-b_\sigma^+ + b_\sigma^-)\sigma} \sim \mathfrak{p}^{-\alpha},$$

hence $\mathfrak{p}^\alpha\mathfrak{b}$ is principal. Since γ has only positive coefficients, the ideal $\mathfrak{b}$ is integral. Finally, $N(\mathfrak{b}) = N(\mathfrak{p})^{\|\gamma\|_1} = N(\mathfrak{p})^{O\left(\varphi(m)^{3/2}\right)}$. □

7.2. Finding short vectors in cyclotomic ideals

Let $\mathfrak{a}$ be an arbitrary ideal in the cyclotomic ring $\mathcal{O}_K$ of conductor m. In this section, we prove the following theorem.

Theorem 7.10 (Approx-SVP for cyclotomic ideals)**.** *Under the extended Riemann hypothesis (ERH) and Assumption 7.11, there is a quantum algorithm* IdealSVP *(Algorithm 7.5) that, when given an ideal $\mathfrak{a}$ in the cyclotomic ring of conductor m, finds an element in $\mathfrak{a}$ of Euclidean norm*

$$\exp\left(\tilde{O}\left(\sqrt{m}\right)\right) \cdot N(\mathfrak{a})^{1/\varphi(m)},$$

and runs in polynomial time in m, $h^+(m)$ and $\log(N(\mathfrak{a}))$. This element approximates SVP in $\mathfrak{a}$ with an approximation factor $\exp(\tilde{O}\left(\sqrt{m}\right))$.

The strategy is the following. Suppose that we have a set $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_d\}$ of ideals of norm $\mathrm{poly}(m)$ that generate the relative class group Cl_K^- as a $\mathbf{Z}[G]$-module.

(1) First, we find an (integral) ideal $\mathfrak{b}$ of small norm such that the class of $\mathfrak{a}\mathfrak{b}$ is in the relative class group Cl_K^-. This is done via a random walk in the class group in Section 7.2.1.
(2) Second, we find $\alpha_1, \ldots, \alpha_d \in \mathbf{Z}[G]$ such that $\mathfrak{a}\mathfrak{b} \sim \mathfrak{p}_1^{\alpha_1} \ldots \mathfrak{p}_d^{\alpha_d}$, and apply the results of Section 7.1 to find ideals $\mathfrak{b}_i \sim \mathfrak{p}_1^{-\alpha_1}$ such that $N(\mathfrak{b}_i) = \exp(\tilde{O}(m^{3/2}))$. This is done in Section 7.2.2.
(3) Finally, the ideal $\mathfrak{c} = \mathfrak{a}\mathfrak{b}\mathfrak{b}_1 \ldots \mathfrak{b}_d$ is principal. Applying the results of Section 6.5 allows to find an element $g \in \mathfrak{c} \subset \mathfrak{a}$ of norm $\exp(\tilde{O}(d\sqrt{m}))$. This is done in Section 7.2.3.

The first step assumes ERH, and the next two work unconditionally. Assumption 7.11 is a statement on the Galois-module structure of Cl_K^- which allows to take $d = \mathrm{polylog}(m)$, and obtain the targeted approximation factor $\exp(\tilde{O}\left(\sqrt{m}\right))$.

Assumption 7.11. *There are integers $d \leq \mathrm{polylog}(m)$ and $B \leq \mathrm{poly}(m)$ such that the following holds. Choose uniformly at random d prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_d$ among the finitely many ideals $\mathfrak{p}$ satisfying $N(\mathfrak{p}) \leq B$ and $[\mathfrak{p}] \in \mathrm{Cl}_K^-$. Then, the factor basis $\mathfrak{B} = \{\mathfrak{p}_i^\sigma \mid \sigma \in G, i = 1, \ldots, d\}$ generates Cl_K^- with probability at least $1/2$.*

This assumption is arguably new, and can be read as a strengthened version of the results of Chapter 4 on generators of subgroups of class groups. This assumption, and its justification, is the object of Section 7.3.

Note that for the algorithm of Theorem 7.10 to really be efficient, one would also require $h^+(m)$ to be polynomially bounded in m. This Assumption 7.13 is discussed in Section 7.2.1.2. Unlike the previous one, this assumption is a well-known question in algebraic number theory, and is related to important conjectures.

7.2.1. Random walk to the relative class group. As previously, let K^+ denote the maximal real subfield of K, and Cl_{K^+} the class group of K^+.

The core of the method to find a close principal multiple of an ideal $\mathfrak{a}$ works within the relative class group $\mathrm{Cl}_K^- \subset \mathrm{Cl}_K$. Therefore, as a first step, we need to "send" the ideal $\mathfrak{a} \in \mathrm{Cl}_K$ into this subgroup. More precisely, we want an integral ideal $\mathfrak{b}$ of small norm such that $\mathfrak{ab} \in \mathrm{Cl}_K^-$; the rest of the method then works with $\mathfrak{ab}$. Let $h_K = |\mathrm{Cl}_K|$ be the class number of K, and $h_K^- = |\mathrm{Cl}_K^-|$ its relative class number. The difficulty of this step is directly related to the index of Cl_K^- inside Cl_K, which is the real class number $h_K^+ = |\mathrm{Cl}_{K^+}|$ of K^+ (indeed, the relative norm map $N_{K/K^+} : \mathrm{Cl}_K \to \mathrm{Cl}_{K^+}$ induces the isomorphism $\mathrm{Cl}_{K^+} \cong \mathrm{Cl}_K/\mathrm{Cl}_K^-$), and is expected to be very small.

7.2.1.1. *The random walk algorithm.* For any $x > 0$, consider the set $\mathcal{S}_x$ of ideals in $\mathcal{O}_K$ of prime norm at most x, and let S_x be the multiset of its image in Cl_K. Let $\mathcal{G}_x$ denote the induced Cayley (multi)graph $\mathrm{Cay}(\mathrm{Cl}_K, S_x)$. From Corollary 3.20 (under ERH), for any $\varepsilon > 0$ there is a constant C and a bound

$$B = O\left((\varphi(m)\log(\Delta_K))^{2+\varepsilon}\right) = O\left((\varphi(m)^2\log(\varphi(m)))^{2+\varepsilon}\right)$$

such that any random walk in $\mathcal{G}_B$ of length at least $C\log(h_K)/\log\log(\Delta_K)$, for any starting point, lands in the subgroup Cl_K^- with probability at least $1/(2h_K^+)$.

A random walk of length $\ell = \lceil C\log(h_K)/\log\log(\Delta_K)\rceil = \tilde{O}(m)$ is a sequence $\mathfrak{p}_1, ..., \mathfrak{p}_\ell$ of ideals chosen independently, uniformly at random in $\mathcal{S}_B$, and their product $\mathfrak{b} = \prod \mathfrak{p}_i$ has a norm bounded by

$$N(\mathfrak{b}) = \prod_{i=1}^{\ell} N(\mathfrak{p}_i) \leq B^\ell = \exp(\mathrm{polylog}(m) \cdot \tilde{O}(\log h_K)) = \exp(\tilde{O}(m)).$$

If $[\mathfrak{a}]$ is the starting point of the random walk in the graph, the endpoint $[\mathfrak{ab}]$ falls in Cl_K^- with probability at least $1/(2h_K^+)$, and therefore an ideal $\mathfrak{b}$ such that $[\mathfrak{ab}] \in \mathrm{Cl}_K^-$ can be found in probabilistic polynomial time in h_K^+. Note that the quantum algorithm of Biasse and Song [BS16] for PIP allows to test the membership $[\mathfrak{ab}] \in \mathrm{Cl}_K^-$, simply by testing the principality of $N_{K/K^+}(\mathfrak{ab})$ as an ideal of $\mathcal{O}_K^+$.

The procedure is summarized as Algorithm 7.3, and the efficiency is stated below. Under ERH and Assumption 7.13, this procedure runs in polynomial time.

Lemma 7.12. *Assuming ERH, the quantum algorithm* WalkToCl$^-$ *(Algorithm 7.3) runs in expected time $O(h_K^+) \cdot \mathrm{poly}(m, \log N(\mathfrak{a}))$ and is correct.*

Algorithm 7.3 WalkToCl$^-(\mathfrak{a})$: random walk to Cl_K^-.

Require: An ideal $\mathfrak{a}$ in $\mathcal{O}_K$.
Ensure: An integral ideal $\mathfrak{b}$ such that $[\mathfrak{ab}] \in \mathrm{Cl}_K^-$ and $N(\mathfrak{b}) \leq \exp(\tilde{O}(m))$.
1: Define the bounds ℓ and B as in Section 7.2.1.1, with $\ell = \tilde{O}(m)$ and $B = \mathrm{poly}(m)$;
2: **repeat**
3: **for** $i = 1$ **to** ℓ **do**
4: Choose $\mathfrak{p}_i$ uniformly among the prime ideals of norm less than B;
5: **end for**
6: $\mathfrak{b} \leftarrow \prod_{i=1}^{\ell} \mathfrak{p}_i$;
7: **until** $N_{K/K^+}(\mathfrak{ab})$ is principal; {using the PIP algorithm of [BS16]}
8: **return** $\mathfrak{b}$.

7.2.1.2. *The real class number.* The time complexity of Algorithm 7.3 has a linear factor h_K^+ (the class number of the real subfield K^+). Assumption 7.13 below ensures that this factor is not a problem. For any integer m, let $h^+(m)$ be the class number of the maximal totally real subfield of the cyclotomic field of conductor m.

Assumption 7.13. *For any integer m, it holds that $h^+(m) \leq \mathrm{poly}(m)$.*

The literature on h_K^+ provides strong theoretical and computational evidence that it is indeed small enough. First, Buhler, Pomerance, Robertson [BPR04] formulate and argue in favor of the following conjecture, based on Cohen-Lenstra heuristics.

Conjecture 7.14 (Buhler, Pomerance, Robertson [BPR04])**.** *For all but finitely many pairs (ℓ, e), where ℓ is a prime and e is a positive integer, we have $h^+(\ell^{e+1}) = h^+(\ell^e)$.*

A stronger version for the case $\ell = 2$ was formulated by Weber.

Conjecture 7.15 (Weber's class number problem)**.** *For any e, $h^+(2^e) = 1$.*

A direct consequence of Conjecture 7.14 is that for fixed ℓ and increasing e, the quantity $h^+(\ell^e)$ is $O(1)$, implying that Assumption 7.13 holds over the class of cyclotomic fields of conductor a power of ℓ.

But even for increasing primes ℓ, the quantity $h^+(\ell)$ itself is also small: Schoof [Sch03] computed all the values of $h^+(\ell)$ for $\ell < 10,000$ (correct under heuristics of type Cohen-Lenstra, and Miller proved in [Mil15] its correctness under ERH at least for the primes $\ell \leq 241$). According to this table, for 75.3% of the primes $\ell < 10,000$ we have $h^+(\ell) = 1$ (matching Schoof's prediction of 71.3% derived from the Cohen-Lenstra heuristics). All the non-trivial values remain very small, as $h^+(\ell) \leq \ell$ for 99.75% of the primes.

7.2.2. Close principal multiple algorithm. Combining the random walk from the previous section, the close principal multiple algorithm in Cl_K^- from Section 7.1.4, and the quantum algorithms for class group computations discussed in Section 6.2.2, one can construct an algorithm for the general close principal multiple problem in $\mathcal{O}_K$.

Theorem 7.16 (Close principal multiple algorithm)**.** *Under ERH and Assumption 7.11, there is a quantum algorithm* ClosePrincipalMultiple *(Algorithm 7.4) that given an ideal $\mathfrak{a}$ in the cyclotomic ring of conductor m, finds an integral ideal $\mathfrak{b}$ such that $\mathfrak{ab}$ is principal and*

$$N(\mathfrak{b}) = \exp\left(\tilde{O}\left(m^{3/2}\right)\right),$$

and runs in polynomial time in m, $h^+(m)$ and $\log(N(\mathfrak{a}))$.

Algorithm 7.4 ClosePrincipalMultiple($\mathfrak{a}$): solves CPM for the ideal $\mathfrak{a}$.

Require: An ideal $\mathfrak{a}$ in $\mathcal{O}_K$.

Ensure: An integral ideal $\mathfrak{b}$ such that $\mathfrak{ab}$ is principal and $N(\mathfrak{b}) = \exp\left(\tilde{O}\left(m^{3/2}\right)\right)$.

1: Consider the two bounds $d = \text{polylog}(m)$ and $B = \text{poly}(m)$ from Assumption 7.11;
2: $\mathfrak{M} \leftarrow \{\mathfrak{p} \mid N(\mathfrak{p}) \leq B, [\mathfrak{p}] \in \mathrm{Cl}_K^-\}$;
3: Choose $\mathfrak{p}_1, \ldots, \mathfrak{p}_d$ uniformly at random in $\mathfrak{M}$;
4: $\mathfrak{B} \leftarrow \{\mathfrak{p}_i^\sigma \mid \sigma \in G, i = 1, \ldots, d\}$;
5: $\mathfrak{b}' \leftarrow$ WalkToCl$^-(\mathfrak{a})$; {Algorithm 7.3}
6: $(y_\mathfrak{q})_{\mathfrak{q}\in\mathfrak{B}} \leftarrow \mathrm{ClDL}_\mathfrak{B}(\mathfrak{ab}')$; {Proposition 6.9}
7: **for** $i = 1$ **to** d **do**
8: $\quad \alpha_i \leftarrow \sum_{\sigma\in G} y_{\mathfrak{p}_i^\sigma}\sigma \in \mathbf{Z}[G]$;
9: $\quad \mathfrak{b}_i \leftarrow$ ClosePrincipalMultiple$^-(\mathfrak{p}_i, \alpha_i)$; {Algorithm 7.2}
10: **end for**
11: $\mathfrak{b} \leftarrow \mathfrak{b}' \prod_{i=1}^d \mathfrak{b}_i$;
12: **return** $\mathfrak{b}$.

Proof. The running time of Algorithm 7.4 follows from Lemma 7.12, Proposition 6.9 and Theorem 7.8. Note that this algorithm might fail when the chosen $\mathfrak{B}$ does not generate Cl_K^-, but following Assumption 7.11, it will succeed after a constant expected number of trials. Let us prove that it is correct. The algorithm WalkToCl$^-$ outputs an integral ideal $\mathfrak{b}'$ such that $[\mathfrak{ab}'] \in \mathrm{Cl}_K^-$ and $N(\mathfrak{b}) \leq \exp(\tilde{O}(m))$. When $\mathfrak{B}$ generates Cl_K^-, algorithm $\mathrm{ClDL}_\mathfrak{B}$ finds a sequence of elements $\alpha_1, \ldots, \alpha_d \in \mathbf{Z}[G]$ such that $\mathfrak{ab}' \sim \prod_{i=1}^d \mathfrak{p}_i^{\alpha_i}$. Now, applying the algorithm from Theorem 7.8 to each $\mathfrak{p}_i^{\alpha_i}$, we obtain ideals $\mathfrak{b}_1, \ldots, \mathfrak{b}_d$ such that $\mathfrak{p}_i^{\alpha_i}\mathfrak{b}_i$ is principal and $N(\mathfrak{b}_i) = \exp\left(\tilde{O}\left(m^{3/2}\right)\right)$ for any $i = 1, \ldots, d$. It follows that the output $\mathfrak{b} = \mathfrak{b}' \prod_{i=1}^d \mathfrak{b}_i$ has the desired properties. □

7.2.3. Proof of Theorem 7.10. The algorithm is summarized in Algorithm 7.5. The running time and correctness follow from Theorem 6.18 and Theorem 7.16. □

Algorithm 7.5 IdealSVP($\mathfrak{a}$): finding mildly short vectors in the ideal $\mathfrak{a}$.

Require: An ideal $\mathfrak{a}$ in $\mathcal{O}_K$.

Ensure: An element $v \in \mathfrak{a}$ of norm $\|v\| \leq \exp\left(\tilde{O}\left(\sqrt{m}\right)\right) \cdot N(\mathfrak{a})^{1/\varphi(m)}$.

1: $\mathfrak{b} \leftarrow$ ClosePrincipalMultiple($\mathfrak{a}$); {Algorithm 7.4}
2: $v \leftarrow$ PrincipalIdealSVP($\mathfrak{b}$); {Algorithm 6.2}
3: **return** v.

7.3. Constructing small factor bases for the relative class group

To argue for Assumption 7.11, we prove (in Proposition 7.17) that if Cl_K^- can be generated by r ideal classes, then $r \cdot \text{polylog}(m)$ uniformly random classes in Cl_K^- will generate it.

Proposition 7.17. *Let K be a cyclotomic field of conductor m, with Galois group G and relative class group Cl_K^-. Let r be the minimal number of $\mathbf{Z}[G]$-generators of Cl_K^-. Let $\alpha \geq 1$ be a parameter, and s be any integer such that*

$$s \geq r(\log_2 \log_2(h_K^-) + \alpha)$$

(note that $\log_2 \log_2(h_K^-) \sim \log_2(\varphi(m))$*). Let* $x_1, \ldots, x_s$ *be* s *independent uniform elements of* Cl_K^-*. The probability that* $\{x_1, \ldots, x_s\}$ *generates* Cl_K^- *as a* $\mathbf{Z}[G]$*-module is at least* $\exp\left(-\frac{3}{2^\alpha}\right) = 1 - O(2^{-\alpha})$*.*

In other words, a set of $\Theta(r \log(\varphi(m)))$ random ideal classes in Cl_K^- will generate this $\mathbf{Z}[G]$-module with very good probability. This proposition is proven at the end of this section.

To justify Assumption 7.11, we first argue that r is as small as $\mathrm{polylog}(m)$. For the case $m = 2^e$, this can be argued by just looking at the value of $h^-(2^e)$ computed up to $e = 9$ in [Was12, Table 3]. These values are square-free, so Cl_K^- is $\mathbf{Z}$-cyclic and therefore $\mathbf{Z}[G]$-cyclic; in other words, $r = 1$. The case of prime conductors was also studied by Schoof [Sch98]: he proved that Cl_K^- is $\mathbf{Z}[G]$-cyclic for every prime conductor $m \leq 509$; again, $r = 1$. While it is unclear that this cyclicity should be the typical behavior asymptotically, it seems reasonable to assume that r remains as small as $\mathrm{polylog}(m)$, at least for a dense class of prime power conductors.

Once it is accepted that $r \leq \mathrm{polylog}(m)$, Assumption 7.11 simply assumes that Proposition 7.17 remains true when imposing that the random classes $g_1, \ldots, g_s$ are chosen as the classes of random ideals of small norm, i.e. $g_i = [\mathfrak{p}_i]$ where $N(\mathfrak{p}_i) \leq \mathrm{poly}(m)$. This restriction on the norms seems reasonable considering that we have proven in Chapter 4 that prime ideals of norm $\mathrm{poly}(m)$ are sufficient to generate Cl_K^-, assuming ERH and Assumption 7.13. More precisely, Theorem 4.16 implies that the relative class group Cl_K^- is generated by ideals of prime norm smaller than $(2.71 h_K^+ \log(\Delta_K) + 4.13)^2$.

We now show a series of results leading to the proof of Proposition 7.17.

Lemma 7.18. *Let* R *be a finite commutative local ring of cardinality* ℓ^n*, for some prime number* ℓ*. A set of* s *independent uniformly random elements in* R *generates* R *as an* R*-module with probability at least* $1 - \ell^{-s}$*.*

Proof. An element generates R if and only if it is invertible, meaning that it is not in the maximal ideal of R. This ideal is a fraction at most ℓ^{-1} of R, so an element does not generate R with probability at most ℓ^{-1}. Among s independent elements, the probability that none of them is a generator is at most ℓ^{-s}. □

Lemma 7.19. *Let* R *be a finite commutative local ring of cardinality* ℓ^n*, for some prime number* ℓ*. Let* M *be a cyclic* R*-module. A set of* s *independent uniformly random elements in* M *generates* M *with probability at least* $1 - \ell^{-s}$*.*

Proof. Let g be a generator of M, and consider the homomorphism $\varphi : R \to M : \alpha \mapsto \alpha g$. Let $x_1, \ldots, x_s$ be s independent uniformly random elements in M. For each i, let α_i be a uniformly random element of the coset $\varphi^{-1}(x_i)$. The elements α_i are independent and uniformly distributed in R, so from Lemma 7.18, they generate R with probability at least $1 - \ell^{-s}$. If the α_i's generate R, then the x_i's generate M, and we conclude. □

Lemma 7.20. *Let* R *be a finite commutative local ring of cardinality* ℓ^n*, for some prime number* ℓ*. Let* M *be an* R*-module, and let* r *be the smallest number of* R*-generators of* M*. A set of* s *independent uniformly random elements in* M *generates* M *with probability at least* $\left(1 - \ell^{-\lfloor s/r \rfloor}\right)^r$*.*

Proof. Proceed by induction on r. The case $r = 1$ is Lemma 7.19. Suppose that for any R-module M' generated by $r - 1$ elements, and any positive s', a set of s' random elements in M' generates M' with probability at least

$$\left(1 - \ell^{-\lfloor s'/(r-1) \rfloor}\right)^{r-1}.$$

Choose s independent uniformly random elements $x_1, \ldots, x_s$ in M, and let $t = \lfloor s/r \rfloor$. Let $g_1, \ldots, g_r$ be a generating set for M. The quotient $M/(Rg_r)$ is generated by $r-1$ elements, so the first $s-t$ random elements generate it with probability at least

$$\left(1 - \ell^{-\lfloor (s-t)/(r-1) \rfloor}\right)^{r-1} \geq \left(1 - \ell^{-\lfloor s/r \rfloor}\right)^{r-1}.$$

Now assume that these $s-t$ elements indeed generate $M/(Rg_r)$. It remains to show that adding the remaining t random elements allows to generate the full module M with probability at least $1-\ell^{-\lfloor s/r \rfloor}$. Let $N \subset M$ be the submodule of M generated by the first $s-t$ random elements. Observe that the module M/N is generated by g_r. Indeed, let m be an arbitrary element of M. Since $M/(Rg_r)$ is generated by N, there is an $n \in N$ such that $m + Rg_r = n + Rg_r$. This implies that there is an element $\alpha g_r \in Rg_r$ such that $m + N = \alpha g_r + N$, proving that M/N is generated by g_r. From Lemma 7.19, M/N is generated by the last t random elements with probability at least $1 - \ell^{-\lfloor s/r \rfloor}$. So M is generated by $x_1, \ldots, x_s$ with probability at least $\left(1 - \ell^{-\lfloor s/r \rfloor}\right)^r$. □

Theorem 7.21. *Let R be a finite commutative ring, M be a finite R-module of cardinality m, and r be the minimal number of R-generators of M. A set of s independent uniformly random elements in M generates M with probability at least $\left(1 - 2^{-\lfloor s/r \rfloor}\right)^{\log_2 m}$.*

Proof. The ring R decomposes as an internal direct sum $\bigoplus_{i=1}^{k} R_i$ of finite local subrings R_i. For each i, define $e_i \in R$ the idempotent which projects to the unity of R_i and to zero in all other components of the decomposition (then, $R_i = e_i R$). In particular, we have that $M = \bigoplus_i e_i M$, and $M_i = e_i M$ may be viewed as an R_i-module.

Let $x_1, \ldots, x_s$ be s independent uniformly random elements in M. They generate M as an R-module if and only if for any i, the projections $e_i x_1, \ldots, e_i x_s$ generate M_i as an R_i-module. Let p_i be the probability that $e_i x_1, \ldots, e_i x_s$ generate M_i, and let r_i be the minimal number of generators of R_i. From Lemma 7.20, p_i is at least $\left(1 - 2^{-\lfloor s/r_i \rfloor}\right)^{r_i}$. We have the two bounds $r_i \leq r$ and $r_i \leq \log_2 |M_i|$, and we deduce

$$p_i \geq \left(1 - 2^{-\lfloor s/r \rfloor}\right)^{\log_2 |M_i|}.$$

Therefore $x_1, \ldots, x_s$ generate M with probability at least

$$\prod_{i=1}^{k} p_i = \left(1 - 2^{-\lfloor s/r \rfloor}\right)^{\sum_i \log_2 |M_i|} = \left(1 - 2^{-\lfloor s/r \rfloor}\right)^{\log_2 m},$$

concluding the proof. □

Proof of Proposition 7.17. Note that a set of elements in Cl_K^- generates it as a $\mathbf{Z}[G]$-module if and only if it generates it as a $(\mathbf{Z}/h_K^-\mathbf{Z})[G]$-module. We deduce from Theorem 7.21 that $x_1, \ldots, x_s$ generate Cl_K^- with probability at least $(1 - 2^{-\lfloor s/r \rfloor})^{\log_2(h_K^-)}$. For any $0 < x \leq 1/2$, we have $\log(1-x) > -(3/2)x$. We have $2^{-\lfloor s/r \rfloor} \leq 2^{-\lfloor \alpha \rfloor} \leq 1/2$, so

$$\begin{aligned}\left(1 - 2^{-\lfloor s/r \rfloor}\right)^{\log_2(h_K^-)} &= \exp\left(\log_2(h_K^-) \log\left(1 - 2^{-\lfloor s/r \rfloor}\right)\right) \\ &\geq \exp\left(-\frac{3}{2}\log_2(h_K^-) 2^{-\lfloor s/r \rfloor}\right).\end{aligned}$$

With $s \geq r(\log_2 \log_2(h_K^-) + \alpha)$, we get $\lfloor s/r \rfloor \geq \log_2 \log_2(h_K^-) + \alpha - 1$ and

$$\left(1 - 2^{-\lfloor s/r \rfloor}\right)^{\log_2(h_K^-)} \geq \exp\left(-\frac{3}{2^\alpha}\right),$$

proving the proposition. □

FUTURE DIRECTIONS

Cryptology remains an inexhaustible source of challenging mathematical questions, and this thesis by no means closes the chapter on any of the three thematics presented.

Regarding the discrete logarithm problem in finite fields of small characteristic, we merely claim to have developed a better understanding of the fastest known heuristic algorithms. The problem of designing a fully provable quasi-polynomial time algorithm remains open, yet we hope that the new geometric understanding of the heuristic methods will help towards achieving this goal. Several other directions could as well be investigated, notably improving the running time of the algorithm: reducing the constants in the exponent, or, more ambitiously, reaching a polynomial complexity.

Mystery lingers around the structure of isogeny graphs in higher dimension, especially regarding the vertical structure. We managed to fully describe certain interesting subgraphs, and get sufficient information about local structures to clear the path to some noteworthy algorithmic applications, yet much remains to be done before we can claim a full understanding. One of the main obstacles seems to be the complexity of the set of orders in CM-fields of arbitrary degree, for which we do not know a complete classification. Advances in this classification problem would undoubtedly lead to new insights on isogeny graphs. In the meantime, the answer to certain questions might already be at closer reach. For instance, we have seen that a short random walk allows to reach a uniformly random abelian variety in a horizontal isogeny graph, and one can naturally ask if a similar process allows to uniformly randomise in the full isogeny graph. Such a process would allow to extend the random self-reducibility theorem from the horizontal graph to the full isogeny class (as is already known for elliptic curves).

In the third part, we have learnt that a quantum computer allows to find "mildly" short vectors in cyclotomic ideal lattices, at least heuristically. A few number-theoretic claims still keep the method from being fully rigorous. However, the extended Riemann hypothesis, the Galois-module structure of the class group, and the growth of the class number of totally real fields are notoriously hard problems, reaching far beyond our ideal lattice problems. Our best chance at eliminating some of the assumptions might be to adapt parts of the algorithm to circumvent the holes in our knowledge. Another worthwhile goal would be to improve the approximation factor. The length of the vector that the algorithm can recover is assuredly much smaller than what can be hoped for in generic lattices, but still too large for a definitive cryptanalytic impact. Finally, it should be emphasised that ideal lattices are not the ultimate goal: while an interesting cryptanalytic target, schemes directly based on the difficulty of Ideal-SVP are rare. The impact of the new methods on NTRU-type cryptosystems, or on the Ring-LWE problem remains uncertain.

BIBLIOGRAPHY

[Adl79] L. M. Adleman, *A subexponential algorithm for the discrete logarithm problem with applications to cryptography*, 20th Annual Symposium on Foundations of Computer Science – FOCS 1979, IEEE Computer Society, 1979, pp. 55–60.

[AH99] L. M. Adleman and M.-D. A. Huang, *Function field sieve method for discrete logarithms over finite fields*, Information and Computation **151** (1999), no. 1-2, 5–16.

[Ajt99] M. Ajtai, *Generating hard instances of the short basis problem*, Automata, Languages and Programming – ICALP 1999 (J. Wiedermann, P. van Emde Boas, and M. Nielsen, eds.), Lecture Notes in Computer Science, vol. 1644, 1999, pp. 1–9.

[Bab86] L. Babai, *On Lovász' lattice reduction and the nearest lattice point problem*, Combinatorica **6** (1986), no. 1, 1–13, Preliminary version in STACS 1985.

[Bac90] E. Bach, *Explicit bounds for primality testing and related problems*, Mathematics of Computation **55** (1990), no. 191, 355–380.

[Bac96] E. Bach, *Weil bounds for singular curves*, Applicable Algebra in Engineering, Communication and Computing **7** (1996), no. 4, 289–298.

[Bas63] H. Bass, *On the ubiquity of Gorenstein rings*, Mathematische Zeitschrift **82** (1963), no. 1, 8–28.

[BBBF18] D. Boneh, J. Bonneau, B. Bünz, and B. Fisch, *Verifiable delay functions*, to appear in Advances in Cryptology – CRYPTO 2018 (2018).

[BCHL16] J. W. Bos, C. Costello, H. Hisil, and K. Lauter, *Fast cryptography in genus 2*, Journal of Cryptology **29** (2016), no. 1, 28–60.

[BEF+17] J. Biasse, T. Espitau, P. Fouque, A. Gélin, and P. Kirchner, *Computing generator in cyclotomic integer rings, a subfield algorithm for the principal ideal problem in $L(1/2)$ and application to cryptanalysis of a FHE scheme*, Advances in Cryptology – EUROCRYPT 2017 (J. Coron and J. B. Nielsen, eds.), Lecture Notes in Computer Science, vol. 10210, Springer, 2017, pp. 60–88.

[BF14] J.-F. Biasse and C. Fieker, *Subexponential class group and unit group computation in large degree number fields*, LMS Journal of Computation and Mathematics **17** (2014), no. suppl. A, 385–403. MR 3240816

[BFT14] N. Bruin, E. V. Flynn, and D. Testa, *Descent via $(3,3)$-isogeny on Jacobians of genus 2 curves*, Acta Arithmetica **165** (2014), no. 3, 201–223.

[BGJT14] R. Barbulescu, P. Gaudry, A. Joux, and E. Thomé, *A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic*, Advances in Cryptology – EUROCRYPT 2014 (P. Q. Nguyen and E. Oswald, eds.), Lecture Notes in Computer Science, vol. 8441, Springer, 2014, pp. 1–16.

[BGL11] R. Bröker, D. Gruenewald, and K. Lauter, *Explicit CM theory for level 2-structures on abelian surfaces*, Algebra & Number Theory, **5–4** (2011), 495–528.

[Bia18] J. Biasse, *Approximate short vectors in ideal lattices of $\mathbf{Q}(\zeta_{p^e})$ with precomputation of the class group*, Selected Areas in Cryptography – SAC 2017 (C. Adams and

J. Camenisch, eds.), Lecture Notes in Computer Science, vol. 10719, 2018, pp. 374–393.

[Bis15] G. Bisson, *Computing endomorphism rings of abelian varieties of dimension two*, Mathematics of Computation **84** (2015), no. 294, 1977–1989.

[BJW17] E. H. Brooks, D. Jetchev, and B. Wesolowski, *Isogeny graphs of ordinary abelian varieties*, Research in Number Theory **3** (2017), no. 1, 28.

[BL94] J. Buchmann and H. W. Lenstra, Jr., *Approximating rings of integers in number fields*, Journal de Théorie des Nombres de Bordeaux **6** (1994), no. 2, 221–260.

[BL04] C. Birkenhake and H. Lange, *Complex abelian varieties*, Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen, Springer, 2004.

[BLS12] R. Bröker, K. Lauter, and A. V. Sutherland, *Modular polynomials via isogeny volcanoes*, Mathematics of Computation **81** (2012), no. 278, 1201–1231.

[BPR04] J. Buhler, C. Pomerance, and L. Robertson, *Heuristics for class numbers of prime-power real cyclotomic fields*,, High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams, Fields Inst. Commun., Amer. Math. Soc., 2004, pp. 149–157.

[BS96] E. Bach and J. P. Sorenson, *Explicit bounds for primes in residue classes*, Mathematics of Computation **65** (1996), 1717–1735.

[BS16] J.-F. Biasse and F. Song, *Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields*, Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms – SODA 2016, SIAM, 2016, pp. 893–902.

[BV11] Z. Brakerski and V. Vaikuntanathan, *Fully homomorphic encryption from Ring-LWE and security for key dependent messages*, Advances in Cryptology – CRYPTO 2011 (P. Rogaway, ed.), Lecture Notes in Computer Science, vol. 6841, Springer, 2011, pp. 505–524.

[CDPR16] R. Cramer, L. Ducas, C. Peikert, and O. Regev, *Recovering short generators of principal ideals in cyclotomic rings*, Advances in Cryptology – EUROCRYPT 2016 (M. Fischlin and J. Coron, eds.), Lecture Notes in Computer Science, vol. 9666, Springer, 2016, pp. 559–585.

[CDW17] R. Cramer, L. Ducas, and B. Wesolowski, *Short Stickelberger class relations and application to Ideal-SVP*, Advances in Cryptology – EUROCRYPT 2017 (J. Coron and J. B. Nielsen, eds.), Lecture Notes in Computer Science, vol. 10210, Springer, 2017, pp. 324–348.

[CE15] J.-M. Couveignes and T. Ezome, *Computing functions on Jacobians and their quotients*, LMS Journal of Computation and Mathematics **18** (2015), no. 1, 555–577.

[CGS14] P. Campbell, M. Groves, and D. Shepherd, *Soliloquy: A cautionary tale*, ETSI 2nd Quantum-Safe Crypto Workshop, 2014, Available at `http://docbox.etsi.org/Workshop/2014/201410_CRYPTO/S07_Systems_and_Attacks/S07_Groves_Annex.pdf`.

[CH10] J. Clark and U. Hengartner, *On the use of financial data as a random beacon*, Electronic Voting Technology Workshop / Workshop on Trustworthy Elections – USENIX EVT/WOTE '10 (D. W. Jones, J. Quisquater, and E. Rescorla, eds.), USENIX Association, 2010.

[CKL08] R. Carls, D. Kohel, and D. Lubicz, *Higher-dimensional 3-adic CM construction*, Journal of Algebra **319** (2008), no. 3, 971–1006.

[Cop84] D. Coppersmith, *Fast evaluation of logarithms in fields of characteristic two*, IEEE transactions on information theory **30** (1984), no. 4, 587–594.

[Cos11] R. Cosset, *Applications des fonctions thêta à la cryptographie sur courbes hyperelliptiques*, Ph.D. thesis, Loria, Nancy, 2011.

[CQ05] G. Cardona and J. Quer, *Field of moduli and field of definition for curves of genus 2*, Computational aspects of algebraic curves, Lecture Notes Series on Computing, vol. 13, World Sci. Publ., Hackensack, NJ, 2005, pp. 71–83.

[CR15] R. Cosset and D. Robert, *Computing (ℓ, ℓ)-isogenies in polynomial time on Jacobians of genus 2 curves*, Mathematics of Computation **84** (2015), no. 294, 1953–1975.

[CV04] C. Cornut and V. Vatsal, *Nontriviality of Rankin-Selberg L-functions and CM points*, Tech. report, 2004.

[Del69] P. Deligne, *Variétés abéliennes ordinaires sur un corps fini*, Inventiones mathematicae, vol. 8, Springer Berlin Heidelberg, 1969, pp. 238–243.

[DH76] W. Diffie and M. Hellman, *New directions in cryptography*, IEEE transactions on Information Theory **22** (1976), no. 6, 644–654.

[Die11] C. Diem, *On the discrete logarithm problem in elliptic curves*, Compositio Mathematica **147** (2011), no. 1, 75–104.

[DJRV16] A. Dudeanu, D. Jetchev, D. Robert, and M. Vuille, *Cyclic isogenies for abelian varieties with real multiplication*, preprint arXiv:1710.05147, 2016, `https://arxiv.org/abs/1710.05147`.

[DL08] I. Dolgachev and D. Lehavi, *On isogenous principally polarized abelian surfaces*, Curves and abelian varieties, Contemporary Mathematics, vol. 465, Amer. Math. Soc., 2008, pp. 51–69.

[DM02] E. N. D. Maisner, *Abelian surfaces over finite fields as Jacobians*, Experimental Mathematics **11** (2002), 321–337.

[DM15] L. Ducas and D. Micciancio, *FHEW: bootstrapping homomorphic encryption in less than a second*, Advances in Cryptology – EUROCRYPT 2015 (E. Oswald and M. Fischlin, eds.), Lecture Notes in Computer Science, vol. 9056, Springer, 2015, pp. 617–640.

[Dud16] A. Dudeanu, *Computational aspects of Jacobians of hyperelliptic curves*, Ph.D. thesis, EPFL, Lausanne, Switzerland, 2016.

[EG02] A. Enge and P. Gaudry, *A general framework for subexponential discrete logarithm algorithms*, Acta Arithmetica **102** (2002), 83–103.

[EH10] K. Eisenträger and S. Hallgren, *Algorithms for ray class groups and Hilbert class fields*, Proceedings of the Twenty-first Annual ACM-SIAM Symposium on Discrete Algorithms – SODA 2010 (Philadelphia, PA, USA) (M. Charikar, ed.), Society for Industrial and Applied Mathematics, 2010, pp. 471–483.

[EHKS14] K. Eisenträger, S. Hallgren, A. Kitaev, and F. Song, *A quantum algorithm for computing the unit group of an arbitrary degree number field*, Proceedings of the 46th Annual ACM Symposium on Theory of Computing – STOC 2014 (D. B. Shmoys, ed.), ACM, 2014, pp. 293–302.

[EL10] K. Eisenträger and K. Lauter, *A CRT algorithm for constructing genus 2 curves over finite fields*, Arithmetics, geometry, and coding theory (AGCT 2005), Séminaires et Congrès, vol. 21, Soc. Math. France, Paris, 2010, pp. 161–176.

[ES10] A. Enge and A. V. Sutherland, *Class invariants by the CRT method*, Algorithmic number theory, Lecture Notes in Computer Science, vol. 6197, Springer, Berlin, 2010, pp. 142–156.

[ET14] A. Enge and E. Thomé, *Computing class polynomials for abelian surfaces*, Experimental Mathematics **23** (2014), no. 2, 129–145.

[FL08] D. Freeman and K. Lauter, *Computing endomorphism rings of Jacobians of genus 2 curves over finite fields*, Algebraic geometry and its applications, Ser. Number Theory Appl., vol. 5, World Sci. Publ., Hackensack, NJ, 2008, pp. 29–66.

[Fly15] E. V. Flynn, *Descent via $(5, 5)$-isogeny on Jacobians of genus 2 curves*, Journal of Number Theory **153** (2015), 270–282.

[FM02] M. Fouquet and F. Morain, *Isogeny volcanoes and the SEA algorithm*, Algorithmic number theory, 5th International Symposium – ANTS-V (C. Fieker and D. R. Kohel, eds.), Lecture Notes in Computer Science, vol. 2369, Springer, Berlin, 2002, pp. 276–291.

[Fri89] E. Friedman, *Analytic formulas for the regulator of a number field*, Inventiones mathematicae **98** (1989), no. 3, 599–622.

[Gal99] S. Galbraith, *Constructing isogenies between elliptic curves over finite fields*, LMS Journal of Computation and Mathematics **2** (1999), 118–138.

[Gau07] P. Gaudry, *Fast genus 2 arithmetic based on theta functions*, Journal of Mathematical Cryptology **1** (2007), no. 3, 243–265.

[GGMZ13] F. Göloğlu, R. Granger, G. McGuire, and J. Zumbrägel, *On the function field sieve and the impact of higher splitting probabilities*, Advances in Cryptology – CRYPTO 2013 (R. Canetti and J. A. Garay, eds.), Lecture Notes in Computer Science, vol. 8043, Springer, 2013, pp. 109–128.

[GHK+06] P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler, and A. Weng, *The 2-adic CM method for genus 2 curves with application to cryptography*, Advances in Cryptology – ASIACRYPT 2006 (X. Lai and K. Chen, eds.), Lecture Notes in Computer Science, vol. 4284, Springer, 2006, pp. 114–129.

[GHS02] S. D. Galbraith, F. Hess, and N. P. Smart, *Extending the GHS Weil descent attack*, Advances in Cryptology – EUROCRYPT 2002 (L. R. Knudsen, ed.), Lecture Notes in Computer Science, vol. 2332, Springer, 2002, pp. 29–44.

[GKZ18] R. Granger, T. Kleinjung, and J. Zumbrägel, *On the discrete logarithm problem in finite fields of fixed characteristic*, Transactions of the American Mathematical Society **270** (2018), no. 5, 3129–3145.

[GL09] E. Goren and K. Lauter, *The distance between superspecial abelian varieties with real multiplication*, Journal of Number Theory **129** (2009), no. 6, 1562–1578.

[GN08] N. Gama and P. Q. Nguyen, *Finding short lattice vectors within Mordell's inequality*, Proceedings of the 40th annual ACM Symposium on Theory of Computing – STOC 2008 (C. Dwork, ed.), ACM, 2008, pp. 207–216.

[GW17] A. Gélin and B. Wesolowski, *Loop-abort faults on supersingular isogeny cryptosystems*, International Workshop on Post-Quantum Cryptography – PQCrypto 2017 (T. Lange and T. Takagi, eds.), Springer, 2017, pp. 93–106.

[Har77] R. Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52.

[How95] E. W. Howe, *Principally polarized ordinary abelian varieties over finite fields*, Transactions of the American Mathematical Society **347** (1995), no. 7, 2361–2401.

[HR82] M. E. Hellman and J. M. Reyneri, *Fast computation of discrete logarithms in $GF(q)$*, Advances in Cryptology – CRYPTO '82 (D. Chaum, R. L. Rivest, and A. T. Sherman, eds.), Plenum Press, New York, 1982, pp. 3–13.

[IK04] H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications, no. v. 53, American Mathematical Society, 2004.

[IT14] S. Ionica and E. Thomé, *Isogeny graphs with maximal real multiplication*, preprint, Jul. 2014, `https://arxiv.org/pdf/1407.6672v1.pdf`.

[JD11] D. Jao and L. De Feo, *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies*, International Workshop on Post-Quantum Cryptography – PQCrypto 2011 (B. Yang, ed.), 2011, pp. 19–34.

[JMV05] D. Jao, S. D. Miller, and R. Venkatesan, *Do all elliptic curves of the same order have the same difficulty of discrete log?*, Advances in Cryptology – ASIACRYPT 2005 (B. K. Roy, ed.), Lecture Notes in Computer Science, vol. 3788, Springer, 2005, pp. 21–40.

[JMV09] D. Jao, S. D. Miller, and R. Venkatesan, *Expander graphs based on GRH with an application to elliptic curve cryptography*, Journal of Number Theory **129** (2009), no. 6, 1491–1504.

[Jou13] A. Joux, *A new index calculus algorithm with complexity $L(1/4 + o(1))$ in small characteristic*, Selected Areas in Cryptography – SAC 2013 (T. Lange, K. E. Lauter, and P. Lisonek, eds.), Lecture Notes in Computer Science, vol. 8282, Springer, 2013, pp. 355–379.

[JT15] C. U. Jensen and A. Thorup, *Gorenstein orders*, Journal of Pure and Applied Algebra **219** (2015), no. 3, 551–562.

[JW18] D. Jetchev and B. Wesolowski, *Horizontal isogeny graphs of ordinary abelian varieties and the discrete logarithm problem*, Acta Arithmetica (2018), in press.

[Kob87] N. Koblitz, *Elliptic curve cryptosystems*, Mathematics of computation **48** (1987), no. 177, 203–209.

[Koh96] D. Kohel, *Endomorphism rings of elliptic curves over finite fields*, Ph.D. thesis, University of California, Berkeley, 1996.

[Kra22] M. Kraïtchik, *Théorie des nombres*, Gauthier, Villars, 1922.

[Kuč92] R. Kučera, *On bases of the Stickelberger ideal and of the group of circular units of a cyclotomic field*, Journal of Number Theory **40** (1992), no. 3, 284–316.

[KW18] T. Kleinjung and B. Wesolowski, *A new perspective on the powers of two descent for discrete logarithms in finite fields*, Thirteenth Algorithmic Number Theory Symposium – ANTS-XIII, 2018, proceedings to appear in the Open Book Series, Mathematical Sciences Publishers.

[LD15] C. Lv and Y. Deng, *On orders in number fields: Picard groups, ring class fields and applications*, Science China Mathematics **58** (2015), no. 8, 1627–1638.

[Len91] H. W. Lenstra, Jr., *Finding isomorphisms between finite fields*, Mathematics of Computation **56** (1991), no. 193, 329–347.

[LLL82] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász, *Factoring polynomials with rational coefficients*, Mathematische Annalen **261** (1982), no. 4, 515–534.

[LLS15] Y. Lamzouri, X. Li, and K. Soundararajan, *Conditional bounds for the least quadratic non-residue and related problems*, Mathematics of Computation **84** (2015), no. 295, 2391–2412.

[LM06] V. Lyubashevsky and D. Micciancio, *Generalized compact knapsacks are collision resistant*, Automata, Languages and Programming – ICALP 2006 (part II) (M. Bugliesi, B. Preneel, V. Sassone, and I. Wegener, eds.), 2006, pp. 144–155.

[LMO79] J. Lagarias, H. Montgomery, and A. Odlyzko, *A bound for the least prime ideal in the Chebotarev density theorem*, Inventiones mathematicae **54** (1979), 271–296.

[LO77] J. Lagarias and A. Odlyzko, *Effective versions of the Chebotarev density theorem*, Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), Academic Press, London, 1977, pp. 409–464.

[LPR13] V. Lyubashevsky, C. Peikert, and O. Regev, *On ideal lattices and learning with errors over rings*, Journal of the ACM **60** (2013), no. 6, 43:1–43:35, Preliminary version in EUROCRYPT 2010.

[LR12a] K. Lauter and D. Robert, *Improved CRT algorithm for class polynomials in genus* 2, Tenth Algorithmic Number Theory Symposium – ANTS-X (E. W. Howe and K. S. Kedlaya, eds.), The Open Book Series, vol. 1, Mathematical Sciences Publisher, 2012, pp. 437–461.

[LR12b] D. Lubicz and D. Robert, *Computing isogenies between abelian varieties*, Compositio Mathematica **148** (2012), no. 5, 1483–1515.

[LS15] A. Langlois and D. Stehlé, *Worst-case to average-case reductions for module lattices*, Designs, Codes and Cryptography **75** (2015), no. 3, 565–599.

[LW17] A. K. Lenstra and B. Wesolowski, *Trustworthy public randomness with sloth, unicorn, and trx*, International Journal of Applied Cryptography **3** (2017), no. 4, 330–343.

[Mar18] C. Martindale, *Isogeny graphs, modular polynomials, and applications*, Ph.D. thesis, Universiteit Leiden, 2018.

[Mer78] R. C. Merkle, *Secure communications over insecure channels*, Communications of the ACM **21** (1978), no. 4, 294–299.

[Mes91] J.-F. Mestre, *Construction de courbes de genre* 2 *à partir de leurs modules*, Effective methods in algebraic geometry (Castiglioncello, 1990), Progress in Mathematics, vol. 94, Birkhäuser Boston, Boston, MA, 1991, pp. 313–334.

[Mic07] D. Micciancio, *Generalized compact knapsacks, cyclic lattices, and efficient one-way functions*, Computational Complexity **16** (2007), no. 4, 365–411, Preliminary version in FOCS 2002.

[Mil75] J. C. P. Miller, *On factorisation, with a suggested new approach*, Mathematics of Computation **29** (1975), no. 129, 155–172.

[Mil86a] V. S. Miller, *Use of elliptic curves in cryptography*, Advances in Cryptology – CRYPTO '85 (H. C. Williams, ed.), Lecture Notes in Computer Science, vol. 218, Springer, 1986, pp. 417–426.

[Mil86b] J. S. Milne, *Abelian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 103–150.

[Mil15] J. C. Miller, *Real cyclotomic fields of prime conductor and their class numbers*, Mathematics of Computation **84** (2015), no. 295, 2459–2469.

[Mum66] D. Mumford, *On the equations defining abelian varieties. I*, Inventiones mathematicae **1** (1966), 287–354.

[MW68] J. C. P. Miller and A. E. Western, *Tables of indices and primitive roots*, Published for the Royal Society at the University Press Cambridge, 1968.

[Nak09] S. Nakamoto, *Bitcoin: A peer-to-peer electronic cash system*, 2009, `http://bitcoin.org/bitcoin.pdf`.

[NS99] J. Neukirch and N. Schappacher, *Algebraic number theory*, Grundlehren der mathematischen Wissenschaften, Springer, Berlin, New York, Barcelona, 1999.

[Odl90] A. M. Odlyzko, *Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: a survey of recent results*, Journal de théorie des nombres de Bordeaux **2** (1990), no. 1, 119–141.

[PGF98] D. Panario, X. Gourdon, and P. Flajolet, *An analytic approach to smooth polynomials over finite fields*, Algorithmic Number Theory: 3rd International Symposium – ANTS-III (J. P. Buhler, ed.), Springer Berlin Heidelberg, 1998, pp. 226–236.

[PH78] S. Pohlig and M. Hellman, *An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance*, IEEE Transactions on information Theory **24** (1978), no. 1, 106–110.

[Pie16] C. Pierrot, *Le logarithme discret dans les corps finis*, Ph.D. thesis, Paris 6, UPMC, Sorbonne-Universités, 2016.

[Pol78] J. M. Pollard, *Monte Carlo methods for index computation mod p*, Mathematics of Computation **32** (1978), 918–924.

[Pom87] C. Pomerance, *Fast, rigorous factorization and discrete logarithm algorithms*, Discrete Algorithms and Complexity (D. S. Johnson, T. Nishizeki, A. Nozaki, and H. S. Wilf, eds.), Academic Press, 1987, pp. 119–143.

[PR06] C. Peikert and A. Rosen, *Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices*, Theory of Cryptography Conference – TCC (S. Halevi and T. Rabin, eds.), 2006, pp. 145–166.

[PW18] C. Pierrot and B. Wesolowski, *Malleability of the blockchain's entropy*, Cryptography and Communications **10** (2018), no. 1, 211–233.

[Reg09] O. Regev, *On lattices, learning with errors, random linear codes, and cryptography*, Journal of the ACM **56** (2009), no. 6, 1–40, Preliminary version in STOC 2005.

[Ric37] F. Richelot, *De transformatione integralium Abelianorum primi ordinis commentatio*, Journal für die reine und angewandte Mathematik **16** (1837), 221–284.

[Rob10] D. Robert, *Fonctions thêta et applications à la cryptologie*, Ph.D. thesis, Université Henri Poincaré - Nancy I, 2010.

[RS62] B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois Journal of Mathematics **6** (1962), no. 1, 64–94.

[RSW96] R. L. Rivest, A. Shamir, and D. A. Wagner, *Time-lock puzzles and timed-release crypto*, 1996.

[Sat00] T. Satoh, *The canonical lift of an ordinary elliptic curve over a finite field and its point counting*, Journal of the Ramanujan Mathematical Society **15** (2000), no. 4, 247–270.

[Sch87] C.-P. Schnorr, *A hierarchy of polynomial time lattice basis reduction algorithms*, Theoretical Computer Science **53** (1987), 201–224.

[Sch95] R. Schoof, *Counting points on elliptic curves over finite fields*, Journal de Théorie des Nombres de Bordeaux **7** (1995), no. 1, 219–254.

[Sch98] R. Schoof, *Minus class groups of the fields of the l-th roots of unity*, Mathematics of Computation **67** (1998), no. 223, 1225–1245.

[Sch03] R. Schoof, *Class numbers of real cyclotomic fields of prime conductor*, Mathematics of computation **72** (2003), no. 242, 913–937.

[Sch10] R. Schoof, *Catalan's conjecture*, Springer Science & Business Media, 2010.

[Sho97] P. W. Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM Journal on Computing **26** (1997), no. 5, 1484–1509.

[Sin78] W. Sinnott, *On the Stickelberger ideal and the circular units of a cyclotomic field*, Annals of Mathematics **108** (1978), no. 1, 107–134.

[Smi08] B. Smith, *Isogenies and the discrete logarithm problem in jacobians of genus 3 hyperelliptic curves*, Advances in Cryptology – EUROCRYPT 2008 (N. P. Smart, ed.), Lecture Notes in Computer Science, vol. 4965, Springer, 2008, pp. 163–180.

[Smi12] B. Smith, *Computing low-degree isogenies in genus 2 with the Dolgachev-Lehavi method*, Arithmetic, geometry, cryptography and coding theory, Contemporary Mathematics, vol. 574, Amer. Math. Soc., 2012, pp. 159–170.

[SSTX09] D. Stehlé, R. Steinfeld, K. Tanaka, and K. Xagawa, *Efficient public key encryption based on ideal lattices*, Advances in Cryptology – ASIACRYPT 2009 (M. Matsui, ed.), Lecture Notes in Computer Science, vol. 5912, Springer, 2009, pp. 617–635.

[ST61] G. Shimura and Y. Taniyama, *Complex multiplication of abelian varieties and its applications to number theory*, Publications of the Mathematical Society of Japan, vol. 6, The Mathematical Society of Japan, Tokyo, 1961.

[ST68] J.-P. Serre and J. Tate, *Good reduction of abelian varieties*, Annals of Mathematics (2) **88** (1968), 492–517.

[Str10] M. Streng, *Complex multiplication of abelian surfaces*, Ph.D. thesis, Universiteit Leiden, 2010.

[Sut11] A. V. Sutherland, *Computing Hilbert class polynomials with the Chinese remainder theorem*, Mathematics of Computation **80** (2011), no. 273, 501–538.

[Sut12] A. V. Sutherland, *Accelerating the CM method*, LMS Journal of Computation and Mathematics **15** (2012), 172–204.

[Tat66] J. Tate, *Endomorphisms of abelian varieties over finite fields*, Inventiones mathematicae **2** (1966), no. 2, 134–144.

[Tat71] J. Tate, *Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda)*, Séminaire Bourbaki vol. 1968/69 Exposés 347-363, Springer, 1971, pp. 95–110.

[Vél71] J. Vélu, *Isogénies entre courbes elliptiques*, Comptes rendus de l'Académie des Sciences, Séries A-B **273** (1971), A238–A241.

[VOW99] P. C. Van Oorschot and M. J. Wiener, *Parallel collision search with cryptanalytic applications*, Journal of cryptology **12** (1999), no. 1, 1–28.

[vW99] P. van Wamelen, *Examples of genus two CM curves defined over the rationals*, Mathematics of Computation **68** (1999), no. 225, 307–320.

[VZGP01] J. Von Zur Gathen and D. Panario, *Factoring polynomials over finite fields: a survey*, Journal of Symbolic Computation **31** (2001), no. 1-2, 3–17.

[Wan97] D. Wan, *Generators and irreducible polynomials over finite fields*, Mathematics of Computation **66** (1997), no. 219, 1195–1212.

[Was12] L. C. Washington, *Introduction to cyclotomic fields*, vol. 83, Springer Science & Business Media, 2012.

[Wat69] W. C. Waterhouse, *Abelian varieties over finite fields*, Annales scientifiques de l'École Normale Supérieure **2** (1969), no. 4, 521–560 (eng).

[Wei74] A. Weil, *Sommes de Jacobi et caractères de Hecke*, Nachrichten der Akademie der Wissenschaften in Göttingen, 2, Mathematisch-Physikalische Klasse, Vandenhoeck & Ruprecht, 1974.

[Wen03] A. Weng, *Constructing hyperelliptic curves of genus 2 suitable for cryptography*, Mathematics of Computation **72** (2003), no. 241, 435–458 (electronic).

[Wes14] B. Wesolowski, *Walking on isogeny graphs of genus 2 hyperelliptic curves*, Master's thesis, EPFL, Lausanne, Switzerland, 2014.

[Wes18a] B. Wesolowski, *Efficient verifiable delay functions*, IACR Cryptology ePrint Archive, Report 2018/623, 2018, `https://eprint.iacr.org/2018/623`, submitted for publication.

[Wes18b] B. Wesolowski, *Generating subgroups of ray class groups with small prime ideals*, Thirteenth Algorithmic Number Theory Symposium – ANTS-XIII, 2018, proceedings to appear in the Open Book Series, Mathematical Sciences Publishers.

[Wie86] D. Wiedemann, *Solving sparse linear equations over finite fields*, IEEE transactions on information theory **32** (1986), no. 1, 54–62.

INDEX

BENJAMIN **WESOLOWSKI**

benjamin.wesolowski@alumni.epfl.ch
www.bweso.com
French citizenship

My interests revolve around the various facets of **cryptography**, with a particular focus on cryptologic algorithms related to **number theory** and **algebraic geometry**. Another aspect of my work relates to randomness and the **blockchain** technology.

EDUCATION

2014 – 2018 **PhD in Computer and Communication Sciences**
École Polytechnique Fédérale de Lausanne (EPFL), Laboratory for Cryptologic Algorithms, Switzerland
- Advisors: Arjen K. Lenstra and Robert Granger
- Thesis title: *Arithmetic and geometric structures in cryptography*

2012 – 2014 **Master of Science in Mathematics, Minor in Information Security**
EPFL, thesis at the University of California, Berkeley, USA
- Thesis advisors: Kenneth A. Ribet (UC Berkeley) and Dimitar Jetchev (EPFL)
- Thesis title: *Walking on isogeny graphs of hyperelliptic curves of genus 2*
- Best average in this section, 3rd (out of 872) best average for complete Master studies at EPFL, 2014

2009 – 2012 **Bachelor's degree in Mathematics**, EPFL

EXPERIENCE

2014 – 2018 **Teaching assistant**, EPFL
- Project supervision (bachelor and master students)
- Managing, designing, supervising exercise sessions for *Advanced information, computation, communication*, for *Analysis*, and for *Global issues: communication*

Jul – Aug 2014 **Research engineer**, Institute for Information and Communication Technologies, HEIG-VD
- Design, proof, and implementation of a new efficient pairing-based broadcast encryption scheme

Feb – Jun 2014 **Visiting student researcher**, University of California, Berkeley
- Study of isogeny graphs of abelian surfaces, applications to hyperelliptic curve cryptography

2010 – 2014 **Student assistant**, EPFL
- Assistant for exercise sessions in topology, linear algebra, C and C++ programming

2013 **Administrative assistant**, EPFL

AWARDS

Teaching Assistant Award 2017, EPFL

Doctoral EDIC Fellowship 2014, EPFL

Kudelski Prize 2014, Kudelski Group
"For a Master Project having significantly contributed to the field of cryptography and information systems security"

Douchet Prize 2014, EPFL
Best Master average in the Mathematics section at EPFL

EPFL Prize 2014, EPFL
3rd (out of 872) best average mark for complete Master studies at EPFL

Undergraduate Awards 2013, Dublin, Ireland
Highly commended for the essay "*Lifting braids : from geometric braids to braid groups*" (2012)

PUBLICATIONS

9 articles in peer-reviewed journals or international conferences with published proceedings

Horizontal isogeny graphs of ordinary abelian varieties and the discrete logarithm problem
With Dimitar Jetchev
Acta Arithmetica (in press)

A new perspective on the powers of two descent for discrete logarithms in finite fields
With Thorsten Kleinjung
ANTS-XIII, Thirteenth Algorithmic Number Theory Symposium (2018)

Generating subgroups of ray class groups with small prime ideals
ANTS-XIII, Thirteenth Algorithmic Number Theory Symposium (2018)

Isogeny graphs of ordinary abelian varieties
With Ernest Hunter Brooks and Dimitar Jetchev
Research in Number Theory (2017)

Loop-abort faults on supersingular isogeny cryptosystems
With Alexandre Gélin
PQCrypto 2017

Short Stickelberger class relations and application to Ideal-SVP
With Ronald Cramer and Léo Ducas
⋆ Honorable mention
Eurocrypt 2017

Trustworthy public randomness with sloth, unicorn, and trx
With Arjen K. Lenstra
International Journal of Applied Cryptography (2016)

Malleability of the blockchain's entropy
With Cécile Pierrot
Cryptography and Communications (2018)

Ciphertext-policy attribute-based broadcast encryption with small keys
With Pascal Junod
ICISC 2015

2 articles in international workshops

Trust, and public entropy: a unicorn hunt
NIST Workshop on Random Bit Generation (2016)

A random zoo: sloth, unicorn and trx
NIST Workshop on Elliptic Curve Cryptography Standards (2016)

1 preprint currently under review

Efficient verifiable delay functions
Cryptology ePrint Archive, Report 2018/623 (2018)

SCIENTIFIC COMMUNICATION

10 presentations in conferences and workshops

An efficient verifiable delay function (invited)
Ethereum Foundation and Stanford Center for Blockchain Research workshop at Stanford (USA, 2018)

A new perspective on the powers of two descent for discrete logarithms in finite fields
ANTS-XIII, Thirteenth Algorithmic Number Theory Symposium (USA, 2018)

Generating subgroups of ray class groups with small prime ideals
ANTS-XIII, Thirteenth Algorithmic Number Theory Symposium (USA, 2018)

Short Stickelberger class relations and application to Ideal-SVP
Eurocrypt 2017 (France, 2017)

Isogeny graphs of ordinary abelian varieties (invited)
⋆ Best presentation award
ECC 2017, 21st Workshop on Elliptic Curve Cryptography (The Netherlands, 2017)

Graphes d'isogénies de variétés abéliennes ordinaires
Journées Codage et Cryptographie (France, 2017)

Malleability of the blockchain's entropy
ArcticCrypt 2016 (Norway, 2016)

Trust, and public entropy: a unicorn hunt
NIST Workshop on Random Bit Generation (USA , 2016)

A random zoo: sloth, unicorn and trx
Journées Codage et Cryptographie (France, 2015)

A random zoo: sloth, unicorn and trx
NIST Workshop on Elliptic Curve Cryptography Standards (USA, 2015)

6 talks at seminars

Horizontal isogeny graphs of ordinary abelian varieties and the discrete logarithm problem
Séminaire de Cryptographie, Rennes (France, 2018)

Mildly short vectors in cyclotomic ideal lattices in quantum polynomial time
CARAMBA seminar, Nancy (France, 2018)

Isogeny graphs of ordinary abelian varieties
LFANT seminar, Bordeaux (France, 2017)

Randomness on the blockchain
RISC seminars, CWI Cryptology Group, Amsterdam (The Netherlands, 2016)

A random zoo: sloth, unicorn and trx
ALMASTY seminars, Université Pierre et Marie Curie, Paris (France, 2015)

Random self-reducibility of the discrete logarithm problem in genus 2
LACAL@RISC Seminar on Cryptologic Algorithms, CWI Amsterdam (The Netherlands, 2015)

COMMUNITY SERVICE

Reviewing for journals and conferences:

- PKC 2018
- Journal of mathematical cryptology (2018)
- Mathcrypt 2018
- Asiacrypt 2017
- QCrypt 2017
- Eurocrypt 2017
- Indocrypt 2016
- Financial cryptography 2016
- Asiacrypt 2015

SKILLS

Languages: french (native language), english (fluent, TOEIC 945/990)

Computer languages:

- Daily use: C, Sage (Python), Magma, LaTeX
- Acquainted with: C++, Java, Scala, PHP, HTML/CSS

REFEREES

Prof. **Arjen K. Lenstra** (PhD director), EPFL
akl@epfl.ch

Dr. **Robert Granger** (PhD co-director)
robbiegranger@gmail.com

Prof. **Ronald Cramer**, CWI, Leiden University
cramer@cwi.nl

Prof. **Dimitar Jetchev**, EPFL
dimitar.jetchev@epfl.ch