THE UNIVERSITY OF
WARWICK

Library Declaration and Deposit Agreement

1. STUDENT DETAILS

Please complete the following:

Full name: ....CHARLOTTE LUCILE TURNER...............

University ID number: ....0866921...

2. THESIS DEPOSIT

2.1 I understand that under my registration at the University, I am required to deposit my thesis with the University in BOTH hard copy and in digital format. The digital version should normally be saved as a single pdf file.

2.2 The hard copy will be housed in the University Library. The digital version will be deposited in the University's Institutional Repository (WRAP). Unless otherwise indicated (see 2.3 below) this will be made openly accessible on the Internet and will be supplied to the British Library to be made available online via its Electronic Theses Online Service (EThOS) service.
[At present, theses submitted for a Master's degree by Research (MA, MSc, LLM, MS or MMedSci) are not being deposited in WRAP and not being made available via EthOS. This may change in future.]

2.3 In exceptional circumstances, the Chair of the Board of Graduate Studies may grant permission for an embargo to be placed on public access to the hard copy thesis for a limited period. It is also possible to apply separately for an embargo on the digital version. (Further information is available in the *Guide to Examinations for Higher Degrees by Research.*)

2.4 *If you are depositing a thesis for a Master's degree by Research, please complete section (a) below. For all other research degrees, please complete both sections (a) and (b) below:*

(a) Hard Copy

I hereby deposit a hard copy of my thesis in the University Library to be made publicly available to readers (please delete as appropriate) ~~EITHER~~ immediately ~~OR after an embargo period~~ of .... ~~months/years as agreed by the Chair of the Board of Graduate Studies~~.

I agree that my thesis may be photocopied. YES / ~~NO~~ *(Please delete as appropriate)*

(b) Digital Copy

I hereby deposit a digital copy of my thesis to be held in WRAP and made available via EThOS.

Please choose one of the following options:

EITHER My thesis can be made publicly available online. YES / ~~NO~~ *(Please delete as appropriate)*

OR My thesis can be made publicly available only after.....[date] (Please give date)
~~YES~~ / NO *(Please delete as appropriate)*

OR My full thesis cannot be made publicly available online but I am submitting a separately identified additional, abridged version that can be made available online.
~~YES~~ / NO *(Please delete as appropriate)*

OR My thesis cannot be made publicly available online. ~~YES~~ / NO *(Please delete as appropriate)*

3. **GRANTING OF NON-EXCLUSIVE RIGHTS**

Whether I deposit my Work personally or through an assistant or other agent, I agree to the following:

Rights granted to the University of Warwick and the British Library and the user of the thesis through this agreement are non-exclusive. I retain all rights in the thesis in its present version or future versions. I agree that the institutional repository administrators and the British Library or their agents may, without changing content, digitise and migrate the thesis to any medium or format for the purpose of future preservation and accessibility.

4. **DECLARATIONS**

(a) I DECLARE THAT:

- I am the author and owner of the copyright in the thesis and/or I have the authority of the authors and owners of the copyright in the thesis to make this agreement. Reproduction of any part of this thesis for teaching or in academic or other forms of publication is subject to the normal limitations on the use of copyrighted materials and to the proper and full acknowledgement of its source.
- The digital version of the thesis I am supplying is the same version as the final, hard-bound copy submitted in completion of my degree, once any minor corrections have been completed.
- I have exercised reasonable care to ensure that the thesis is original, and does not to the best of my knowledge break any UK law or other Intellectual Property Right, or contain any confidential material.
- I understand that, through the medium of the Internet, files will be available to automated agents, and may be searched and copied by, for example, text mining and plagiarism detection software.

(b) IF I HAVE AGREED (in Section 2 above) TO MAKE MY THESIS PUBLICLY AVAILABLE DIGITALLY, I ALSO DECLARE THAT:

- I grant the University of Warwick and the British Library a licence to make available on the Internet the thesis in digitised format through the Institutional Repository and through the British Library via the EThOS service.
- If my thesis does include any substantial subsidiary material owned by third-party copyright holders, I have sought and obtained permission to include it in any version of my thesis available in digital format and that this permission encompasses the rights that I have granted to the University of Warwick and to the British Library.

5. **LEGAL INFRINGEMENTS**

I understand that neither the University of Warwick nor the British Library have any obligation to take legal action on behalf of myself, or other rights holders, in the event of infringement of intellectual property rights, breach of contract or of any other right, in the thesis.

Please sign this agreement and return it to the Graduate School Office when you submit your thesis.

Student's signature: ....[redacted]..................... Date: 16th December 2013

Lattice methods for finding rational points on varieties over number fields

by

Charlotte Lucile Turner

Thesis

Submitted to the University of Warwick

for the degree of

Doctor of Philosophy

Mathematics Institute

December 2013

THE UNIVERSITY OF WARWICK

Contents

List of Algorithms **iv**

Declaration **vi**

Abstract **vii**

Chapter 1 Introduction **1**

Chapter 2 Varieties over Number Fields **5**

2.1 Number Fields . . . 5

2.1.1 Ideals and norms . . . 6

2.1.2 Primes, valuations and places . . . 7

2.1.3 Decomposition of primes . . . 8

2.1.4 $\mathfrak{p}$-adic completion . . . 9

2.1.5 Units . . . 10

2.2 Projective space and varieties . . . 10

Chapter 3 Height and length **13**

3.1 Heights . . . 13

3.1.1 Ideal class of a projective point . . . 15

3.2 Length . . . 16

3.3 Logarithmic maps . . . 17

3.3.1 The image of $\widehat{l}$ in $\mathbb{R}^{r_1+r_2}$ . . . 19

3.3.2 Convexity of μ . . . 19

3.4 The effect of units . . . 20

3.5 A fundamental domain for the action of Λ on $\Pi(h)$ . . . 22

3.5.1 A base point that is a minimum for μ . . . 22

3.5.2 A fundamental domain . . . 23

3.5.3 Maximum value of μ on the fundamental domain $C(h)$ . . . 24

3.6 Dimension reduction 25
3.7 A bound on vector length 26
3.8 Examples 27

Chapter 4 Choosing a prime **28**
4.1 Conditions on suitable primes 28
4.1.1 Good reduction 28
4.1.2 Degree one 28
4.1.3 Principal 29
4.1.4 Norm 29
4.2 Decomposition of rational primes 29
4.3 Existence of suitable primes 30
4.3.1 Density of primes 32
4.4 Algorithm 34

Chapter 5 Constructing sets of lifts **35**
5.1 Taylor expansions, polynomial functions and power series 35
5.2 Hensel lifting 40
5.3 First sets of lifts 42
5.4 Further sets of lifts 44
5.4.1 Construction of vectors 45
5.5 Higher dimensional varieties 48
5.6 Implementation 52
5.7 Interpretation of sets of lifts 53

Chapter 6 Constructing lattices of lifts from sets **55**
6.1 $\mathcal{O}_K$-lattices 55
6.1.1 Index-ideals of sub-lattices 56
6.2 Lattices of lifts 58
6.3 Implementation 60
6.3.1 $\mathfrak{p}$-adic precision 60
6.3.2 Constructing a lattice from a set 61

Chapter 7 Points from lattices via $\mathbb{Z}$-lattice enumeration **62**
7.1 A $\mathbb{Z}$-lattice from an $\mathcal{O}_K$-lattice 63
7.2 Precision 63
7.2.1 Unit roundoff, precision and matrix entry precision 63
7.2.2 Adjusted length bounds 65

7.3 Approximating the Gram matrix . . . 67
7.3.1 Adjusting precision . . . 70
7.4 Finding points . . . 71

Chapter 8 Points from lattices via lattice reduction 72
8.1 Effective methods over number fields . . . 76
8.1.1 Lattice reduction methods . . . 76
8.1.2 Norms, scalar multiplication and imaginary quadratic fields . 79

Chapter 9 Algorithms and examples 81
9.1 Processing lattice points . . . 81
9.1.1 Processing in $\mathbb{Z}^{d(N+1)}$ . . . 81
9.1.2 Processing in $\mathcal{O}_K^{N+1}$ . . . 82
9.1.3 Processing in $\mathbb{P}^N(K)$ . . . 82
9.2 Finding points by $\mathbb{Z}$-lattice enumeration . . . 83
9.3 Finding points by lattice reduction . . . 86
9.3.1 Finding points from a sublattice or subvariety . . . 87
9.4 Examples . . . 92

Bibliography 96

List of Algorithms

1 Primes of degree one 34
2 Approximation to T_2 matrix with bounded length error 69
3 Points from an $\mathcal{O}_K$-lattice via restriction of scalars and $\mathbb{Z}$-lattice enumeration 84
4 Points on a variety via $\mathbb{Z}$-lattice enumeration 86
5 Points on a variety via lattice reduction 88
6 Points on a subvariety after lattice reduction 90
7 Points on a subvariety after lattice reduction with recursion 92

Acknowledgements

I would first like to thank my supervisor, John Cremona, for all of his guidance and encouragement through my doctoral study. John has been an excellent mentor and our meetings have always given me inspiration and confidence.

My heartfelt thanks go to Robert Miller for transatlantic proofreading, his love and steadfast confidence in me, and many mathematical conversations.

I am grateful to the staff and my fellow students at the Warwick Mathematics Institute for their support, especially the Number Theory group. Thanks go to David McCormick for his answers when I needed to “Ask an Analyst”. I am grateful for the financial support of EPSRC.

I would like to thank Wynne, Valérie and Claire Turner for being behind me all the way.

Declaration

This thesis is submitted to the University of Warwick in support of my application for the degree of Doctor of Philosophy. It has been composed by myself and has not been submitted in any previous application for any degree.

Abstract

We develop a method for finding all rational points of bounded height on a variety defined over a number field K. Given a projective variety V we find a prime $\mathfrak{p}$ of good reduction for V with certain properties and find all points on the reduced curve $\bar{V}(\mathbb{F}_{\mathfrak{p}})$. For each point $\bar{P} \in \bar{V}(\mathbb{F}_{\mathfrak{p}})$ we may define lattices of lifts of $\bar{P}$: these lattices contain all points which are congruent to $\bar{P} \mod \mathfrak{p}$ satisfying the defining polynomials of V modulo a power of $\mathfrak{p}$. Short vectors in these lattices are possible representatives for points of bounded height on the original variety $V(K)$. We make explicit the relationship between the length of a vector and the height of a point in this setting. We will discuss methods for finding points in these lattices and how they may be used to find points of $V(K)$, including a method involving lattice reduction over number fields.

The method is implemented in Sage and examples are included in this thesis.

Chapter 1

Introduction

Let V be a variety defined over a number field K. A basic problem of explicit arithmetic geometry is to determine the set $V(K)$ of K-rational points of V. Common variants of this question include determining the set of all points of $V(K)$ of height up to some bound, proving that no such points exist or finding a single point of $V(K)$. For example, in performing a descent on an elliptic curve E/K one constructs homogeneous spaces C/K which are smooth curves of genus one; one wishes to find a single point of $C(K)$.

A family of methods for finding rational points if the variety is a curve $\mathcal{C}$ over $\mathbb{Q}$ have been suggested, more or less independently, by several people. In these methods one determines a lattice (a free $\mathbb{Z}$-module of rank $N+1$, if $\mathcal{C} \subset \mathbb{P}^N(\mathbb{Q})$) of points that are "near" $\mathcal{C}$. Short vectors in the lattice correspond to points near or on $\mathcal{C}$. These may be found by enumeration of lattice vectors (such as the algorithm of Fieker and Pohst [14]) or via lattice reduction (such as LLL-reduction [21]). In the work of Elkies [13] this lattice contains rational points that are near the curve under the usual Euclidean norm. The idea of constructing lattices of points that are p-adically near $\mathcal{C}$ for some prime p has been suggested by Heath-Brown [17] and further developed and implemented by Watkins [32], Womack [33] and Long [22] when $\mathcal{C}$ is an intersection of two quadrics in $\mathbb{P}^3$. Roberts developed and implemented this for quadric intersections defined over function fields $\mathbb{F}_q(t)$ in [26].

The reports by Cremona and Roberts [11] and Cremona, Roberts and the author [10] contain the most comprehensive accounts of such methods so far. They describe a method for finding rational points on any smooth, irreducible curve in $\mathbb{P}^2$ or $\mathbb{P}^3$ defined over $\mathbb{Q}$ or $\mathbb{F}_q(t)$. The idea of extending such a method to curves defined over number fields is mentioned in [10].

A version of this method for varieties defined over $\mathbb{Q}$ has been implemented in Magma [4] by Mark Watkins as PointSearch(S, H): given a scheme S defined over $\mathbb{Q}$ in either affine or projective space, it will find rational points of height less than H using a p-adic method. It provides a flag to choose whether to find all such points or to stop after only one point has been found. The PointsQI function finds rational points of bounded height in the special case of quadric intersections defined over $\mathbb{Q}$. There is no published work explaining or justifying these methods, except for a brief online note by Watkins [32].

In this thesis we define several related lattice-based methods for finding rational points on varieties defined over a number field K. We deal with important complications that do not arise in the case of varieties defined over $\mathbb{Q}$. We give a full explanation and justification of how to construct $\mathcal{O}_K$-lattices of lifts for varieties of any dimension $\geqslant 1$.

Let $V \subset \mathbb{P}^N(K)$ be a variety defined over a number field K by homogeneous polynomials in $K[X_0, \dots, X_N]$. By reducing these polynomials modulo a suitable prime $\mathfrak{p}$ and finding points on the resulting reduced variety $\bar{V}$ we obtain a finite list of reduced points that comprise $\bar{V}(\mathbb{F}_\mathfrak{p})$. Each point of $V(K)$ reduces to one such reduced point $\bar{P}$ modulo $\mathfrak{p}$. For each $\bar{P}$ we may construct a sequence $(L_i)_{i\geqslant 1}$ of **lattices of lifts**: $\mathcal{O}_K$-modules inside $\mathcal{O}_K^{N+1}$ containing all vectors x such that $x \equiv \bar{P} \mod \mathfrak{p}$ and $\underline{F}(x) \equiv 0 \mod \mathfrak{p}^i$. We use Hensel lifting to refine the points to solutions modulo higher powers of $\mathfrak{p}$. Each K-rational point of V can be represented by a vector in L_i for some reduced point $\bar{P}$. Our aim is to find all rational points on V with height up to some bound. After fixing a lattice of lifts L_i, points of small height on V reducing to $\bar{P} \mod \mathfrak{p}$ are represented by short vectors in L_i. We find short vectors either by lattice enumeration or by using a method involving lattice reduction (described by Cremona and Roberts in [11]) which reduces the rank of the lattice. This reduction in the rank of the lattice reduces our search to a subvariety of V which will usually have smaller dimension. In the case where V is a curve, this reduction of rank means that we may find points of small height on V by solving a system of polynomials that defines a variety of dimension 0.

We begin in Chapter 2 by collecting some basic information about number fields and about varieties which we will need in later chapters. In Chapter 3 we recall the definition of height for a projective point and link it to a notion of length for vectors in K^n. This is one part in which our situation is quite different from the case of varieties over $\mathbb{Q}$ since we may have infinitely many units in $\mathcal{O}_K$—these will affect the length of a vector. A potentially useful consequence of this work is that we may use it, combined with a lattice enumeration method (such as that explained in Chapter 7), to find all points of $\mathbb{P}^N(K)$ with height up to some bound.

To reduce the variety V modulo a prime $\mathfrak{p}$ we first need to find a suitable $\mathfrak{p}$. The difference here from the rational case is that not every prime ideal is principal. In Chapter 4 we explain why we choose to work with principal primes, describe some other attributes of the primes with which we prefer to work and explain an algorithm for constructing them.

Chapter 5 explains how to systematically construct suitable $\mathfrak{p}$-adic lifts of a point $\bar{P}$ on a reduced variety $\bar{V}$. We begin with the case of curves before generalising to varieties of any dimension. This is an important improvement on the descriptions of [32], [11] and [10], as we describe this procedure to arbitrary $\mathfrak{p}$-adic precision. We achieve this by ignoring issues of linear dependence and by generalising the linear forms defined by gradient vectors and quadratic forms defined by Hessian matrices to higher degrees.

We explain what is meant by an $\mathcal{O}_K$-lattice in Chapter 6 and we explain how to use the set of lifts defined in Chapter 5 to define an $\mathcal{O}_K$-lattice of lifts. We recall the concept of lattice index for $\mathcal{O}_K$-lattices, show that the index of our lattice of lifts L_i is a power of $\mathfrak{p}$ and find bounds for its exponent.

In Chapter 7 we convert an $\mathcal{O}_K$-lattice to a $\mathbb{Z}$-lattice by restricting scalars and find points using existing lattice enumeration techniques. This means an increase in rank: an $\mathcal{O}_K$-lattice of rank n becomes a $\mathbb{Z}$-lattice of rank nd where d is the degree of K over $\mathbb{Q}$. The Gram matrix by which we specify a $\mathbb{Z}$-lattice has entries in $\mathbb{R}$ represented by floating-point numbers. We give the details about precision in floating-point arithmetic that we need and calculate the appropriate adjustment in length needed to compensate for the fact that the Gram matrix is not given exactly.

In [11] Cremona and Roberts explain how, by constructing a lattice of lifts with large index and performing LLL reduction on a lattice basis, we can reduce our search for points of bounded height to a sublattice of our lattice of lifts with smaller rank. In Chapter 8 we survey the existing forms of lattice reduction for $\mathcal{O}_K$-lattices and explain Cremona and Roberts' idea. We show that, with the right kind of lattice reduction, one can apply such a technique over imaginary quadratic fields and we demonstrate a problem with this for other number fields. We cannot conclude whether or not this is possible for number fields in general.

By discussing what kind of lattice reduction is needed we see that, unfortunately, the hope we expressed in [10] that we could use Fieker and Stehlé's lattice reduction [15] for such a technique was wrong. However, we do show that the lattice reduction described by Napias in [23] (and probably that of Fieker and Pohst from [14]) can be used for number fields whose ring of integers is a euclidean ring. Although we conclude that we only know a handful of number fields over which we can use lattice reduction in this way, the information provided in this chapter could be a starting-point for future work on $\mathcal{O}_K$-lattice reduction that would allow the technique of reducing the rank of the lattice to be used in more generality.

In Chapter 9 we gather material from the rest of the thesis to describe algorithms for finding points on varieties. We give some examples of points found on curves over number fields using one of these methods. Some of the algorithms described in this thesis have been implemented in Sage [30] and we hope that after some further work these methods will be included in future releases of Sage.

Chapter 2

Varieties over Number Fields

None of the material in this chapter is new, but it serves to remind us of important basic results and fix our notation. Much of this material may be found in [5], [24] and [28].

2.1 Number Fields

Let K be a number field of degree d and let $\mathcal{O}_K$ be the ring of integers of K.

Definition 1. *We say that $\alpha_1, \ldots, \alpha_d \in \mathcal{O}_K$ form an **integral basis** for K if $K = \oplus_{i=1}^{d} \mathbb{Q}\alpha_i$ and $\mathcal{O}_K = \oplus_{i=1}^{d} \mathbb{Z}\alpha_i$.*

Theorem 2.1 (Theorem 4.1.8 of [5])**.** *Let K be a number field of degree d.*

1. *There exists an $\alpha \in K$ such that*

$$K = \mathbb{Q}(\alpha).$$

   *Such an α is called a **primitive element** and its minimal polynomial over $\mathbb{Q}$ is irreducible of degree d.*

2. *There exist exactly d field embeddings of K into $\mathbb{C}$. They are the maps $\sigma_j : \alpha \mapsto \theta_j$ where the $\theta_j \in \mathbb{C}$ are the roots of the minimal polynomial of α. These embeddings are $\mathbb{Q}$-linear.*

Definition 2. *The **signature** of K is a pair (r_1, r_2) where r_1 is the number of **real embeddings** of K whose images lie in $\mathbb{R}$ and $2r_2$ is the number of **complex embeddings** whose images are not contained in $\mathbb{R}$.*

The $2r_2$ complex embeddings come in pairs: if σ_j is a complex embedding sending α to θ_j then there is an embedding $\bar{\sigma}_j$ that sends α to $\bar{\theta}_j$. We will adopt the convention of numbering the real embeddings of K by $\sigma_1, \ldots, \sigma_{r_1}$ and the complex embeddings by $\sigma_{r_1+1}, \ldots, \sigma_{r_1+2r_2}$ so that $\sigma_{r_1+k} = \bar{\sigma}_{r_1+r_2+k}$.

Definition 3. *Let $x \in K$. Then the (field)* ***norm*** *of x is given by*

$$\mathcal{N}(x) = \prod_{j=1}^{d} |\sigma_j(x)|.$$

Note that the norm is always non-negative.

2.1.1 Ideals and norms

We use the word **ideal** to refer to fractional ideals of $\mathcal{O}_K$ and reserve the term **integral ideal** for those ideals contained in $\mathcal{O}_K$. Every ideal is an $\mathcal{O}_K$-module of rank 1. An ideal of $\mathcal{O}_K$ is **principal** if it is generated as an $\mathcal{O}_K$-module by a single element $a \in K$; such an ideal $a\mathcal{O}_K$ may also be written $\langle a \rangle$.

Definition 4. *An integral ideal $\mathfrak{p}$ of $\mathcal{O}_K$ is called a* ***prime ideal*** *if $\mathcal{O}_K/\mathfrak{p}$ is an integral domain.*

Definition 5. *The* ***norm*** *of an integral ideal $\mathfrak{a}$ of $\mathcal{O}_K$ is the cardinality of the finite ring $\mathcal{O}_K/\mathfrak{a}$. It is denoted $\mathcal{N}(\mathfrak{a})$. We extend this definition to fractional ideals by multiplicativity: if $\mathfrak{c} = \mathfrak{a}\mathfrak{b}^{-1}$ where $\mathfrak{a}$ and $\mathfrak{b}$ are integral ideals, then*

$$\mathcal{N}(\mathfrak{c}) = \frac{\mathcal{N}(\mathfrak{a})}{\mathcal{N}(\mathfrak{b})}.$$

The norm of a fractional ideal is a rational number, not necessarily an integer.

Lemma 2.2 (Proposition 4.6.15 of [5])**.** *Let $x \in K$. Then*

$$\mathcal{N}(x) = \mathcal{N}(\langle x \rangle).$$

Definition 6. *We say that two ideals $\mathfrak{a}, \mathfrak{b}$ of $\mathcal{O}_K$ are* ***equivalent*** *if there exists $a \in K^*$ such that*

$$\mathfrak{a} = \langle a \rangle \mathfrak{b}.$$

The set of equivalence classes of ideals of $\mathcal{O}_K$ form a group called the ***class group*** *of K that is denoted by* $\mathrm{Cl}(K)$.

The class of principal ideals is the identity class of $\mathrm{Cl}(K)$. If the class group $\mathrm{Cl}(K)$ is trivial then all ideals of $\mathcal{O}_K$ are principal and $\mathcal{O}_K$ is a **principal ideal domain**.

Definition 7. *Let $\alpha_1, \ldots, \alpha_d$ be an integral basis for K. Then*

$$D(K) = (\det(\sigma_j(\alpha_i))_{ij})^2$$

*is a non-zero integer called the **discriminant** of K.*

Proposition 2.3 (Theorem 7.1.2 of [29])**.** *Every class of* $\mathrm{Cl}(K)$ *contains an integral ideal $\mathfrak{a}$ of $\mathcal{O}_K$ satisfying*

$$\mathcal{N}(\mathfrak{a}) \leqslant \sqrt{|D(K)|}\left(\frac{4}{\pi}\right)^{r_2}\frac{d!}{d^d}.$$

The quantity $\sqrt{|D(K)|}\left(\frac{4}{\pi}\right)^{r_2}\frac{d!}{d^d}$ is called the **Minkowski bound** for K and it depends only on the discriminant and signature of K.

Corollary 2.4. *The class group of K is finite.*

Proof. There are only finitely many ideals with a given norm, so this follows from Proposition 2.3. □

The cardinality of the class group is called the **class number** of K and is given by $h_k = |\operatorname{Cl}(K)|$.

2.1.2 Primes, valuations and places

Theorem 2.5 (Theorem 4.6.14 of [5])**.** *Every fractional ideal $\mathfrak{a}$ of $\mathcal{O}_K$ can be written in a unique way as*

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})},$$

where the product runs over a finite set of prime ideals and each $v_{\mathfrak{p}}(\mathfrak{a})$ is in $\mathbb{Z}$. The ideal $\mathfrak{a}$ is an integral ideal if and only if all $v_{\mathfrak{p}}(\mathfrak{a})$ are non-negative.

The quantity $v_{\mathfrak{p}}(\mathfrak{a})$ is the **valuation** of $\mathfrak{a}$ at $\mathfrak{p}$. We can define valuations on K by considering the valuation of a principal ideal: if $x \in K$, $v_{\mathfrak{p}}(x) = v_{\mathfrak{p}}(\langle x \rangle)$. Each prime ideal $\mathfrak{p}$ defines a non-Archimedean **absolute value** $|.|_{\mathfrak{p}}$ on K which is related to the valuation by $|x|_{\mathfrak{p}} = \mathcal{N}(\mathfrak{p})^{-v_{\mathfrak{p}}(x)}$. The embeddings $\sigma_1, \ldots, \sigma_d$ define the Archimedean absolute values of K, given by $|\sigma_j(x)|$.

The equivalence classes of absolute values on K are called the **places** of K. The **finite places** are defined by the non-Archimedean absolute values associated to the prime ideals of K and the **infinite places** are given by the Archimedean absolute values associated to the embeddings of K into $\mathbb{R}$ and $\mathbb{C}$ with σ_{r_1+j} being identified with $\sigma_{r_1+r_2+j}$ because $|\sigma_{r_1+j}(x)| = |\sigma_{r_1+r_2+j}(x)|$ for all $x \in K$ and $1 \leqslant j \leqslant r_2$. Therefore there are $r_1 + r_2$ infinite places of K. The set of all places of K is denoted M_K; M_K^∞ denotes the infinite places and M_K^f, the finite places. We associate a number n_j to each infinite place as follows:

$$n_j = \begin{cases} 1 & \text{if } \sigma_j \text{ is real} \\ 2 & \text{if } \sigma_j \text{ is complex.} \end{cases}$$

It will sometimes be convenient to consider each Archimedean absolute value as being associated to an infinite place of K rather than to an embedding. With this in mind, we define $|x|_j = |\sigma_j(x)|^{n_j}$ for each $1 \leqslant j \leqslant r_1+r_2$. For complex embeddings, this is a slight abuse of notation as $|.|_j$ is not an absolute value (it does not satisfy the triangle inequality) but this will not be of any importance to us. The n_j is called the **local degree** at this infinite place. There is a corresponding definition of local degree for finite places, but our definition of $|.|_{\mathfrak{p}}$ has already been normalised to take this into account. We will change between using $|\sigma_j(x)|$ and $|x|_j$ dependent on context.

Proposition 2.6 (Product Formula, Theorem 2 of IV.4 of [3])**.** *For any $x \in K^*$ we have*

$$\prod_{v \in M_K} |x|_v = 1;$$

therefore

$$\sum_{v \in M_K} \log(|x|_v) = 0,$$

with the normalisation that $|x|_j = |\sigma_j(x)|^{n_j}$ for each infinite place of M_K.

2.1.3 Decomposition of primes

This material can be found in Section I.8 of [24]. Let L/K be an extension of number fields. For any prime $\mathfrak{q}$ of L there exists a prime ideal of K such that one has the relation

$$\mathfrak{q} \cap \mathcal{O}_K = \mathfrak{p}.$$

We say that $\mathfrak{q}$ is a prime **above** $\mathfrak{p}$ and that $\mathfrak{p}$ lies **below** $\mathfrak{q}$. If $\mathfrak{p}$ is a prime of K then $\mathfrak{p}$ decomposes in L: there exist positive integers e_i such that

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{q}_i^{e_i},$$

where $\mathfrak{q}_i$ are all of the prime ideals of L above $\mathfrak{p}$.

Definition 8. *The integer e_i is called the **ramification index** of $\mathfrak{p}$ at $\mathfrak{q}_i$. The degree*

$$f_i = [\mathcal{O}_L/\mathfrak{q}_i : \mathcal{O}_K/\mathfrak{p}]$$

*of the extension of residue fields is called the **degree** of $\mathfrak{q}_i$. (This is sometimes called the inertia degree or residual degree).*

For any extension of number fields, ramification indices and degrees satisfy the following formula:

$$\sum_{i=1}^{g} e_i f_i = d.$$

Let $\mathfrak{p}_i$ be a prime of K which lies above a rational prime p of $\mathbb{Q}$. Then the norm of $\mathfrak{p}_i$ satisfies

$$\mathcal{N}(\mathfrak{p}_i) = p^{f_i}.$$

2.1.4 $\mathfrak{p}$-adic completion

Definition 9. *Let $\mathfrak{p}$ be a prime ideal of K. We define $K_{\mathfrak{p}}$ to be the completion of K with respect to the metric induced on K by the absolute value defined by $\mathfrak{p}$. $K_{\mathfrak{p}}$ is given by the set of $\mathfrak{p}$-adically Cauchy sequences in K, up to equivalence. Two Cauchy sequences are **equivalent** if their difference converges to 0.*

The **ring of $\mathfrak{p}$-adic integers** is denoted by $\mathcal{O}_{K_{\mathfrak{p}}}$: it is the set of $\alpha \in K_{\mathfrak{p}}$ such that $|\alpha|_{\mathfrak{p}} \leqslant 1$. We may also use a more explicit representation for the p-adics. Every $\mathfrak{p}$-adic integer can be uniquely represented by a sequence $(x_n)_{n=1}^{\infty}$ such that $x_n \in \mathcal{O}_K$ is chosen to be in a fixed set of representatives of $\mathcal{O}_K/\mathfrak{p}^n$ and

$$x_n \equiv x_{n+1} \mod \mathfrak{p}^n$$

for every $n \geqslant 1$.

By considering a $\mathfrak{p}$-adic integer $x \in \mathcal{O}_{K_{\mathfrak{p}}}$ modulo $\mathfrak{p}^m$ for some $m > 0$ we can truncate our representation of x to have only m terms. Such a truncation is an element of $\mathcal{O}_K$ that is congruent to x modulo $\mathfrak{p}^m$.

2.1.5 Units

Let $\mathcal{O}_K^*$ denote the group of units of $\mathcal{O}_K$.

Lemma 2.7. *If $u \in \mathcal{O}_K^*$ then $\mathcal{N}(u) = 1$.*

Proof. If $u \in \mathcal{O}_K^*$ then $\langle u \rangle = \mathcal{O}_K$, so the result follows from the definition of ideal norm. □

Theorem 2.8 (Dirichlet's Unit Theorem, Theorem 4.9.5 of [5])**.** *Let (r_1, r_2) be the signature of a number field K. Then*

$$\mathcal{O}_K^* \simeq \mu(K) \times \mathbb{Z}^{r_1+r_2-1},$$

where $\mu(K)$ is the subgroup of roots of unity in K.

We may choose a set of units $\varepsilon_1, \ldots, \varepsilon_{r_1+r_2-1}$ so that every unit $x \in \mathcal{O}_K^*$ may be written as

$$x = \zeta \prod_{k=1}^{r_1+r_2-1} \varepsilon_k^{t_k},$$

where $t_k \in \mathbb{Z}$ and ζ is a root of unity in K. We call the set $\{\varepsilon_k\}_{k=1}^{r_1+r_2-1}$ a system of **fundamental units** for K and say that $r_1 + r_2 - 1$ is the **unit rank** of K.

2.2 Projective space and varieties

We denote by $\mathbb{P}^N(K)$ the **projective space** of dimension N over K.

Definition 10. *Let $P \in \mathbb{P}^N(K)$. We say that $(x_0, \ldots, x_N) \in K^{N+1}$ is a **representative** of P if $P = [x_0 : \ldots : x_N]$.*

We note that such a representative for P is not unique: if x represents P and $\lambda \in K^*$ then λx also represents P. If the ith coordinate of a representative of P is zero then the ith coordinate is zero in all representatives of P. Every P has a representative (in fact, infinitely many) that is in $\mathcal{O}_K^{N+1}$ and in this thesis we will always use such integral representatives.

Let $\bar{K}$ be the algebraic closure of K and let f be a homogeneous polynomial in $\bar{K}[X_0, \ldots X_N]$. Although it does not make sense in general to evaluate f at a projective point P (as such a value will be affected by scaling) the set of points $P \in P^N(\bar{K})$ such that $f(P) = 0$ is well defined because of the homogeneity of f.

Definition 11. *Let $\underline{F} = (F_1, \ldots, F_m)$ be a tuple of homogeneous polynomials in $\bar{K}[X_0, \ldots, X_N]$. Then the* ***projective variety*** *V defined by $\underline{F}$ is*

$$V = \left\{ P \in \mathbb{P}^N(\bar{K}) \;\middle|\; F_i(P) = 0 \text{ for all } F_i \in \underline{F} \right\}.$$

To a variety V we may associate an ideal $I(V) \subset \bar{K}[X_0, \ldots, X_N]$ consisting of all polynomials that vanish at every point of V.

Such an ideal is finitely generated so we may fix a set of homogeneous polynomials $\{F_1, \ldots, F_m\}$ that generate $I(V)$ to define a variety V. We say that a variety is **defined over** K if there exists a set of polynomials defining V that are all in $K[X_0, \ldots, X_N]$. We will assume from now on that all of our varieties are defined over K. We may assume, by scaling, that the polynomials $F_1, \ldots, F_N \in \mathcal{O}_K[X_0, \ldots, X_N]$.

Definition 12. *A variety V is* ***geometrically irreducible*** *if $I(V)$ is a prime ideal in $\bar{K}[X_0, \ldots, X_N]$.*

Definition 13. *The set of* K***-rational points*** *of V is the set*

$$V(K) = \left\{ P \in \mathbb{P}^N(K) \;\middle|\; F_i(P) = 0 \text{ for all } F_i \in \underline{F} \right\}.$$

We will refer to them as ***rational points*** *as the number field K will be fixed for each variety.*

The aim of this thesis will be to develop algorithms for finding rational points on a variety V defined over K.

Definition 14. *The* ***coordinate ring*** *of V is the polynomial ring given by $\bar{K}(V) = \frac{\bar{K}[X_0, \ldots, X_n]}{I(V)}$. The* ***dimension*** *of V is the transcendence degree of $\bar{K}(V)$ over $\bar{K}$.*

A variety in $\mathbb{P}^N$ is defined by at least $N - \dim(V)$ homogeneous polynomials. The word **curve** is used for a variety of dimension one.

Definition 15. *We say that a variety V is* ***smooth*** *or* ***non-singular*** *at $P \in V$ if the* ***Jacobian matrix***

$$\nabla \underline{F}(x) = \left(\frac{\partial F_i}{\partial X_j}(x) \right)_{ij}$$

has rank $N - \dim V$ when x is any representative for P. If V is smooth at all $P \in V$ we say that V is smooth. A point of a variety which is not smooth is called ***singular****.*

We will assume throughout that varieties we are dealing with are projective, smooth and geometrically irreducible. We will always define a variety using a specific tuple of polynomials $\underline{F} \subset \mathcal{O}_K[X_0, \ldots, X_N]$.

Let $\mathfrak{p}$ be a prime ideal of K. We may reduce the coefficients of the polynomials $\underline{F}$ modulo $\mathfrak{p}$ to obtain a new variety, defined by polynomials $\bar{F}_1, \ldots, \bar{F}_m$ over $\mathbb{F}_{\mathfrak{p}}$.

Definition 16. *A prime ideal $\mathfrak{p}$ of K is a* ***prime of good reduction*** *or simply a* ***good prime*** *if the variety $\bar{V}$ defined by the* ***reduced polynomials*** $\bar{\underline{F}}$ *is smooth of the same dimension as V and the polynomial ideal defined by $\bar{\underline{F}}$ is prime in $\mathbb{F}_{\mathfrak{p}}[X_0, \ldots, X_N]$.*

Strictly speaking, this is a property of the polynomials $\underline{F}$ rather than of V itself but this definition will suffice for our purposes as we will always fix a tuple of defining polynomials $\underline{F}$ for our variety. We say that $\mathfrak{p}$ is a **bad prime** if it is not a good prime for V.

Definition 17. *Let $x = (x_0, \ldots, x_N) \in K^{N+1}$. Then the* ***content ideal*** *of x is the ideal*

$$I(x) = \langle x_0, \ldots, x_N \rangle.$$

The content ideal $I(x)$ is integral if and only if $x \in \mathcal{O}_K^{N+1}$.

Lemma 2.9. *Let $P \in \mathbb{P}^N(K)$. Then $I(x)$ lies in the same ideal class for every representative x of P.*

Proof. Let $x \in K^{N+1}$ be a representative for P with content ideal $\langle x_0, \ldots, x_N \rangle$. Then every representative of P is of the form λx for some $\lambda \in K^*$ and

$$\langle \lambda x_0, \ldots, \lambda x_N \rangle = \langle \lambda \rangle \langle x_0, \ldots, x_N \rangle.$$

□

Definition 18. *Let $\mathfrak{a}$ be an ideal of K. We say that $x \in \mathcal{O}_K^{N+1}$ is $\mathfrak{a}$-primitive if $I(x)$ is coprime to $\mathfrak{a}$.*

We have now introduced the basic concepts of number theory and geometry that we will use in this thesis. Our overall aim is to describe methods for finding rational points on varieties from their representatives in certain lattices contained in $\mathcal{O}_K^{N+1}$. In the next chapter we will describe the concepts of height for a point of $P \in \mathbb{P}^N(K)$ and length for a vector in $\mathcal{O}_K^{N+1}$, and relate the length of some representative of P to the height of P.

Chapter 3

Height and length

It is well known that the number of points of projective space $\mathbb{P}^N(K)$ whose height is at most a given bound B_H is finite. It is the aim of this chapter to find a $B_L > 0$ so that every point in $\mathbb{P}^N(K)$ with height at most B_H is represented by a vector of $\mathcal{O}_K^{N+1}$ of length at most B_L. This reduces the problem of finding points of bounded height on a projective variety $V \subseteq \mathbb{P}^N(K)$ to the checking of points in a finite, explicitly defined subset of $\mathcal{O}_K^{N+1}$. Naively, one could then simply check every point of $\mathcal{O}_K^{N+1}$ with length less than B_L. We will construct lattices later in this thesis to significantly reduce the quantity of points to be checked.

In this chapter we will explain what we mean by height and length in this context and link them to construct a suitable length bound B_L. We use standard definitions for height, T_2 and the logarithmic map that can be found in [28], [15] and [24] respectively.

3.1 Heights

Let $P \in \mathbb{P}^N(K)$ and let $x \in K^{N+1}$ be a representative for P. We recall that a representative for P is not unique. In this chapter we will prove the existence of certain short representatives in $\mathcal{O}_K^{N+1}$ for a point P of height less than B_H.

Definition 19. *Let P be represented by $x = (x_0, \dots, x_N)$. Then the* ***logarithmic height*** *of P is defined to be:*

$$H(P) = H([x_0 : \cdots : x_N]) = \sum_{v \in M_K} \max_i \log |x_i|_v.$$

We will use the convention that $\log(0) = -\infty$ if a coordinate x_i of x is equal to 0, but note that each term in the sum must be finite as no representative for a projective point may have all of its coordinates equal to 0.

Lemma 3.1. *The logarithmic height of P does not depend on the representative $(x_0, \dots, x_N)$ of P.*

Proof. Let x and λx be two representatives for P. Then

$$\begin{aligned}
H([\lambda x_0 : \cdots : \lambda x_N]) &= \sum_{v \in M_K} \max_i \log |\lambda x_i|_v \\
&= \sum_{v \in M_K} \max_i \log(|\lambda|_v |x_i|_v) \\
&= \sum_{v \in M_K} \max_i \bigl(\log(|\lambda|_v) + \log(|x_i|_v)\bigr) \\
&= \sum_{v \in M_K} \log(|\lambda|_v) + \sum_{v \in M_K} \max_i \log(|x_i|_v) \\
&= \sum_{v \in M_K} \log(|\lambda|_v) + H([x_0 : \cdots : x_N]).
\end{aligned}$$

By the product formula (Proposition 2.6) $\sum_{v \in M_K} \log(|\lambda|_v) = 0$, so the height of P does not depend on the representative used to calculate it. □

We may split up the sum in the formulation of the height to consider the finite and infinite places of K separately. We recall that the set of finite places M_K^f of K is in one-to-one correspondence with prime ideals of K. The set of infinite places M_K^∞ of K is in correspondence with embeddings σ_j of K into $\mathbb{R}$ or $\mathbb{C}$ with local degree n_j. We have

$$\begin{aligned}
H(P) &= \sum_{v \in M_K^\infty} \max_i \log |x_i|_v + \sum_{v \in M_K^f} \max_i \log |x_i|_v \\
&= \sum_{j=1}^{r_1 + r_2} n_j \max_i \{\log |\sigma_j(x_i)|\} + \sum_{\mathfrak{p}} \max_i \{\log |x_i|_{\mathfrak{p}}\},
\end{aligned}$$

where $\mathfrak{p}$ ranges over all prime ideals of K.

Although the height of P does not depend on the representative used, the individual terms in the sum do. If x is a representative for P we may define

$$H_\infty(x) = \sum_{j=1}^{r_1 + r_2} n_j \max_i \{\log |\sigma_j(x_i)|\},$$

and

$$H_f(x) = \sum_{\mathfrak{p}} \max_i \{\log |x_i|_{\mathfrak{p}}\},$$

the **infinite** and **finite height** of x. $H_\infty(x)$ and $H_f(x)$ do vary as x varies amongst representatives for P but they always satisfy

$$H(P) = H_\infty(x) + H_f(x).$$

Given a point $x = (x_0, \dots, x_N) \in K^{N+1}$, we have the following important relationship between the content ideal $I(x)$ and the finite height $H_f(x)$:

$$\begin{aligned} H_f(x_0, \dots, x_N) &= \sum_{\mathfrak{p}} \max_i \{\log |x_i|_{\mathfrak{p}}\} \\ &= \log \left(\prod_{\mathfrak{p}} \max_i \{|x_i|_{\mathfrak{p}}\} \right) \\ &= \log \left(\prod_{\mathfrak{p}} \max_i \left\{ \mathcal{N}(\mathfrak{p})^{-v_{\mathfrak{p}}(x_i)} \right\} \right) \\ &= -\log \left(\prod_{\mathfrak{p}} \min_i \left\{ \mathcal{N}(\mathfrak{p})^{v_{\mathfrak{p}}(x_i)} \right\} \right) \\ &= -\log \mathcal{N}(I(x)). \end{aligned}$$

3.1.1 Ideal class of a projective point

Recall from Lemma 2.9 that if $P \in \mathbb{P}^N(K)$ then the content ideals of its representatives must all lie in the same ideal class. Denote this class by $c(P)$.

Let us fix A to be a set of integral ideals, one in each class of $\mathrm{Cl}(K)$, such that each ideal in A has minimal norm amongst integral ideals in its class. Then $|A| = |\mathrm{Cl}(K)| = h_K < \infty$. We will denote the maximum norm attained by an ideal of A by $N_K = \max_{\mathfrak{a} \in A} \mathcal{N}(\mathfrak{a})$. By the Minkowski bound we know that $N_K \leqslant \sqrt{|D(K)|} \left(\frac{4}{\pi}\right)^{r_2} \frac{d!}{d^d}$. It is clear that N_K is an invariant of the field K.

Each projective point P has a representative $x \in \mathcal{O}_K^{N+1}$ such that $I(x) \in A$; we define the ideal of P to be $I(P) := I(x)$. If x is a representative for P such that $I(x) = I(P)$ then $\mathcal{N}(I(x))$ is minimal amongst integral representatives for P and $H_f(x)$ is maximal amongst integral representatives for P. Such a representative satisfies $1 \leqslant \mathcal{N}(I(x)) \leqslant N_K$ and therefore

$$-\log(N_K) \leqslant H_f(x) \leqslant 0.$$

The ideal $\langle 1 \rangle = \mathcal{O}_K$ will always be in A, as the representative of the trivial class of $\mathrm{Cl}(K)$. If the class number $h_K = 1$ then $N_K = 1$ and in this case we can always choose x to be a primitive representative for P: $H_f(x) = 0$ for all such x. All of this leads us to be able to relate the height of P to the infinite height of a representative.

Proposition 3.2. *Let $P \in \mathbb{P}^N(K)$. Then there exists a representative $x \in \mathcal{O}_K^{N+1}$ of P such that*

$$H_\infty(x) \leqslant H(P) + \log(N_K).$$

Proof. Choose x to be a representative of P such that $I(x) \in A$ and therefore $0 < \mathcal{N}(I(x)) \leqslant N_K$. The finite height of x is $H_f(x) = -\log \mathcal{N}(I(x))$, so $-\log(N_K) \leqslant H_f(x)$. The finite and infinite heights of a representative sum to the height of the point, so

$$H_\infty(x) = H(P) - H_f(x) \leqslant H(P) + \log(N_K).$$

□

For every $x \in \mathcal{O}_K^{N+1}$ the finite height satisfies $H_f(x) \leqslant 0$. By choosing an integral representative whose content ideal has the smallest possible norm, we are choosing $x \in \mathcal{O}_K^{N+1}$ so that $H_f(x)$ is maximal. For such an x, $H_\infty(x)$ is minimised amongst integral representatives of P. This is a benefit as $H_\infty(x)$ is linked to the length of x; minimising $H_\infty(x)$ is a step towards choosing an integral representative with short length. We wish to work with integral representatives as $\mathcal{O}_K^{N+1}$ has a lattice structure: in particular there exists a vector of shortest length for any subset of $\mathcal{O}_K^{N+1}$.

3.2 Length

We may associate to a number field K the following bilinear form. For $x, y \in K$ define

$$T_2(x, y) = \sum_{j=1}^{d} \sigma_j(x)\bar{\sigma}_j(y) = \sum_{j=1}^{r_1+r_2} n_j \sigma_j(x)\bar{\sigma}_j(y),$$

and define the T_2**-norm** of x to be $\|x\| = \sqrt{T_2(x, x)}$. We note that our two definitions of T_2 above are equivalent; we will use each of them, depending on whether it is more convenient to consider places (with multiplicities) or embeddings of K. Let $K_\mathbb{R}$ be defined from K by extension of scalars to $\mathbb{R}$ on the $\mathbb{Q}$-vector space K; $K \otimes_\mathbb{Q} \mathbb{R} \cong \mathbb{R}^d$. We may extend the definitions of σ_j, T_2 and $\|.\|$ to $K_\mathbb{R}$ by linearity over $\mathbb{R}$.

We can associate $K_\mathbb{R}$ to another, isomorphic Euclidean space. Let σ be the map given by

$$\begin{aligned} K_{\mathbb{R}} &\xrightarrow{\sigma} \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \\ x &\mapsto (\sigma_1(x), \ldots, \sigma_{r_1+r_2}(x)). \end{aligned}$$

This fixes an $\mathbb{R}$-linear isomorphism of vector spaces over $\mathbb{R}$ from $K_{\mathbb{R}}$ to $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. Then the T_2-norm on $K_{\mathbb{R}}$ is given by the Hermitian inner product on $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ given by the diagonal matrix D with entries $D_{jj} = n_j$. Any ideal $I \subset K$ is mapped to a lattice in $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ as σ respects the $\mathbb{Z}$-module structure.

We may also use T_2 to measure vector length. For $x, y \in K_{\mathbb{R}}^n$ we abuse notation to define $T_2(x, y) = \sum_{i=1}^{n} T_2(x_i, y_i)$ and to let $\|x\| = \sqrt{T_2(x, x)}$. This is not truly a norm on K^n or $K_{\mathbb{R}}^n$ because it is sub-multiplicative: if $\lambda \in K_{\mathbb{R}}$ then $\|\lambda x\| \leqslant \|\lambda\|\|x\|$, but we will also refer to this $\|.\|$ as the T_2-norm on K^n and ${K_{\mathbb{R}}}^n$.

We may extend the σ map to vectors. Applying $\sigma : K_{\mathbb{R}}^n \to (\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})^n$ gives an $n \times (r_1 + r_2)$ matrix:

$$\sigma(x) = (\sigma_j(x_i))_{ij},$$

and we may interpret the square of the T_2-norm of x as a weighted sum of the squares of sizes of entries of the matrix $\sigma(x)$:

$$\|x\|^2 = \sum_{i,j} n_j |(\sigma(x))_{ij}|^2 = \sum_{i,j} n_j |\sigma_j(x_i)|^2.$$

3.3 Logarithmic maps

In this section we will introduce the logarithmic map $l : K^* \to \mathbb{R}^{r_1+r_2}$ and a variant, $\widehat{l} : (K^*)^n \to \mathbb{R}^{r_1+r_2}$. l encodes information about about the size of the image of an element of K under each of the embeddings of K into $\mathbb{R}$ or $\mathbb{C}$.

We define the logarithmic map $l : K^* \to \mathbb{R}^{r_1+r_2}$ as follows:

$$l(x) = (n_1 \log |\sigma_1(x)|, \ldots, n_{r_1+r_2} \log |\sigma_{r_1+r_2}(x)|).$$

This map is sometimes referred to in the literature as the "logarithmic embedding" but it is worth noting that this is not an embedding but a homomorphism, with the roots of unity in K^* forming the kernel. We extend the definition of l to vectors in $(K^*)^n$, with image contained in the matrix space $\mathbb{R}^{n \times (r_1+r_2)}$. We note that l cannot apply to vectors with a zero entry.

$$\begin{aligned} l :&(K^*)^n \longrightarrow \mathbb{R}^{n\times(r_1+r_2)} \\ &(x_1,\ldots,x_n) \mapsto \begin{pmatrix} l_{11}(x) & \cdots & l_{1(r_1+r_2)}(x) \\ \vdots & \ddots & \vdots \\ l_{n1}(x) & \cdots & l_{n(r_1+r_2)}(x) \end{pmatrix}, \end{aligned}$$

where

$$l_{ij}(x) = n_j \log|\sigma_j(x_i)|.$$

We also define a related map $\widehat{l} : (K^*)^n \to \mathbb{R}^{r_1+r_2}$ given by

$$\widehat{l}(x) = \left(\max_i l_{i1}(x), \ldots, \max_i l_{i(r_1+r_2)}(x)\right),$$

and denote the jth entry of $\widehat{l}(x)$ by $\widehat{l}_j(x)$:

$$\widehat{l}_j(x) = \max_i l_{ij}(x).$$

For any $x \in (K^*)^n$, it is clear that

$$l_{ij}(x) \leqslant \widehat{l}_j(x) \text{ and } \sum_{i=1}^{n} l_{ij}(x) \leqslant n\widehat{l}_j(x).$$

The map $\widehat{l}$ has been constructed to have the following useful property. If x is a vector in $(K^*)^n$, we can link the image of x under the logarithmic map to the infinite height of x as follows:

$$\begin{aligned} \sum_j \widehat{l}_j(x) &= \sum_{j=1}^{r_1+r_2} \widehat{l}_j(x) \\ &= \sum_{j=1}^{r_1+r_2} n_j \max_i \log|\sigma_j(x_i)| \\ &= H_\infty(x). \end{aligned}$$

$\widehat{l}(x)$ is a richer invariant than $H_\infty(x)$. We will use it to help us to compare $H_\infty(x)$ with $\|x\|$.

3.3.1 The image of $\widehat{l}$ in $\mathbb{R}^{r_1+r_2}$

Let $z_1, \ldots, z_{r_1+r_2}$ be coordinates on $\mathbb{R}^{r_1+r_2}$. We define $\Pi(h)$ to be the hyperplane given by $\sum_j z_j = h$ in $\mathbb{R}^{r_1+r_2}$. Then every $x \in (K^*)^{N+1}$ such that $H_\infty(x) = h$ has image $\widehat{l}(x) \in \Pi(h)$. By choosing a representative x of P that has $H_f(x)$ as large as possible, $H_\infty(x)$ is minimised. In this case the image of x under $\widehat{l}$ lies on the hyperplane $\Pi(H_\infty(x))$ and the distance of this hyperplane from the origin has been minimised. By considering representatives of P with minimal infinite height h we will restrict our search for representatives of P to only those $x \in \mathcal{O}_K^n$ that map to $\Pi(h)$ under $\widehat{l}$.

An important specialisation occurs when K is $\mathbb{Q}$ or when K is an imaginary quadratic field. In this case $r_1 + r_2 = 1$, so the unit rank of K is 0 and $\Pi(h)$ is simply the point $z_1 = h$ on the real line. Much of what follows will be trivially true in this situation; we will refer to this as the "unit rank 0" case.

The length $\|x\|$ is related to the logarithmic embedding $l(x)$ by

$$\|(x_0, \ldots, x_N)\|^2 = \sum_{i,j} n_j |\sigma_j(x_i)|^2 = \sum_{i,j} n_j \exp(l_{ij}(x))^{2/n_j},$$

and we know that $\widehat{l}_j(x) \geqslant l_{ij}(x)$ for every i. We use this relationship when we come to construct a function $\mu : \mathbb{R}^{r_1+r_2}$ that links $\widehat{l}(x)$ to an upper bound for $\|x\|$. We will show that μ is convex and eventually use this to derive a bound B_L so that every point $P \in \mathbb{P}^N(K)$ such that $H(P) \leqslant B_H$ has a representative with T_2-norm less than or equal to B_L.

Let $\mu : \mathbb{R}^{r_1+r_2} \to \mathbb{R}$ be given by

$$\mu(z_1, \ldots, z_{r_1+r_2}) = (N+1) \sum_j n_j (\exp(z_j))^{2/n_j}.$$

We will define what it means for a function to be convex and give a useful property of convex functions, before proving that μ is convex.

3.3.2 Convexity of μ

We will use the following criterion to show that μ is convex.

Theorem 3.3 (Theorem 4.5 of [27]). *If f is a twice continuously differentiable real-valued function on an open convex set C in $\mathbb{R}^n$, then f is convex on C if and only if its Hessian matrix*

$$H(f)(x) = \left(\frac{\partial^2 f}{\partial z_i \partial z_j}(x) \right)_{ij}$$

is positive semi-definite for every $x \in C$.

We will use the following fact later to derive an upper bound for the value of μ on a polytope contained in $\Pi(h)$.

Theorem 3.4 (Corollary 32.3.2 of [27])**.** *Let f be a convex function and let C be a non-empty closed bounded convex set contained in the relative interior of the domain of f. Then the supremum of f relative to C is finite and it is attained at some extreme point of C.*

In the case where C is a polytope, the extreme points of C are exactly its vertices.

Proposition 3.5. *There exists a convex function $\mu : \mathbb{R}^{r_1+r_2} \to \mathbb{R}$ that satisfies*

$$\mu \circ \widehat{l}(x) \geqslant \|x\|^2.$$

Proof. Let μ be as defined at the end of Section 3.3.1. Noticing that

$$\|(x_0, \ldots, x_N)\|^2 = \sum_{i,j} n_j \left(\exp(l_{ij}(x))\right)^{2/n_j} \leqslant (N+1) \sum_j n_j \left(\exp\left(\widehat{l}_j(x)\right)\right)^{2/n_j},$$

we see that

$$\mu \circ \widehat{l}(x) \geqslant \|x\|^2.$$

We wish to check that μ is convex on $\mathbb{R}^{r_1+r_2}$. Differentiating μ,

$$\frac{\partial^2 \mu}{\partial z_j \partial z_i} = \begin{cases} \frac{4}{n_j}(N+1)\exp(z_j)^{2/n_j} & \text{if } i = j \\ 0 & \text{if } i \neq j. \end{cases}$$

This implies that the Hessian matrix for μ is diagonal with positive entries, therefore positive definite. By Theorem 3.3, μ is a convex function. □

3.4 The effect of units

We have found a way to define integral representatives of P whose finite height $H_f(x)$ is as large as possible, by choosing a representative $x \in \mathcal{O}_K^{N+1}$ such $I(x) = I(P)$. This minimises $H_\infty(x)$ amongst integral representatives for P. Such an x is unique only up to multiplication by units of $\mathcal{O}_K$; multiplication by a non-unit would change the ideal $I(x)$.

Recall that $\widehat{l}(x) \in \Pi(H_\infty(x))$. We will study the effect of multiplication by units on the image of x under $\widehat{l}$, and use μ to relate this to $\|x\|$.

The logarithmic map l maps all units of $\mathcal{O}_K$ into the hyperplane $\Pi(0) \subset \mathbb{R}^{r_1+r_2}$. We find that $l(\zeta) = (0, \dots, 0)$ for every root of unity ζ in K, so we need only consider products of fundamental units. Because scaling by a root of unity does not change the length, infinite height or finite height of a point in $(K^*)^{N+1}$ and it does not affect its image under $\widehat{l}$, we work from now on in an environment defined only up to multiplication by roots of unity. The images under l of the units of $\mathcal{O}_K$ form a lattice of full rank in $\Pi(0)$ because l is an injective homomorphism of $\mathbb{Z}$-modules from $\mathcal{O}_K^*/\mu(K)$ into $\Pi(0)$. A fundamental unit ε_k is a basis element of $\mathcal{O}_K^*$ (modulo roots of unity); we call its image $R_k := l(\varepsilon_k) \in \mathbb{R}^{r_1+r_2}$. The R_k form a basis for a lattice Λ, the image under l of the units of K, lying in $\Pi(0)$. Notice that a different choice of fundamental units would mean only a change of basis for Λ.

In the unit rank 0 case there are no fundamental units as the only units of $\mathcal{O}_K^*$ are roots of unity. The hyperplane $\Pi(0)$ is simply the origin, we take $\Lambda = \Pi(0)$.

We consider the effect of scaling an element of $(K^*)^{N+1}$ by a product of fundamental units:

$$\begin{aligned}
\widehat{l}\left(\prod_k \varepsilon_k^{t_k} x\right) &= \widehat{l}\left(\prod_k \varepsilon_k^{t_k} x_0, \dots, \prod_k \varepsilon_k^{t_k} x_N\right) \\
&= \Bigg(\widehat{l}_1(x) + \sum_k t_k n_1 \log|\sigma_1(\varepsilon_k)|, \dots, \\
&\qquad\qquad \widehat{l}_{r_1+r_2}(x) + \sum_k t_k n_{r_1+r_2} \log|\sigma_{r+s}(\varepsilon_k)|\Bigg) \\
&= \left(\widehat{l}_1(x), \dots, \widehat{l}_{r_1+r_2}(x)\right) + \sum_k t_k R_k \\
&= \widehat{l}(x) + l\left(\prod_k \varepsilon_k^{t_k}\right).
\end{aligned}$$

We see that scaling by a vector x by a unit moves the logarithmic image by the corresponding lattice vector in Λ. This gives an action of the lattice Λ on the hyperplane $\Pi(H_\infty(x))$. Vectors in $(K^*)^{N+1}$ are unit multiples of one another if and only if their images under $\widehat{l}$ are equivalent under the action of Λ. Let $C(h)$ be a fixed fundamental domain for the action of Λ on $\Pi(h)$. For every $x \in (K^*)^n$ such that $H_\infty(x) = h$, there exists a unit $u \in \mathcal{O}_K^*$ such that $\widehat{l}(ux) \in C(h)$.

Proposition 3.6. *Let $P \in \mathbb{P}^N(K)$, with no zero coordinates. Then there exists a representative $x \in \mathcal{O}_K^{N+1}$ for P satisfying*

$$H_\infty(x) = H(P) + \log(\mathcal{N}(I(P))),$$

and

$$\widehat{l}(x) \in C(H_\infty(x)) \subset \Pi(H_\infty(x)).$$

Proof. The first part is a step in the proof of Proposition 3.2. The second is a consequence of the fact that the image of $\mathcal{O}_K^*$ under l forms a lattice Λ acting on $\Pi(h)$. Multiplying x by a unit allows us to move its image inside $\Pi(h)$ to be in $C(h)$. □

We have already proven that given a point $P \in \mathbb{P}^N(K)$ there exists a representative x for P with $H_\infty(x) = H(P) + \log(\mathcal{N}(I(P)))$ for which

$$\widehat{l}(x) \in \Pi(H(P) + \log(\mathcal{N}(I(P)))),$$

holds. If we specify a particular fundamental domain for the action of Λ on $\Pi\big(H(P) + \log(\mathcal{N}(I(P)))\big)$, then by evaluating the maximum value of μ on that region we can identify an upper bound for $\|x\|$ for those $x \in \mathcal{O}_K^{N+1}$ that map into that fundamental domain. Proposition 3.6 proves that such a representative x for P exists.

3.5 A fundamental domain for the action of Λ on $\Pi(h)$

In this section we will choose a fundamental domain for the action of the lattice Λ on the hyperplane $\Pi(h) \subset \mathbb{R}^{r_1+r_2}$ for each h. We recall that in the unit rank 0 case, such a fundamental domain is the point $\Pi(h)$.

Many choices of fundamental domain would suffice for the purpose of finding an upper bound on $\|x\|$. We wish both for a simple calculation and for the maximal value of μ on the fundamental domain to be reasonably small. Although not optimal, we believe that the following represents a reasonable choice.

3.5.1 A base point that is a minimum for μ

We will base our fundamental domain around the point of $\Pi(h)$ for which the value of μ is minimal. The hyperplane given by $\Pi(h) = \{g(z_1, \ldots, z_{r_1+r_2}) := \sum_{j=1}^{r_1+r_2} z_j = h\}$ forms our constraint, so using Lagrange multipliers (see for example [1] page 1109) we wish to solve the equation

$$\nabla\mu = \lambda\nabla g,$$

for some $\lambda \in \mathbb{R}$. It is clear that $\nabla g = (1, \ldots, 1)$ so this is equivalent to saying that $\frac{\partial\mu}{\partial z_j} = \lambda$ for all j. We solve for z_j: the equation

$$\lambda = \frac{\partial\mu}{\partial z_j} = 2(N+1)\left(\exp(z_j)\right)^{2/n_j},$$

holds if and only if

$$z_j = \frac{n_j}{2} \log \left(\frac{\lambda}{2(N+1)} \right).$$

We then use the constraint given by the fact that $(z_1, \ldots, z_{r_1+r_2}) \in \Pi(h)$:

$$\begin{aligned} h = \sum_{j=1}^{r_1+r_2} z_j &= \sum_{j=1}^{r_1+r_2} \frac{n_j}{2} \log \left(\frac{\lambda}{2(N+1)} \right) \\ &= \left(\frac{r_1 + 2r_2}{2} \right) \log \left(\frac{\lambda}{2(N+1)} \right), \end{aligned}$$

which can be simplified to

$$\frac{2h}{d} = \log \left(\frac{\lambda}{2(N+1)} \right),$$

and we solve to find that

$$z_j = \frac{n_j h}{d}. \tag{3.1}$$

Let $z_{\min}(h)$ be the point in $\mathbb{R}^{r_1+r_2}$ defined by equation 3.1. The value of μ at $z_{\min}(h)$ is $(N+1)d\exp(2h/d)$, which is a minimum for μ on $\Pi(h)$.

3.5.2 A fundamental domain

We choose our fundamental domain $C(h)$ to be the parallelotope with edges parallel to the directions of logarithmic embeddings of units R_k and centred at the $z_{\min}(h)$. This is clearly a closed, convex region with vertices that we can calculate.

$$C(h) = \left\{ z_{\min}(h) + \sum_{k=1}^{r_1+r_2-1} \lambda_k R_k : \lambda_k \in [-1/2, 1/2] \right\}$$

The extreme points of $C(h)$ are the points $z_{\min}(h) + \sum_k \lambda_k R_k$ where each $\lambda_k = \pm 1/2$. There are $2^{r_1+r_2-1}$ of them and by Theorem 3.4 the maximum value for μ on $C(h)$ is attained at (at least) one of them.

3.5.3 Maximum value of μ on the fundamental domain $C(h)$

To find a maximum value of μ on $C(h)$ we need to evaluate μ at the extreme points of $C(h)$. For convenience, we define a constant

$$c_K = \begin{cases} \sum_j n_j \prod_k \exp\bigl(|\log|\sigma_j(\varepsilon_k)||\bigr) & \text{if the unit rank of } K > 0, \\ 2 & \text{if } K \text{ is imaginary quadratic,} \\ 1 & \text{if } K = \mathbb{Q}. \end{cases} \tag{3.2}$$

After fixing a set of fundamental units for K, c_K depends only on K. It may be beneficial to choose these fundamental units carefully to attempt to minimise the bounds that follow.

Proposition 3.7. *Let $x \in C(h)$. Then*

$$\mu(x) \leqslant (N+1)\exp(2h/d)c_K.$$

Proof. Because μ is convex and $C(h)$ is a polytope, μ attains its maximum on $C(h)$ at one of the vertices of $C(h)$. We evaluate μ at these points:

$$\begin{aligned} \mu\left(z_{\min} + \sum_k \lambda_k R_k\right) &= (N+1)\sum_j n_j \left(\exp\left(n_j h/d + \sum_k \lambda_k n_j \log|\sigma_j(\varepsilon_k)|\right)\right)^{2/n_j} \\ &= (N+1)\sum_j n_j \left(\exp(n_j h/d)\right)^{2/n_j} \prod_k |\sigma_j(\varepsilon_k)|^{2\lambda_k} \\ &= (N+1)\sum_j n_j \exp(2h/d) \prod_k |\sigma_j(\varepsilon_k)|^{2\lambda_k} \\ &= (N+1)\exp(2h/d)\sum_j n_j \left|\sigma_j\left(\prod_k \varepsilon_k^{2\lambda_k}\right)\right|. \end{aligned}$$

To avoid calculating this for each of the $2^{r_1+r_2-1}$ possible sets of values for $\lambda_k = \pm 1/2$, we choose for each λ_k the larger value of the values of $|\sigma_j(\varepsilon_k^{2\lambda_k})|$ for $\lambda_k = \pm 1/2$ in the following way. Because

$$\begin{aligned} \bigl|\log|\sigma_j(\varepsilon_k)|\bigr| &\geqslant \pm\log\bigl|\sigma_j(\varepsilon_k)\bigr| \\ &= \log\bigl|\sigma_j(\varepsilon_k^{\pm 1})\bigr|, \end{aligned}$$

we see that

$$\max|\sigma_j(\varepsilon_k^{\pm 1})| = \exp\bigl|\log|\sigma_j(\varepsilon_k)|\bigr|.$$

We substitute this maximum value to find that

$$\mu\left(z_{\min}(h)+\sum_k \lambda_k R_k\right) \leqslant (N+1)\exp(2h/d)c_K,$$

and this upper bound is attained at one of the vertices of $C(h)$. □

Note that the maximum value of μ on $C(h)$ depends only on h, the ambient dimension N, the number field K and a choice of fundamental units. We may calculate $(N+1)\exp(2/d)c_K$ once for a given number field and ambient dimension and then scale for the parameter h.

We are now ready to state a result relating the height and length of representatives of projective points.

Theorem 3.8. *Let $P \in \mathbb{P}^N(K)$, with no zero coordinates. Recall that $I(P)$ is an integral ideal in the ideal class of P with minimal norm. Then there exists a representative $x \in \mathcal{O}_K^{N+1}$ for P satisfying*

$$\|x\|^2 \leqslant (N+1)\exp\left(\frac{2(H(P)+\log(\mathcal{N}(I(P))))}{d}\right)c_K.$$

Proof. Proposition 3.6 shows that we may choose a representative x so that x has infinite height equal to $H(P)+\log(\mathcal{N}(I(P)))$ and so that $\widehat{l}(x)$ lies in our chosen fundamental domain $C\big(H(P)+\log(\mathcal{N}(I(P)))\big)$. The function μ is convex and satisfies $\mu\circ\widehat{l}(x) \geqslant \|x\|^2$ by Proposition 3.5. The result then follows from Proposition 3.7. □

3.6 Dimension reduction

Because we have used the logarithmic map which can be applied only to $(K^*)^{N+1}$, our results so far only apply to projective points that have no zero coordinates. We show in this section that a point with zero coordinates has the same height and length as a certain point without zero coordinates in a projective space of smaller dimension. We assume the 0th coordinate to be 0 for simplicity of exposition.

Lemma 3.9. *Let $(0,x_1,\ldots,x_N) \in K^{N+1}$ with not all of the x_i equal to 0 and let $P=[0,x_1,\ldots,x_N] \in \mathbb{P}^N(K)$. Then $(x_1,\ldots,x_N) \in K^N$ represents a point $P' \in \mathbb{P}^{N-1}(K)$ such that*

$$H(P)=H(P') \qquad \textit{and} \qquad \|(0,x_1,\ldots,x_N)\| = \|(x_1,\ldots,x_N)\|.$$

Proof. We recall the formal definition that $\log(0) = -\infty$ and that

$$H(P) = \sum_{v \in M_K} \max_i \log |x_i|_v.$$

Because there is some $x_i \neq 0$, for each place $v \in M_K$ there is some $|x_i|_v > -\infty$, so a zero coordinate will not contribute to the sum. Therefore we can conclude that $H(P) = H(P')$. Since $\sigma_j(0) = 0$ for all j, the contribution to the length from the 0th coordinate is zero. □

Lemma 3.9 shows that every point P in $\mathbb{P}^N(K)$ with exactly q zero coordinates ($q \leqslant N$) has the same height as a point P' with no zero coordinates in $\mathbb{P}^{N-q}(K)$ and every representative for P has the same length as a representative for P'.

3.7 A bound on vector length

The bound in Theorem 3.8 only applies to projective points of $\mathbb{P}^N(K)$ without zero coordinates. We extend this result using Lemma 3.9 to prove that the same bound applies to all points of $\mathbb{P}^N(K)$. This is the main result of this chapter.

Theorem 3.10. *Let K be a number field and c_K as defined in equation 3.2. Let A be a set of integral representatives for the ideal classes of K with minimal norm and let $N_K = \max_{\mathfrak{a} \in A} \mathcal{N}(\mathfrak{a})$.*

Let $B_H > 0$. Then every $P \in \mathbb{P}^N(K)$ such that $H(P) \leqslant B_H$ has a representative $x \in \mathcal{O}_K^{N+1}$ such that

$$\|x\|^2 \leqslant B_L$$

where

$$B_L = (N+1) \exp\left(\frac{2(B_H + \log(N_K))}{d}\right) c_K.$$

Proof. By Lemma 3.9 combined with Theorem 3.8 we see that every point in $\mathbb{P}^N(K)$ with q zero coefficients has a representative whose length is less than or equal to

$$(N+1-q) \exp\left(\frac{2(B_H + \log(\mathcal{N}(I(P))))}{d}\right) c_K.$$

The maximum value of $(N+1-q)$ is $(N+1)$ and so the upper bound given by Theorem 3.8 holds for projective points with any number of zero coefficients. The result then follows from the fact that the maximum value of $\mathcal{N}(I(P))$ amongst all projective points is N_K. □

3.8 Examples

It is clear that the upper bound on the squared length of a representative x for points with logarithmic height less than or equal to B_H depends only on the number field, the ambient dimension and the height bound. To get a better understanding of this quantity we calculate it for several examples of number fields $K = \mathbb{Q}(x)/f(x)$.

$f(x)$	(r_1, r_2)	N_K	$c_K \leqslant$	B_L
x	$(0, 0)$	1	1	$(N+1)\exp(2B_H)$
x^2+1	$(0, 1)$	1	2	$2(N+1)\exp(B_H)$
x^2-5	$(2, 0)$	1	3.236068	$3.236068(N+1)\exp(B_H)$
x^2+31	$(0, 1)$	2	2	$4(N+1)\exp(B_H)$
x^3-2	$(1, 1)$	1	7.7702405	$7.7702405(N+1)\exp(\frac{2}{3}B_H)$
$x^3-59x-132$	$(3, 0)$	16	14413078	$91517338(N+1)\exp(\frac{2}{3}B_H)$
x^4-x-1	$(2, 1)$	1	9.2888648	$9.2888648(N+1)\exp(\frac{1}{2}B_H)$
$g(x)$	$(2, 3)$	1	33.749686	$33.749686(N+1)\exp(\frac{1}{4}B_H)$

We use $g(x)$ to denote $x^8 - x^6 - x^5 - x^3 + x^2 + x - 1$ to save space in the table. The values of c_K are not necessarily the smallest possible as we have not proved that when the unit rank is greater than 1 the optimal choice of fundamental units has been used. However, the units used form an LLL-reduced basis of Λ and so our value of c_K is likely to be reasonable.

The calculation of the class group (needed to calculate N_K) and fundamental units (needed for c_K) can be slow for fields of large degree; there exist faster methods that depend on the Generalised Riemann Hypothesis. We note that even for number fields of small degree, the constant c_K can get rather large.

Chapter 4

Choosing a prime

A key step in our method of finding rational points on a variety V is to choose a suitable prime. We reduce the variety at the prime and then for each point on the reduced variety construct a lattice of lifts. We require that the chosen prime is a prime of good reduction for V and we impose some further conditions which will improve the theoretical exposition and the implementation of the lattice methods we will later describe.

In this chapter we will explain the kinds of primes we need and want for our methods, show that infinitely many such primes exist and explain our method for finding them.

4.1 Conditions on suitable primes

4.1.1 Good reduction

We require the prime used to be of good reduction for the variety because our constructions in the following chapters require every point on the reduced variety to be smooth. This will be necessary for Hensel lifting in the construction of sets of lifts.

4.1.2 Degree one

Recall from Chapter 2 that a rational prime decomposes in K as $p\mathcal{O}_K = \prod_i \mathfrak{p}_i^{e_i}$ and that each of the $\mathfrak{p}_i$ gives rise to a residue field $\mathcal{O}_K/\mathfrak{p}_i$ with degree $f_i = [\mathcal{O}_K/\mathfrak{p}_i : \mathbb{Z}/p\mathbb{Z}]$. We wish to use primes whose degree is 1 because it allows for quick computation: if $f_i = 1$ then $\mathcal{O}_K/\mathfrak{p}_i \cong \mathbb{Z}/p\mathbb{Z}$ and we take advantage of the fact that arithmetic in $\mathbb{Z}/p\mathbb{Z}$ runs efficiently. By choosing primes with degree 1, we also fix the fact that $\mathcal{N}(\mathfrak{p}) = p$; knowledge of the norm of our prime will be useful when employing the method of finding points described in Chapter 8. When the number field in question is $\mathbb{Q}$, all primes have degree 1.

4.1.3 Principal

Ensuring that the primes we use are always principal has two main benefits. One is ease of exposition: if the prime ideal $\mathfrak{p}$ is principal we may fix a generator π of $\mathfrak{p}$ and work concretely with elements of $\mathcal{O}_K$ at every stage. Secondly it means that our $\mathcal{O}_K$-lattices, whose index-ideal will be a power of $\mathfrak{p}$, will be free. This will allow us to work with bases rather than pseudo-bases for them. (More information on $\mathcal{O}_K$-lattices and pseudo-bases of can be found in Chapter 6.) Principal primes have practical computational advantages too, as Hermite normal form (whose use is described in Chapter 6 in the construction of lattices of lifts) is available for principal ideal domains; we may use the same code even in non-PIDs by taking care to ensure that all ideals arising are principal.

4.1.4 Norm

To a lattice such as the lattices of lifts described in Chapter 6 we may associate an ideal called the index-ideal. We show in Chapter 6 that the index-ideal of a lattice of lifts is a power of the prime used and we give bounds for its exponent.

In Chapter 8 we will describe a way of finding points from a lattice of lifts which requires that the norm of the index-ideal be larger than a given bound. We use the lower bound on the exponent to show that the norm of the index-ideal will be large enough if the norm of the prime we use is greater than a certain bound.

In Chapter 7 we will describe how to use $\mathbb{Z}$-lattice enumeration on any $\mathcal{O}_K$-lattice. In this case, if we use a lattice of lifts there is no need to bound the norm of the prime. In fact, there is a compromise to be found. Large primes cause the lattices of lifts to be sparse, with fewer points to find and check up to a given length bound. On the other hand, the number of rational points on a reduced variety will increase as the prime increases, so more lattices will be constructed and checked.

We will show that there are infinitely many primes of K that satisfy our conditions.

4.2 Decomposition of rational primes

We will obtain primes of K by decomposing rational primes. The following theorem will help us to find primes of degree 1.

Theorem 4.1 (Theorem 4.8.13 of [5]). *Let $K = \mathbb{Q}(\alpha)$ be a number field, where α is an algebraic integer whose (monic) minimal polynomial is denoted $T(x) \in \mathbb{Z}[x]$. Then for any rational prime p not dividing the index $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ one can obtain the prime decomposition of $p\mathcal{O}_K$ as follows. Let*

$$T(X) \equiv \prod_{i=1}^{g} T_i(x)^{e_i} \mod p$$

be the decomposition of T into irreducible factors in $\mathbb{F}_p[x]$, where the T_i are taken to be monic. Then p decomposes as

$$p\mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i},$$

where

$$\mathfrak{p}_i = \langle p, T_i(\alpha) \rangle.$$

Furthermore, the residue degree f_i of $\mathfrak{p}_i$ is equal to the degree of T_i.

The final sentence indicates that we may find a prime of degree 1 in K from a linear factor of the minimal polynomial modulo a rational prime.

4.3 Existence of suitable primes

We have constructed a list of properties that our chosen prime should have, but it is still necessary to prove that such primes exist. In this section we show that all but finitely many primes of K are primes of good reduction for a given variety. We also demonstrate that the set of rational primes whose decomposition in $\mathcal{O}_K$ includes a principal prime of degree 1 has positive density. We will conclude by proving that there are infinitely many principal primes of degree one that are primes of good reduction for the variety.

Proposition 4.2. *Let K be a number field and V, a geometrically smooth projective algebraic variety defined over K. Then there are only finitely many prime ideals $\mathfrak{p}$ of K such that the reduced variety $\bar{V}$ defined over $\mathbb{F}_\mathfrak{p}$ is singular.*

We start by proving a result over algebraically closed fields.

Lemma 4.3. *Let k be an algebraically closed field and V, a projective algebraic variety defined over k by homogeneous polynomials $F_1, \ldots, F_M \in k[X_0, \ldots, X_N]$. Let $\nabla F = \left(\frac{\partial F_i}{\partial X_j}\right)_{ij}$ be the Jacobian matrix of the F_j and let m_l be the determinants* *of* $(N - \dim(V)) \times (N - \dim(V))$ *minors of* $\nabla(F)$. *We call the number of such minors* D. *Then* V *is smooth if and only if there exist* $g_{i,j}$ *and* $h_{l,j} \in k[X_0, \ldots, X_N]$ *and integers* $n_j \geqslant 0$ *such that*

$$\sum_{i=1}^{M} g_{i,j} F_i + \sum_{l=1}^{D} h_{l,j} m_l = X_j^{n_j}, \text{ for each } 0 \leqslant j \leqslant N. \tag{4.1}$$

Proof of Lemma 4.3. V is smooth if and only if there is no point $P \in V(k)$ such that the Jacobian $\nabla F(x)$ for any x representing P has rank less than $N - \dim(V)$. Let $I = \langle F_i, m_l \rangle \subseteq k[X_0, \ldots, X_N]$ be the ideal generated by the defining polynomials F_i and determinants of minors of ∇F. Then V is smooth if and only if the variety $V(I)$ of the ideal I is empty in $\mathbb{P}^N(k)$. The result follows by application of the Projective Weak Nullstellensatz. (See Chapter 3 of [8].) □

Proof of Proposition 4.2. To apply Lemma 4.3, we pass to the algebraic closure $\bar{K}$ of our number field K. By Lemma 4.3 there exist $g_{i,j}$ and $h_{l,j} \in \bar{K}[X_0, \ldots, X_N]$ and integers $n_j \geqslant 0$ such that Equations 4.1 hold.

Let L/K be the finite extension of K given by adjoining all the coefficients of the $g_{i,j}$ and $h_{l,j}$. We can then scale Equations 4.1 so that they have coefficients in the ring of integers $\mathcal{O}_L$ of L. Then there exist $g'_{i,j}$ and $h'_{l,j} \in \mathcal{O}_L[X_0, \ldots, X_N]$ and nonzero $R \in \mathcal{O}_L$ such that the equation

$$\sum_{i=1}^{N} g'_{i,j} F_i + \sum_{l=1}^{D} h'_{j,l} m_l = R X_j^{n_j}$$

holds for each j.

Let $\mathfrak{q}$ be a prime ideal in $\mathcal{O}_L$ and $\mathbb{F}_\mathfrak{q}$ the corresponding residue field. Let $x \mapsto \bar{x}$ denote the $\mathfrak{q}$-reduction map on $\mathcal{O}_L$. Then

$$\sum_{i=1}^{N} \bar{g}'_{i,j} \bar{F}_i + \sum_{l=1}^{D} \bar{h}'_{j,l} \bar{m}_l = \bar{R} X_j^{n_j} \tag{4.2}$$

holds for each j. If $\mathfrak{q}$ does not divide the ideal $R\mathcal{O}_L$ then we can scale Equations 4.2 by the inverse S of R in $\mathbb{F}_\mathfrak{q}$ to obtain the equations

$$\sum_{i=1}^{N} S\bar{g}'_{i,j} \bar{F}_i + \sum_{l=1}^{D} S\bar{h}'_{j,l} \bar{m}_l = X_j^{n_j},$$

where the polynomials $S\bar{g}'_{i,j}$ and $S\bar{h}'_{j,l}$ are now in $\mathbb{F}_\mathfrak{q}[X_0, \ldots, X_N]$. The residue field $\mathbb{F}_\mathfrak{q}$ is an algebraic extension of $\mathbb{F}_\mathfrak{p}$ for a unique prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$. Therefore for such $\mathfrak{p} \subset \mathcal{O}_K$, $Sg^{\bar{\prime}}_{i,j}$ and $Sh^{\bar{\prime}}_{j,l}$ are polynomials defined over the algebraic closure of $\mathbb{F}_\mathfrak{p}$, $\bar{\mathbb{F}_\mathfrak{p}}$. By Lemma 4.3 the variety defined over $\mathbb{F}_\mathfrak{p}$ by all of the $\bar{F_i}$ and $\bar{m_l}$ is non-singular over $\bar{\mathbb{F}_\mathfrak{p}}$ and so over $\mathbb{F}_\mathfrak{p}$. We may therefore conclude that if $\mathfrak{q}$ does not divide R, $\mathfrak{q}$ is a prime of good reduction for V.

It remains to note that since $R \neq 0$ there are only finitely many primes of $\mathcal{O}_L$ dividing $R\mathcal{O}_L$. For each such prime $\mathfrak{q}$ there is a unique prime of K lying below $\mathfrak{q}$, so there are only finitely many primes of K whose decomposition in L contains a prime of L dividing $R\mathcal{O}_L$. We conclude that there can only be finitely many bad primes for V in K. □

4.3.1 Density of primes

In this section we prove that a number field has infinitely many principal primes of degree one. Let K be a number field and let S be a set of primes of K.

Definition 20. *The **Dirichlet density** of S is*

$$\delta(S) = \lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in S} \mathcal{N}(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p}} \mathcal{N}(\mathfrak{p})^{-s}},$$

if this limit exists, where $\mathfrak{p}$ ranges over all primes of K in the denominator.

We will not explain this definition here, but it can be shown (Lemma 3.2 of [7]) that the denominator can be replaced by $\log(1/(s-1))$. The following proposition is a corollary of the Chebotarev density theorem (Theorem 13.4 of [24]).

Proposition 4.4 (Corollary 13.6 of [24]). *Let L/K be a finite extension of number fields of degree n and let $P(L/K)$ be the set of unramified prime ideals of K whose decomposition in L contains a prime of degree 1 over K. Then*

$$\delta(P(L|K)) \geqslant \frac{1}{n}$$

and equality holds if and only if L is a Galois extension of K.

Proposition 4.5. *1. The set of rational primes whose decomposition in K contains a prime of degree one has positive Dirichlet density (within primes of $\mathbb{Q}$).*

2. The set of primes of degree one in K has Dirichlet density 1 in the set of primes of K.

3. The set of principal primes of K has Dirichlet density $1/h_K$ in the set of primes of K, where h_K is the class number of K.

Proof. 1. This follows immediately from the application of Proposition 4.4 to the extension $K/\mathbb{Q}$.

2. We sketch the proof, following Example 3.3 of [7]. It is equivalent to show that the Dirichlet density of the set of primes $\mathfrak{p}$ in K with degree $f_{\mathfrak{p}} > 1$ is zero. We denote this set by $S_{>1}$. For such $\mathfrak{p}|p$, $\mathcal{N}(\mathfrak{p})^{-s} = p^{-f_{\mathfrak{p}}s} \leqslant p^{-2s}$. There are at most $[K : \mathbb{Q}]$ such $\mathfrak{p}$ over each p in $\mathbb{Q}$. Hence the numerator $\sum_{\mathfrak{p}\in S_{>1}} \mathcal{N}(\mathfrak{p})^{-s}$ is bounded above by $[K : \mathbb{Q}] \sum_p p^{-2s}$ and this is bounded for s close to 1. Dividing by $\log(1/(s-1))$ and letting $s \to 1^+$ gives a limit of 0.

3. There exists a Galois extension H of K called the **Hilbert class field** of K (see Section VI.6 of [24]), with the properties that $\mathrm{Gal}(H/K) = \mathrm{Cl}(K)$ and that a prime of K has a prime of degree one in its decomposition in H if and only if it is principal. (In fact, as H is Galois, all primes of H above a principal prime will have degree one.) We apply Proposition 4.4 to the extension H/K and note that $[H : K] = |\,\mathrm{Gal}(H/K)| = |\,\mathrm{Cl}(K)| = h_K$ as H is Galois over K. □

Corollary 4.6. *There are infinitely many principal primes of degree one in K.*

Proof. We start by showing that the density of principal degree one primes of K is the same as the density of principal primes of K. Let S_{prin} be the set of principal primes of K. We know from part 3 of Proposition 4.5 that $\delta(S_{\mathrm{prin}}) = 1/h_K$.

Using the method of proof of part 2 of Proposition 4.5, we show that the density of primes of degree greater than 1 inside S_{prin} is 0:

$$\lim_{s\to1^+} \frac{\sum_{\mathfrak{p}\in S_{>1}\cap S_{\mathrm{prin}}} \mathcal{N}(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p}\in S_{\mathrm{prin}}} \mathcal{N}(\mathfrak{p})^{-s}} = \lim_{s\to1^+} \frac{\sum_{\mathfrak{p}\in S_{>1}\cap S_{\mathrm{prin}}} \mathcal{N}(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p}} \mathcal{N}(\mathfrak{p})^{-s}} \cdot \lim_{s\to1^+} \frac{\sum_{\mathfrak{p}} \mathcal{N}(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p}\in S_{\mathrm{prin}}} \mathcal{N}(\mathfrak{p})^{-s}}$$
$$= 0.h_K = 0.$$

Labelling the set of primes of degree 1 in K as S_1, $\delta(S_{\mathrm{prin}} \cap S_1) = \delta(S_{\mathrm{prin}}) = 1/h_K$. By part 1 of Proposition 4.5, there are infinitely many rational primes whose decomposition in K yields a prime of degree one. Since the density of principal degree one primes of K is positive there are infinitely many principal primes of degree one in K. □

By combining Corollary 4.6 and Proposition 4.2 we have proven that there are infinitely many primes of K suitable for use in the construction of lattices of lifts for any variety.

4.4 Algorithm

We will use Theorem 4.1 to construct an iterator that yields principal primes of degree 1 that are primes of good reduction for our variety V. We do not claim that this algorithm will yield all such primes; in particular we avoid primes that divide $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ so that Theorem 4.1 applies.

Primes of degree one dividing a rational prime p correspond to linear polynomials in the factorisation of $T(x)$ modulo p. If n is a root of $T(x)$ modulo p then $x - n$ is a factor of $T(x)$ and the ideal $\langle p, \alpha - n \rangle$ is a prime dividing p of degree one.

This algorithm comes from Theorem 4.8.13 of [5] and its implementation has been influenced by the rings.number_fields.small_primes_of_degree_one module of Sage [30], written by Nick Alexander.

Algorithm 1: Primes of degree one

```
Input:
    - $K$, a number field with integral primitive element $\alpha$ which has minimal
      polynomial $T \in \mathbb{Z}[x]$,
    - $N$, a lower bound for the norm of primes, by default set to 0,
    - is_good, a function which takes as input a prime ideal of $K$ and outputs
      True or False. Must satisfy is_good($\mathfrak{p}$) = False if $\mathfrak{p} | [\mathcal{O}_K : \mathbb{Z}[\alpha]]$.
Output: - Prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ with degree 1 and norm greater than $N$ for
          which is_good($\mathfrak{p}$) is True.
Procedure:
Set $p$ to be the next prime larger than $N$.
For each root $n$ of $T \mod p$ with $0 \leqslant n < p$:
    set $\mathfrak{p} \leftarrow \langle p, \alpha - n \rangle$.
    If is_good($\mathfrak{p}$) = True:
        yield $\mathfrak{p}$.
Replace $p$ by the next rational prime and repeat the previous step.
```

It is essential that is_good($\mathfrak{p}$) = False for any $\mathfrak{p} | [\mathcal{O}_K : \mathbb{Z}[\alpha]]$. We will also set it to return False for any bad primes for V and all non-principal primes.

Chapter 5

Constructing sets of lifts

The aim of this chapter is to explain the construction of a set of lifts of a point on a reduced variety. We will focus on curves for the main part of the chapter. The general concepts that work for curves apply to all varieties. We will show how to generalise the construction of sets of lifts for curves to the case of higher dimensional varieties towards the end of the chapter. We also explain how we may view these sets of lifts as local analytic parametrisations of residue discs of $V(K_{\mathfrak{p}})$. The material in this chapter was inspired by the method given in [10] but goes significantly further, generalising the procedure explained there.

We will begin with some material about multivariate Taylor expansions, describe the first and second sets of lifts and then explain an inductive step allowing us to continue finding higher lifts. Let V be a variety and $\mathfrak{p}$, a prime. We will construct a sequence of vectors in $\mathcal{O}_K^{N+1}$ that will generate sets of points that are lifts of a particular point of $\bar{V}(\mathbb{F}_{\mathfrak{p}})$ and satisfy the defining polynomials of V modulo powers of $\mathfrak{p}$. This will involve passing to the $\mathfrak{p}$-adic completion of our number field, which makes it easier to prove the existence of the vectors that we require. In practice, we only need to specify them to some finite $\mathfrak{p}$-adic precision. We may do this by truncating the coefficients of a vector $x \in \mathcal{O}_{K_{\mathfrak{p}}}^n$ at the required precision to give an approximation $\widehat{x}$ which actually lies in $\mathcal{O}_K^n$.

5.1 Taylor expansions, polynomial functions and power series

Let G be a multivariate polynomial, an element of $R[X_1, \ldots, X_n]$ for some coefficient ring R. We will use X to denote the vector $(X_1, \ldots, X_n)$.

Definition 21. *The **gradient** vector of G at x is defined by:*

$$\nabla G(x) = \left(\frac{\partial G}{\partial X_1}(x), \dots, \frac{\partial G}{\partial X_n}(x) \right).$$

For any $x \in R^n$, this defines a polynomial

$$\nabla G(x)(X) = \frac{\partial G}{\partial X_1}(x) X_1 + \cdots + \frac{\partial G}{\partial X_n}(x) X_n,$$

which is a linear form in X.

The notation ∇G has been used before and the gradient vector is a special case of the Jacobian matrix. We may interpret $\nabla G(x)(X)$ as a polynomial function of total degree $\deg(G)$. It has degree $\deg(G) - 1$ in x and degree 1 in X.

Lemma 5.1. *For any polynomial $G \in R[X_1, \dots X_n]$ and any $x \in R^n$, the linear form defined by the gradient of G satisfies:*

$$\nabla\big(\nabla G(x)(X)\big)(x)(X) = \nabla G(x)(X).$$

Proof. Because $\nabla G(x)(X)$ is a linear polynomial it is clear that the equality

$$\frac{\partial}{\partial X_i} \nabla G(x)(X) = \frac{\partial G}{\partial X_i}(x),$$

holds for each X_i. □

Definition 22. *The **Hessian** matrix of G is a symmetric matrix of second derivatives defined by*

$$\operatorname{Hess}(G)(x) = \left(\frac{\partial^2 G}{\partial X_i \partial X_j}(x) \right)_{ij}.$$

For any $x \in R^n$, the Hessian of G defines a quadratic form in X given by

$$\operatorname{Hess}(G)(x)(X) = X \operatorname{Hess}(G)(x) X^t = \sum_{i,j=1}^{n} \frac{\partial^2 G}{\partial X_i \partial X_j}(x) X_i X_j.$$

We wish to generalise the idea of the gradient and Hessian and their associated forms. We look at an i-dimensional array of all ith derivatives of G and form the corresponding homogeneous polynomial in $X_1, \dots, X_n$ of degree i. We will use **multi-indices** to ease notation. A multi-index $\alpha = (\alpha_1, \dots, \alpha_n)$ is a list of non-negative integers. We say α has **size** $|\alpha| = \sum_i \alpha_i$. There are finitely many α such that $|\alpha| = m$ for any non-negative integer m. We say that $X^\alpha = X_1^{\alpha_1} ... X_n^{\alpha_n}$. We can also use multi-indexes in defining derivatives: $D^\alpha = \dfrac{\partial^{\alpha_1}}{\partial X_1^{\alpha_1}} \cdots \dfrac{\partial^{\alpha_n}}{\partial X_n^{\alpha_n}}$. We will also need $\alpha! = \prod_i \alpha_i!$.

Definition 23. *The ith **Hessian form** of G at x is given by:*

$$H_i(G)(x)(X) = \sum_{|\alpha|=i} \frac{D^\alpha G(x)}{\alpha!} X^\alpha.$$

We note that $H_0(G)(x)(X) = G(x)$, $H_1(G)(x)(X) = \nabla G(x)(X)$ and $H_2(G)(x)(X) = \mathrm{Hess}(G)(x)(X)$. The ith Hessian form has degree i in X and degree $\deg(G) - i$ in x for $i \leqslant \deg(G)$.

Lemma 5.2. *[Taylor Expansion] Let $y, y' \in R^n$, $G \in R[X_1, \ldots, X_n]$ and c some scalar parameter. Then we may perform a Taylor expansion on G:*

$$G(y + cy') = \sum_{i=0}^{\deg(G)} H_i(G)(y)(cy') = \sum_{i=0}^{\deg(G)} c^i H_i(G)(y)(y').$$

Proof. The first equality is the well-known Taylor expansion formula, the second recognises that $H_i(G)(y)(X)$ is a homogeneous polynomial of degree i in X. □

We wish to generalise the usual Taylor expansion to deal with expressions of the form $G(y_0 + cy_1 + c^2y_2 + \cdots + c^r y_r)$. We will grade the terms of such an expansion by the power of c that appears in the term. A general expression of this kind (especially for arbitrary r and degree of G) looks complicated to formulate, as it involves taking repeated Taylor expansions to fully expand. However, this can be calculated by hand or computer for any particular G and r. We will show in the general case that such an expansion exists, but do not attempt to describe explicitly the relationship with the usual Taylor expansion except in some easy cases.

We work with power series in a scalar parameter c, before specialising to finite sums.

Lemma 5.3. *Let $(y_t)_{t=0}^\infty$ be a sequence of vectors in R^n and $G \in R[X_1, \ldots, X_n]$. Then there exist unique polynomial functions $G_s : (R^n)^{s+1} \to R$ such that:*

$$G\left(\sum_{t=0}^\infty c^t y_t\right) = \sum_{s=0}^\infty c^s G_s(y_0, \ldots, y_s).$$

Proof. Considering $\sum_{t=0}^\infty c^t y_t$ as a vector of power series in c, the existence of the G_s follows by expanding $G(\sum_{t=0}^\infty c^t y_t)$ term by term. Each G_s depends only on

$y_0, \ldots, y_s$ because y_t appears on the left hand side multiplied by c^t. If G_s depends on y_t, then $c^t | c^s$, so $t \leqslant s$. □

To ease notation, we may write $G_s(y_0, \ldots, y_j)$ for some $j > s$. In this case G_s does not depend on any of the y_i for $i > s$, so $G_s(y_0, \ldots, y_j) = G_s(y_0, \ldots, y_s)$. For $j < s$ we may write $G_s(y_0, \ldots, y_j, 0, \ldots, 0)$ to indicate the value of G_s evaluated with the last $s - j - 1$ vectors set to 0. We now use the results of Lemmas 5.3 and 5.2 to find out more information about the $G_s(y_0, \ldots, y_s)$.

Lemma 5.4. *Let G and G_j be as defined in Lemma 5.3. Then,*

$$G_j(y_0, \ldots, y_j) = \nabla G(y_0)(y_j) + G_j(y_0, \ldots, y_{j-1}, 0),$$

for each j.

Proof. By Lemma 5.3, we know that

$$G\left(\sum_{t=0}^{j} c^t y_t\right) = \sum_{s=0}^{m(G,j)} c^s G_s(y_0, y_1, \ldots, y_j, 0, \ldots, 0),$$

and similarly

$$G\left(\sum_{t=0}^{j-1} c^t y_t\right) = \sum_{s=0}^{m(G,j-1)} c^s G_s(y_0, y_1, \ldots, y_{j-1}, 0, \ldots, 0).$$

These sums are finite, as they are simply Taylor expansions of the polynomial G on a finite number of terms. The number of terms $m(G, k) + 1$ depends on the degree of G and the number of terms k.

The coefficients of c^s in these two expressions agree for all $s < j$. Using Lemma 5.2, we take the first two terms of a Taylor expansion of $G\big(\sum_{t=0}^{j} c^t y_t\big)$ with base point $\sum_{t=0}^{j-1} c^t y_t$ to find that:

$$G\left(\sum_{t=0}^{j} c^t y_t\right) = G\left(\sum_{t=0}^{j-1} c^t y_t\right) + \nabla G\left(\sum_{t=0}^{j-1} c^t y_t\right)(c^j y_j) + \text{ higher order terms in } c.$$

Comparing the coefficients of c^j on each side, we conclude that

$$G_j(y_0, \ldots, y_j) = G_j(y_0, \ldots, y_{j-1}, 0) + \nabla G(y_0)(y_j).$$

□

In Lemma 5.3 we show that $G\left(\sum_{t=0}^{\infty} c^t y_t\right)$ may be viewed as a power series in c, with coefficients $G_s(y_0,\dots y_s)$. We may investigate $G\left(\sum_{t=0}^{\infty} c^t y_t\right)$ by performing Taylor expansions recursively:

$$\begin{aligned}
G\left(\sum_{t=0}^{\infty} c^t y_t\right) &= \sum_{i=0}^{\deg(G)} H_i(G)(y_0)\left(\sum_{t=1}^{\infty} c^t y_t\right) \\
&= \sum_{i=0}^{\deg(G)} c^i H_i(G)(y_0)\left(\sum_{t=1}^{\infty} c^{t-1} y_t\right) && \text{(by the homogeneity of } H_i\text{)} \\
&= \sum_{i=0}^{\deg(G)} c^i \sum_{j=0}^{i} H_j\big(H_i(G)(y_0)\big)(y_1)\left(\sum_{t=2}^{\infty} c^{t-1} y_t\right) \\
&= \sum_{i=0}^{\deg(G)} c^i \sum_{j=0}^{i} c^j H_j\big(H_i(G)(y_0)\big)(y_1)\left(\sum_{t=2}^{\infty} c^{t-2} y_t\right). && (5.1)
\end{aligned}$$

We can continue with such Taylor expansions as long as we like and the expressions contained therein will get more and more complicated. By comparing this sort of expansion with that of Lemma 5.3 we may check small powers of c to work out the first few G_s explicitly.

$\underline{s = 0}$:

$$G(y_0) = G_0(y_0).$$

$\underline{s = 1}$:

$$\begin{aligned}
G(y_0 + cy_1) &= G(y_0) + c\nabla G(y_0)(y_1) + \text{ h.o.t.} \\
\text{so: } G_1(y_0, y_1) &= \nabla G(y_0)(y_1).
\end{aligned}$$

$\underline{s = 2}$:

$$\begin{aligned}
G(y_0 + cy_1 + c^2y_2) &= G(y_0) + \nabla G(y_0)(cy_1 + c^2y_2) + \\
&\qquad H_2(G)(y_0)(cy_1 + c^2y_2) + \text{ h.o.t.} \\
&= G_0(y_0) + G_1(y_0, y_1) + c^2\nabla G(y_0)(y_2) + \\
&\qquad c^2H_2(G)(y_0)(y_1 + cy_2) + \text{ h.o.t.} \\
\text{so: } G_2(y_0, y_1, y_2) &= \nabla G(y_0)(y_2) + H_2(G)(y_0)(y_1).
\end{aligned}$$

This process looks more complicated at each stage and it quickly becomes difficult to write an explicit expression for G_s in general. We will avoid this difficulty by using Lemma 5.4 to provide the (partial) information about G_s that we need.

We will define a variety V with a tuple of m polynomials which we denote by $\underline{F}$. All of the material in this section may be applied to such a tuple componentwise, using the following notation. We write $H_i(\underline{F})(x)(X)$ for the tuple of polynomials $\left(H_i(F_j)(x)(X)\right)_j$. The degrees of the polynomials in $\underline{F}$ are given by $\deg(\underline{F}) = \left(\deg(F_j)\right)_j$ and we may use this componentwise as follows: if $x = (x_1, \ldots, x_m)$ is a vector of length m and c a scalar parameter then $c^{\deg(\underline{F})}x = \left(c^{\deg(F_1)}x_1, \ldots, c^{\deg(F_m)}x_m\right)$.

5.2 Hensel lifting

Recall that $\mathcal{O}_{K_\mathfrak{p}}$ is the completion of $\mathcal{O}_K$ with respect to the $\mathfrak{p}$-adic metric.

Proposition 5.5 (Hensel's Lemma)**.** *Let $\underline{G}$ be a tuple of m polynomials in n variables (with $m \leqslant n$) defined over $\mathcal{O}_K$. Let $x_1 \in \mathcal{O}_K^n$ satisfy $\underline{G}(x_1) \equiv 0 \mod \mathfrak{p}$ with the Jacobian $\nabla\underline{G}(x_1)$ having full rank $m \mod \mathfrak{p}$. Then there exists an $x \in \mathcal{O}_{K_\mathfrak{p}}^n$ such that $\underline{G}(x) = 0$ and $x \equiv x_1 \mod \mathfrak{p}$.*

Proof. We construct a $\mathfrak{p}$-adically convergent sequence (x_i) of elements of $\mathcal{O}_K^n$ with the property that $\underline{G}(x_i) \equiv 0 \mod \mathfrak{p}^i$. This sequence will define $x \in \mathcal{O}_{K_\mathfrak{p}}^n$.

Because $\nabla\underline{G}(x_1)$ is an $m \times n$ matrix of full rank m, there exists an $m \times m$ submatrix of $\nabla\underline{G}(x_1)$ of full rank $\mod \mathfrak{p}$. For simplicity we may assume without loss of generality that the first m columns of $\nabla\underline{G}(x_1)$ form such a submatrix and denote it by $\nabla\underline{G}(x_1)_m$. There exists an $m \times m$ matrix A with entries in $\mathcal{O}_K$ that forms an inverse to $\nabla\underline{G}(x_1)_m \mod \mathfrak{p}$. Therefore, $A\nabla\underline{G}(x_1) \equiv (I_m|D) \mod \mathfrak{p}$, where I_m is the $m \times m$ identity matrix and D is some $m \times (n-m)$ matrix.

We proceed by induction. Assume that $x_k \in \mathcal{O}_K^n$ satisfies $x_k \equiv x_1 \mod \mathfrak{p}$ and $\underline{G}(x_k) \equiv 0 \mod \mathfrak{p}^k$. Set $x_{k+1} = x_k + \pi^k y$. We will solve for y to find a x_{k+1} such that $\underline{G}(x_{k+1}) \equiv 0 \mod \mathfrak{p}^{k+1}$. We take a Taylor expansion of $\underline{G}(x_{k+1})$ at x_k to find:

$$\underline{G}(x_{k+1}) = \underline{G}(x_k + \pi^k y) \equiv \underline{G}(x_k) + \nabla\underline{G}(x_k)(\pi^k y) \mod \mathfrak{p}^{k+1}.$$

Therefore, $\underline{G}(x_{k+1}) \equiv 0 \mod \mathfrak{p}^{k+1}$ if and only if

$$\nabla\underline{G}(x_k)(\pi^k y) \equiv -\underline{G}(x_k) \mod \mathfrak{p}^{k+1}.$$

We may divide through by π^k:

$$\nabla\underline{G}(x_k)(y) \equiv \frac{-\underline{G}(x_k)}{\pi^k} \mod \mathfrak{p},$$

and because $x_k \equiv x_1 \mod \mathfrak{p}$, we have

$$\nabla \underline{G}(x_1)(y) \equiv \frac{-\underline{G}(x_k)}{\pi^k} \mod \mathfrak{p}. \tag{5.2}$$

Congruence 5.2 holds if and only if

$$A\nabla \underline{G}(x_1)(y) \equiv A\left(\frac{-\underline{G}(x_k)}{\pi^k}\right) \mod \mathfrak{p}.$$

We know that the first m columns of $A\nabla\underline{G}(x_1)$ form an identity matrix $\mod \mathfrak{p}$ and so we choose $y \in \mathcal{O}_K^n$ so that

$$y_i = \begin{cases} \text{the } i\text{th entry of } A\left(\frac{-\underline{G}(x_k)}{\pi^k}\right) & \text{for } 1 \leqslant i \leqslant m, \\ 0 & \text{for } i > m. \end{cases}$$

Then we have

$$A\nabla \underline{G}(x_1)(y) \equiv A\left(\frac{-\underline{G}(x_k)}{\pi^k}\right) \mod \mathfrak{p},$$

so $x_{k+1} = x_k + \pi^k y$ satisfies $x_{k+1} \equiv 0 \mod \mathfrak{p}$ and $\underline{G}(x_{k+1}) \equiv 0 \mod \mathfrak{p}^{k+1}$. We know that $\underline{G}(x_1) \equiv 0 \mod \mathfrak{p}$ so by induction there exists a sequence (x_i) of vectors, each congruent to the last modulo increasing powers of $\mathfrak{p}$: $x_i \equiv x_{i-1} \mod \mathfrak{p}^i$. They also satisfy $\underline{G}(x_i) \equiv 0 \mod \mathfrak{p}^i$. The entries of the x_i form $\mathfrak{p}$-adic Cauchy sequences of elements of $\mathcal{O}_K$; they therefore converge to elements of $\mathcal{O}_{K_\mathfrak{p}}$ and their limit is a vector $x \in \mathcal{O}_{K_\mathfrak{p}}^n$ that is a root of $\underline{G}$. □

Note that, unless $m = n$, x_i is not unique and therefore x is not unique because we made a choice of $m \times m$ submatrix of $\nabla\underline{G}(x_1)$. However, once such a choice has been fixed the values of x_i and therefore of x are unique.

For the next part of this chapter we will be constructing sets of lifts in the case of curves. We will construct vectors that define sets of lifts of a reduced point $\bar{P}$. At each stage we will construct $s_i \in \mathcal{O}_{K_\mathfrak{p}}^{N+1}$ using Hensel lifting but the sets of lifts are actually subsets of $\mathcal{O}_K^{N+1}$. When $x \in \mathcal{O}_{K_\mathfrak{p}}^{N+1}$ we use the notation $\widehat{x} \in \mathcal{O}_K^{N+1}$ for a truncation of x to the necessary precision. For any given $m \in \mathbb{Z}_{>0}$ we have

$$x \equiv \widehat{x} \mod \mathfrak{p}^m.$$

The precision needed will always be clear from the context. By using this notation, we emphasise that there is always an exact $\mathcal{O}_{K_\mathfrak{p}}$-vector x from which the truncated $\mathcal{O}_K$-vector $\widehat{x}$ is taken.

We begin with the first and second sets of lifts, as they are needed for the process of induction.

5.3 First sets of lifts

Let $\mathcal{C}$ be a projective curve in $\mathbb{P}^N$ defined over K by $\underline{F} \in \mathcal{O}_K[X_0, \dots, X_N]$ and let $\mathfrak{p}$ be a principal prime of good reduction for $\mathcal{C}$ with generator π. We note that in general $\mathcal{C}$ may not be a complete intersection and hence may be defined by more than $N-1$ polynomials. However, for any point P on $\mathcal{C}$ (or indeed $\bar{P}$ on $\bar{\mathcal{C}}$) only $N-1$ of the polynomials are needed to define $\mathcal{C}$ at that point. Because $\mathcal{C}$ is smooth, the Jacobian of such a tuple of polynomials will have full rank $N-1$ when evaluated at a representative of P. The choice of tuple of polynomials will vary with P. We will assume for simplicity that our curves are always complete intersections; in practice for each reduced point $\bar{P}$ a suitable tuple of polynomials can be chosen.

Let $\bar{P}$ be a rational point on the reduced curve $\bar{\mathcal{C}}$. We may choose a representative for $\bar{P}$ in $\mathbb{F}_{\mathfrak{p}}^{N+1}$; there are $\mathcal{N}(\mathfrak{p}) - 1$ possible choices, one for each non-zero element of $\mathbb{F}_{\mathfrak{p}}$. By choosing a lift of each coordinate from $\mathbb{F}_{\mathfrak{p}}$ to $\mathcal{O}_K$, we may choose an integral representative s for $\bar{P}$. $s \in \mathcal{O}_K^{N+1}$ satisfies $s \equiv \bar{P} \mod \mathfrak{p}$ and $\underline{F}(x) \equiv 0 \mod \mathfrak{p}$. s is $\mathfrak{p}$-primitive. If it were not then each coordinate of s would be in $\mathfrak{p}$ and reducing $s \mod \mathfrak{p}$ would give the zero vector in $\mathbb{F}_{\mathfrak{p}}^{N+1}$, which does not represent a point in $\mathbb{P}^N(\mathbb{F}_{\mathfrak{p}})$. This choice of s is clearly not unique: the set of all integral representatives for $\bar{P}$ is the set of all $x \in \mathcal{O}_K^{N+1}$ that reduce $\mod \mathfrak{p}$ to some representative of $\bar{P}$ in $\mathbb{F}_{\mathfrak{p}}^{N+1}$. If s is some integral representative for $\bar{P}$, then every integral representative for $\bar{P}$ is given by $cs + \pi y$ for some $c \in \mathcal{O}_K$ satisfying $c \not\equiv 0 \mod \mathfrak{p}$ and some $y \in \mathcal{O}_K^{N+1}$.

Because $\nabla \underline{F}(s)$ has full rank, we may employ Hensel lifting to construct a $\mathfrak{p}$-adic solution from s. By Proposition 5.5 there exists an $s_0 \in \mathcal{O}_{K_{\mathfrak{p}}}^{N+1}$ such that $s \equiv s_0 \mod \mathfrak{p}$ and $\underline{F}(s_0) = 0$. Although s_0 depends on the choice of representative s, the sets we proceed to construct will be unique. We fix s_0 to be a lift of s and recall that $\widehat{s}_0$ will represent a truncation of s_0.

Definition 24. *Let S_k be the set of all points $x \in \mathcal{O}_K^{N+1}$ such that*

$$\begin{aligned} x \textit{ is a representative for } \bar{P} \mod \mathfrak{p} \textit{ and} \\ F(x) \equiv 0 \mod \mathfrak{p}^k. \end{aligned}$$

We note that these sets nest: $S_{k+1} \subseteq S_k$ for each k.

Lemma 5.6. *We have*

$$S_1 = \left\{ c_0 \widehat{s}_0 + \pi y \;\middle|\; c_0 \in \mathcal{O}_K, c_0 \not\equiv 0 \mod \mathfrak{p}, y \in \mathcal{O}_K^{N+1} \right\},$$

where $\widehat{s}_0$ is any $\mod \mathfrak{p}$ approximation to s_0.

Proof. If $x \in S_1$ then x is a representative for $\bar{P} \mod \mathfrak{p}$ and x may be written as $c_0\widehat{s}_0 + \pi y$ for some $c_0 \not\equiv 0 \mod \mathfrak{p}$ and some $y \in \mathcal{O}_K^{N+1}$.

If $x = c_0\widehat{s}_0 + \pi y$ then $\underline{F}(x) \equiv \underline{F}(c_0\widehat{s}_0) \mod \mathfrak{p}$. Because $\underline{F}(x)$ is a set of homogeneous polynomials, $\underline{F}(c_0\widehat{s}_0) \equiv 0$ if and only if $\underline{F}(\widehat{s}_0) \equiv 0 \mod \mathfrak{p}$.

□

S_1 is simply the set of all elements of $\mathcal{O}_K^{N+1}$ that reduce to $\bar{P} \mod \mathfrak{p}$. However, the sets S_i for $i > 1$ have a more complicated structure.

Lemma 5.7. *Let $s_0 \in \mathcal{O}_{K_\mathfrak{p}}^{N+1}$ be as above. Then the Jacobian matrix for $\underline{F}$ evaluated at s_0 gives a surjective linear map $\nabla\underline{F}(s_0)(X) : \mathcal{O}_{K_\mathfrak{p}}^{N+1} \to \mathcal{O}_{K_\mathfrak{p}}^{N-1}$ with s_0 contained in the kernel.*

Proof. The fact that s_0 lies in the kernel of $\nabla\underline{F}(s_0)(X)$ follows from the fact that $\nabla F_j(X)(X) = \lambda_j F_j(X)$ for some scalar λ_j for each F_j, by Euler's theorem on homogeneous functions. $\nabla\underline{F}(s_0)(X)$ is linear, so we need only to prove that $\nabla\underline{F}(s_0)(X)$ is surjective. The matrix $\nabla\underline{F}(s_0)$ has full rank $\mod \mathfrak{p}$, so it defines a surjective map $\mathbb{F}_\mathfrak{p}^{N+1} \to \mathbb{F}_\mathfrak{p}^{N-1}$.

Let $y \in \mathcal{O}_K^{N-1}$. Because $\nabla\underline{F}(s_0)(X)$ is surjective $\mod \mathfrak{p}$ there exists an $x \in \mathcal{O}_K^{N+1}$ such that

$$\nabla\underline{F}(s_0)(x) \equiv y \mod \mathfrak{p}.$$

By Lemma 5.1, the Jacobian of $\nabla\underline{F}(s_0)(X) - y$ is $\nabla\underline{F}(s_0)$ and this has full rank $\mod \mathfrak{p}$. Therefore by Hensel's Lemma (Proposition 5.5) we may lift x, which satisfies $\underline{F}(s_0)(x) - y \equiv 0 \mod \mathfrak{p}$, to a $\mathfrak{p}$-adic solution $x' \in \mathcal{O}_{K_\mathfrak{p}}^{N+1}$ such that $\nabla\underline{F}(s_0)(x') = y$. □

This use of Hensel's Lemma proves the existence of solutions to equations of the form $\nabla\underline{F}(s_0)(X) - y \equiv 0 \mod \mathfrak{p}^m$ for any y and any m and is a key step in the construction of further sets of lifts. By considering the s_i as lying in the $\mathfrak{p}$-adic completion at their construction, we do not have to fix a $\mathfrak{p}$-adic precision at the start or update our calculations at each stage but can use $\widehat{s}_i$ to represent the truncation of s_i to the required precision.

The rank of the kernel of $\nabla\underline{F}(s_0)(X)$ is 2. Choose a vector $s_1 \in \mathcal{O}_{K_\mathfrak{p}}^{N+1}$ that is linearly independent of s_0 modulo $\mathfrak{p}$ (and therefore also linearly independent over

$\mathcal{O}_{K_\mathfrak{p}}$, by the same method as the proof of Lemma 5.7) such that s_0 and s_1 generate the kernel of $\nabla \underline{F}(s_0)(X)$. The new vector s_1 will be used in the construction of the second lattice of lifts.

Lemma 5.8. *If $x \in S_1$ then $x \in S_2$ if and only if $x \equiv c_0(\widehat{s}_0 + \pi c_1 \widehat{s}_1) \mod \mathfrak{p}^2$ for some $c_0, c_1 \in \mathcal{O}_K$ with $c_0 \not\equiv 0 \mod \mathfrak{p}$. Here $\widehat{s}_0$ and $\widehat{s}_1$ are any approximations* $\mod \mathfrak{p}^2$ *and* $\mod \mathfrak{p}$ *respectively.*

Proof. Write $x = c_0\widehat{s}_0 + \pi y \in S_1$ and set $\deg \underline{F} - 1$ to be the multi-index $(\deg(F_i) - 1)_i$. We perform a Taylor expansion based at $c_0\widehat{s}_0$:

$$\begin{aligned} \underline{F}(x) = \underline{F}(c_0\widehat{s}_0 + \pi y) &\equiv \underline{F}(c_0\widehat{s}_0) + \nabla \underline{F}(c_0\widehat{s}_0)(\pi y) \mod \mathfrak{p}^2 \\ &\equiv c_0^{\deg(\underline{F})}\underline{F}(\widehat{s}_0) + \pi c_0^{\deg(\underline{F})-1}\nabla \underline{F}(\widehat{s}_0)(y) \mod \mathfrak{p}^2 \\ &\equiv c_0^{\deg(\underline{F})-1}\pi \nabla \underline{F}(\widehat{s}_0)(y) \mod \mathfrak{p}^2, \end{aligned}$$

because $\widehat{s}_0$ is a $\mod \mathfrak{p}^2$ approximation to s_0. Since $c_0 \not\equiv 0 \mod \mathfrak{p}$, $x \in S_2$ if and only if $\nabla \underline{F}(\widehat{s}_0)(y) \equiv 0 \mod \mathfrak{p}$. This is the case if and only if y is a linear combination of $\widehat{s}_0$ and $\widehat{s}_1$, so $x \in S_2$ if and only if

$$x \equiv c_0\widehat{s}_0 + \pi a_0\widehat{s}_0 + \pi a_1\widehat{s}_1 \mod \mathfrak{p}^2.$$

By relabelling constants, we have

$$x = c_0(\widehat{s}_0 + \pi c_1\widehat{s}_1) + \pi^2 y$$

for some $c_0, c_1 \in \mathcal{O}_K$ such that $c_0 \notin \mathfrak{p}$. As x is an arbitrary element of S_1 and $S_1 \supset S_2$,

$$S_2 = \left\{ c_0(\widehat{s}_0 + \pi c_1\widehat{s}_1) + \pi^2 y \;\middle|\; c_0, c_1 \in \mathcal{O}_K, c_0 \not\equiv 0 \mod \mathfrak{p}, y \in \mathcal{O}_K^{N+1} \right\}.$$

□

5.4 Further sets of lifts

We apply the results of Section 5.1 to the polynomials defining $\mathcal{C}$ at $\bar{P}$ and start to think $\mathfrak{p}$-adically by setting our power series parameter $c = \pi\alpha$.

Lemma 5.9. *There exist tuples of homogeneous polynomials $\underline{F}_j$ with the same de-*

grees as $\underline{F}$, such that

$$\underline{F}\left(\sum_{t=0}^{\infty}(\pi c')^t y_t\right) = \sum_{j=0}^{\infty}(\pi c')^j \underline{F}_j(y_0,\ldots,y_j), \tag{5.3}$$

and

$$\underline{F}_j(y_0,\ldots,y_j) = \nabla\underline{F}(y_0)(y_j) + \underline{F}_j(y_0,\ldots,y_{j-1},0).$$

Proof. Apply Lemmas 5.3 and 5.4 to $\underline{F}$, with $c = \pi c'$.

□

Although the notation $\underline{F}_j$ for the terms in the power series expansion for $\underline{F}$ is similar to that used for that for the individual polynomials F_i in $\underline{F}$, there should be no confusion as the F_i will not feature individually again in this chapter.

5.4.1 Construction of vectors

We are now in position to construct further vectors s_i. We will consider $\underline{F}$ as above:

$$\underline{F}\left(\sum_{t=0}^{\infty}(\pi c')^t y_t\right) = \sum_{s=0}^{\infty}(\pi c')^s \underline{F}_s(y_0,\ldots,y_s),$$

and solve

$$\underline{F}_s(y_0,\ldots,y_s) = 0,$$

for each s in turn.

Recall that $s_0, s_1 \in \mathcal{O}_{K_\mathfrak{p}}^{N+1}$ and that $\underline{F}(s_0) = 0$ and $\nabla\underline{F}(s_0)(s_1) = 0$. We define a sequence of $s_i \in \mathcal{O}_{K_\mathfrak{p}}^{N+1}$ inductively. Let the vector s_i be a solution to

$$\nabla\underline{F}(s_0)(s_i) = -\underline{F}_i(s_0,\ldots,s_{i-1},0),$$

noting that this is satisfied for $i = 0$ and 1.

Such vectors s_i always exist because $\nabla\underline{F}(s_0)$ is surjective, and solutions are unique up to addition of an element of $\ker(\nabla\underline{F}(s_0))$. By definition, the s_i satisfy

$$\underline{F}_i(s_0,\ldots,s_i) = 0,$$

for each i. We note that sequences of vectors $(s_0,\ldots,s_i)$ generated in this way do not necessarily form a linearly independent set, even if $i \leqslant N+1$.

From the definition of the s_i and $\widehat{s}_i$ and our Taylor expansion reduced modulo

$\mathfrak{p}^{i+1}$ we observe that $\underline{F}$ satisfies

$$\begin{aligned}\underline{F}\left(\sum_{t=0}^{i}\pi^t s_t\right) &\equiv \sum_{s=0}^{i}\pi^s \underline{F}_s(s_0,\ldots,s_i) \mod \mathfrak{p}^{i+1}\\ &\equiv \sum_{s=0}^{i}\pi^s \underline{F}_s(\widehat{s}_0,\ldots,\widehat{s}_i) \mod \mathfrak{p}^{i+1}\\ &\equiv 0 \mod \mathfrak{p}^{i+1}.\end{aligned}$$

Theorem 5.10. *The set S_i of all points x in $\mathcal{O}_{K_\mathfrak{p}}^{N+1}$ such that*

$$\begin{aligned}&\underline{F}(x) \equiv 0 \mod \mathfrak{p}^i \text{ and}\\ &x \text{ reduces to } \bar{P} \mod \mathfrak{p}\end{aligned}$$

is defined by

$$S_i = \left\{ c_0(\widehat{s}_0 + c_1\pi\widehat{s}_1 + \ldots + c_1^{i-1}\pi^{i-1}\widehat{s}_{i-1}) + \pi^i y \;\middle|\; \begin{array}{c} c_0, c_1 \in \mathcal{O}_K, \\ c_0 \not\equiv 0 \mod \mathfrak{p}, \\ y \in \mathcal{O}_K^{N+1} \end{array} \right\},$$

where $\widehat{s}_j$ is any $\mod \mathfrak{p}^{i-j}$ approximation to s_j.

Proof. Note that S_1 and S_2 are both of the form described in the statement of Theorem 5.10, as shown in Lemmas 5.6 and 5.8. We proceed by induction.

Assume that

$$S_{i-1} = \left\{ c_0(\widehat{s}_0 + c_1\pi\widehat{s}_1 + \cdots + c_1^{i-2}\pi^{i-2}\widehat{s}_{i-2}) + \pi^{i-1} y \;\middle|\; \begin{array}{c} c_0, c_1 \in \mathcal{O}_K, \\ c_0 \not\equiv 0 \mod \mathfrak{p}, \\ y \in \mathcal{O}_K^{N+1} \end{array} \right\},$$

and recall that $S_i \subseteq S_{i-1}$. If x is an element of S_{i-1} then

$$x = c_0(\widehat{s}_0 + c_1\pi\widehat{s}_1 + \cdots + c_1^{i-2}\pi^{i-2}\widehat{s}_{i-2}) + \pi^{i-1}y,$$

for some $c_0, c_1 \in \mathcal{O}_K$ with $c_0 \not\equiv 0 \mod \mathfrak{p}$ and some $y \in \mathcal{O}_K^{N+1}$. Then, $x \in S_i$ if and only if $\underline{F}(x) \equiv 0 \mod \mathfrak{p}^i$. We perform a Taylor expansion on $\underline{F}$:

$$\begin{aligned}\underline{F}(x) \equiv{}& \underline{F}(c_0(\widehat{s}_0 + c_1\pi\widehat{s}_1 + \cdots + c_1^{i-2}\pi^{i-2}\widehat{s}_{i-2})) +\\ &\qquad \nabla\underline{F}(c_0(\widehat{s}_0 + c_1\pi\widehat{s}_1 + \cdots + c_1^{i-2}\pi^{i-2}\widehat{s}_{i-2}))(\pi^{i-1}y) \mod \mathfrak{p}^i\\ \equiv{}& c_0^{d-1}(c_0\underline{F}(\widehat{s}_0 + c_1\pi\widehat{s}_1 + \cdots + c_1^{i-2}\pi^{i-2}\widehat{s}_{i-2}) + \pi^{i-1}\nabla\underline{F}(\widehat{s}_0)(y)) \mod \mathfrak{p}^i.\end{aligned}$$

Therefore $\underline{F}(x) \equiv 0 \mod \mathfrak{p}^i$ if and only if the congruence

$$\pi^{i-1}\nabla\underline{F}(\widehat{s}_0)(y) \equiv -c_0\underline{F}(\widehat{s}_0 + c_1\pi\widehat{s}_1 + \cdots + c_1^{i-2}\pi^{i-2}\widehat{s}_{i-2}) \mod \mathfrak{p}^i, \tag{5.4}$$

holds. Recalling that the construction of the s_i means that $\underline{F}_t(s_0, \ldots, s_t) = 0$ for all $t \leqslant i-2$, we expand the main part of the right hand side:

$$\begin{aligned}\underline{F}(\widehat{s}_0 + \cdots + c_1^{i-2}\pi^{i-2}\widehat{s}_{i-2}) \equiv \sum_{t=0}^{i-2}(c_1\pi)^t\underline{F}_t(\widehat{s}_0, \ldots, \widehat{s}_t) + &\\ (c_1\pi)^{i-1}\underline{F}_{i-1}(\widehat{s}_0, \ldots, \widehat{s}_{i-2}, 0) \mod \mathfrak{p}^i&\\ \equiv 0 + (c_1\pi)^{i-1}\underline{F}_{i-1}(\widehat{s}_0, \ldots, \widehat{s}_{i-2}, 0) \mod \mathfrak{p}^i.&\end{aligned}$$

We substitute back in to Congruence (5.4):

$$\pi^{i-1}\nabla\underline{F}(\widehat{s}_0)(y) \equiv -c_0(c_1\pi)^{i-1}\underline{F}_{i-1}(\widehat{s}_0, \ldots, \widehat{s}_{i-2}, 0) \mod \mathfrak{p}^i.$$

We divide by π^{i-1} and conclude that $\underline{F}(x) \equiv 0 \mod \mathfrak{p}^i$ if and only if

$$\nabla\underline{F}(\widehat{s}_0)(y) \equiv -c_0c_1^{i-1}\underline{F}_{i-1}(\widehat{s}_0, \ldots, \widehat{s}_{i-2}, 0) \mod \mathfrak{p}. \tag{5.5}$$

Recall that s_{i-1} is defined so that $\nabla\underline{F}(s_0)(s_{i-1}) = -\underline{F}_{i-1}(s_0, \ldots, s_{i-2}, 0)$ and that this definition is unique up to addition of an element of $\ker\nabla\underline{F}(s_0)$. Therefore all solutions to Congruence (5.5) will be of the form

$$y = c_0c_1^{i-1}\widehat{s}_{i-1} + a_0\widehat{s}_0 + a_1\widehat{s}_1 + \pi y',$$

for some $a_0, a_1 \in \mathcal{O}_K$ and $y' \in \mathcal{O}_K^{N+1}$.

After some relabelling of constants we see that if $x \in S_{i-1}$, then $x \in S_i$ if and only if

$$x = c_0(\widehat{s}_0 + c_1\pi\widehat{s}_1 + \cdots + c_1^{i-1}\pi^{i-1}\widehat{s}_{i-1}) + \pi^i y,$$

for some $c_0, c_1 \in \mathcal{O}_K$ with $c_0 \not\equiv 0 \mod \mathfrak{p}$, and some $y \in \mathcal{O}_K^{N+1}$.

$$S_i = \left\{ c_0(\widehat{s}_0 + c_1\pi\widehat{s}_1 + \cdots + c_1^{i-1}\pi^{i-1}\widehat{s}_{i-1}) + \pi^i y \;\middle|\; \begin{array}{c} c_0, c_1 \in \mathcal{O}_K, \\ c_0 \not\equiv 0 \mod \mathfrak{p}, \\ y \in \mathcal{O}_K^{N+1} \end{array} \right\}.$$

Therefore, by induction, S_i takes this form for each $i > 0$. □

5.5 Higher dimensional varieties

The method used to construct lattices of lifts in the case of curves can be extended to work in essentially the same way for higher dimensional varieties. We will generalise our work to describe the sets of lifts for a point on a smooth reduced variety $\bar{V}$, where $\dim(V) \geqslant 1$.

Just as in the case of curves, after finding a lift $s_0 \in \mathcal{O}_{K_{\mathfrak{p}}}^{N+1}$ of $\bar{P}$ the key first step is to find a basis for $\ker(\nabla \underline{F}(s_0))$ that includes s_0. These vectors span the tangent space of $V(K_{\mathfrak{p}})$ at s_0 and this tangent space is $\dim(V)$-dimensional, as V is smooth. To generalise our construction to a variety of dimension D we require D parameters; we will therefore be using multivariate power series.

Let $c = (c_1, \ldots, c_D)$ be a tuple of parameters. When working with univariate power series and Taylor expansions we used a sequence of vectors (y_i). Here we will index vectors by multi-indices: y_α. If γ and α are multi-indices we will say that $\gamma \leqslant \alpha$ if $\gamma_i \leqslant \alpha_i$ for each i. Recall that $|\alpha| = \sum \alpha_i$, and let $n_\alpha = \#\{\gamma : \gamma \leqslant \alpha\}$. We say that $\gamma < \alpha$ if $\gamma \leqslant \alpha$ and $|\gamma| < |\alpha|$ or, equivalently, if $\gamma \leqslant \alpha$ and there is some index i where $\gamma_i < \alpha_i$. If $|\alpha| = 0$ then we will denote it by 0 and if $|\alpha| = 1$ then the multi-index whose ith coefficient $\alpha_i = 1$ will be denoted by i.

Let (y_γ) be a sequence indexed by multi-indices on D variables. The number of multi-indices of size j on D variables is given by $\phi_D(j) = \binom{D+j-1}{j}$. Where the number of variables is unambiguous, we will shorten this to $\phi(j)$. We use the notation $(y_\gamma)_{\gamma \leqslant \alpha}$ to indicate the finite subsequence of (y_γ) consisting of those y_γ such that $\gamma \leqslant \alpha$. We will use the notation $(y_\gamma : \textsf{condition})$ to indicate the sequence (z_γ) where

$$z_\gamma = \begin{cases} y_\gamma & \text{if } \gamma \text{ satisfies } \textsf{condition} \text{ and} \\ 0 & \text{else.} \end{cases}$$

These new notations perform the same functions as the notations described for the sequences that are inputs to G_s on page 38. As an example, $(y_\gamma : \gamma < \alpha)_{\gamma \leqslant \alpha}$ is the finite sequence with one position for each multi-index $\gamma \leqslant \alpha$. Its coefficients are y_γ for each $\gamma < \alpha$ and 0 for α.

Lemma 5.11 (Generalisation of Lemma 5.3). *Let R be a coefficient ring and let $c = (c_1, \ldots, c_D)$ be a tuple of variables. Let (y_α) be a sequence of vectors indexed by multi-indices on D variables and let $G \in R[X_1, \ldots, X_n]$. Then there exist unique* *polynomial functions $G_\alpha : (R^n)^{n_\alpha} \to R$ such that:*

$$G\left(\sum_{j=0}^{\infty}\sum_{|\alpha|=j} c^\alpha y_\alpha\right) = \sum_{j=0}^{\infty}\sum_{|\alpha|=j} c^\alpha G_\alpha((y_\gamma)_{\gamma\leqslant\alpha}).$$

Proof. As in the univariate case, the existence of the G_α follows from a term-by-term expansion of $G\left(\sum_{j=0}^{\infty}\sum_{|\alpha|=j} c^\alpha y_\alpha\right)$. The fact that G_α only depends on $\gamma \leqslant \alpha$ follows for the same reason as in the univariate case: y_γ appears on the left hand side multiplied by c^γ so if G_α depends on y_γ then $c^\gamma | c^\alpha$ and $\gamma \leqslant \alpha$. □

Lemma 5.12 (Generalisation of Lemma 5.4)**.** *Let G and G_α be as in Lemma 5.11. Then we have*

$$G_\alpha((y_\gamma)_{\gamma\leqslant\alpha}) = \nabla G(y_0)(y_\alpha) + G_\alpha((y_\gamma : \gamma < \alpha)_{\gamma\leqslant\alpha}).$$

Proof. This proof is a generalisation of that of Lemma 5.4. We perform a Taylor expansion to allow us to compare $G\left(\sum_{t=0}^{j}\sum_{|\alpha|=t} c^\alpha y_\alpha\right)$ to $G\left(\sum_{t=0}^{j-1}\sum_{|\alpha|=t} c^\alpha y_\alpha\right)$.

$$G\left(\sum_{t=0}^{j}\sum_{|\alpha|=t} c^\alpha y_\alpha\right) = G\left(\sum_{t=0}^{j-1}\sum_{|\alpha|=t} c^\alpha y_\alpha\right) + \nabla G\left(\sum_{t=0}^{j-1}\sum_{|\alpha|=t} c^\alpha y_\alpha\right)\left(\sum_{|\alpha|=j} c^\alpha y_\alpha\right).$$

We compare coefficients of c^α for some $|\alpha| = j$ and find that

$$\begin{aligned} G_\alpha\big((y_\gamma)_{\gamma\leqslant\alpha}\big) &= G_\alpha\big((y_\gamma : |\gamma| \leqslant j-1)_{\gamma\leqslant\alpha}\big) + \nabla G(y_0)(y_\alpha) \\ &= G_\alpha\big((y_\gamma : \gamma < \alpha)_{\gamma\leqslant\alpha}\big) + \nabla G(y_0)(y_\alpha). \end{aligned}$$

□

Let V be a variety of dimension D defined by a tuple of polynomials $\underline{F}$ in $\mathcal{O}_K[X_0, \ldots, X_N]$ and let $\bar{P}$ be a smooth point on the reduced curve $\bar{V}(\mathbb{F}_\mathfrak{p})$. $\underline{F}$ is a tuple of m polynomials where $m \geqslant N - D$. As in the case of curves, exactly $N - D$ polynomials are required to define $\bar{V}$ at any particular reduced point $\bar{P}$. We assume for simplicity that V is a complete intersection, defined by $N - D$ polynomials. In practice, for each reduced point $\bar{P}$ a suitable subset of $\underline{F}$ of size $N - D$ can be found.

We will now construct sets of lifts $S_1 \supset S_2 \supset \ldots$ for $\bar{P}$. We may apply Hensel's Lemma (Proposition 5.5) to $\nabla\underline{F}(\bar{P})$ and so construct $s_0 \in \mathcal{O}_{K_\mathfrak{p}}^{N+1}$, a lift of $\bar{P}$ satisfying $\underline{F}(s_0) = 0$.

For exactly the same reasons as when $D = 1$, the first set of lifts is given by

$$S_1 = \left\{ c_0 \widehat{s}_0 + \pi y \;\middle|\; c_0 \in \mathcal{O}_K, c_0 \not\equiv 0 \mod \mathfrak{p}, y \in \mathcal{O}_K^{N+1} \right\}.$$

By the same argument as Lemma 5.7, $\nabla \underline{F}(s_0)$ defines a surjective linear map $\mathcal{O}_{K_\mathfrak{p}}^{N+1} \to \mathcal{O}_{K_\mathfrak{p}}^{N-D}$. The kernel is $D+1$ dimensional and, as before, $s_0 \in \ker(\nabla \underline{F}(s_0))$. We extend from s_0 to fix a basis $s_0, s_1, \ldots, s_D \in \mathcal{O}_{K_\mathfrak{p}}^{N+1}$ for this kernel. Then $\nabla \underline{F}(s_0)(y) = 0$ if and only if $y = \sum_{i=0}^{D} c_i s_i$ for some $c_0, \ldots, c_D \in \mathcal{O}_{K_\mathfrak{p}}$.

Lemma 5.13 (Generalisation of Lemma 5.8)**.** *The second set of lifts is*

$$S_2 = \left\{ c_0 \left(\widehat{s}_0 + \pi \sum_{i=1}^{D} c_i \widehat{s}_i \right) + \pi^2 y \;\middle|\; c_0, \ldots, c_D \in \mathcal{O}_K, c_0 \not\equiv 0 \mod \mathfrak{p}, y \in \mathcal{O}_K^{N+1} \right\},$$

where $\widehat{s}_0$ is an approximation $\mod \mathfrak{p}^2$ to s_0 and $\widehat{s}_i$ is an approximation $\mod \mathfrak{p}$ to s_i for $1 \leqslant i \leqslant D$.

Proof. Let $x \in S_1$. Then $x \in S_2$ if and only if $\underline{F}(x) \equiv 0 \mod \mathfrak{p}^2$. We write $x = c_0 \widehat{s}_0 + \pi y$. Performing a Taylor expansion on $\underline{F}$ yields:

$$\begin{aligned} \underline{F}(c_0 \widehat{s}_0 + \pi y) &\equiv \underline{F}(c_0 \widehat{s}_0) + \nabla \underline{F}(c_0 \widehat{s}_0)(\pi y) \mod \mathfrak{p}^2 \\ &\equiv c_0^{\deg(\underline{F})-1} \big(c_0 \underline{F}(s_0) + \pi \nabla \underline{F}(\widehat{s}_0)(y) \big) \mod \mathfrak{p}^2. \end{aligned}$$

We know that $c_0 \not\equiv 0 \mod \mathfrak{p}$, so $\underline{F}(x) \equiv 0 \mod \mathfrak{p}^2$ if and only if

$$c_0 \underline{F}(\widehat{s}_0) + \pi \nabla \underline{F}(\widehat{s}_0)(y) \equiv 0 \mod \mathfrak{p}^2.$$

Recall that $\underline{F}(s_0) = 0$, so $\underline{F}(\widehat{s}_0) \equiv 0 \mod \mathfrak{p}^2$ and consequently $x \in S_2$ if and only if

$$\nabla \underline{F}(\widehat{s}_0)(y) \equiv 0 \mod \mathfrak{p}.$$

This means that $y \equiv \sum_{i=0}^{D} a_i \widehat{s}_i \mod \mathfrak{p}$ for some $a_i \in \mathcal{O}_K$. This implies that

$$x \equiv c_0 \widehat{s}_0 + \sum_{i=0}^{D} a_i \widehat{s}_i \mod \mathfrak{p}^2,$$

so, by rearranging constants, we have

$$x = c_0 \left(\widehat{s}_0 + \sum_{i=1}^{D} c_i \widehat{s}_i \right) + \pi^2 y,$$

where $c_i \in \mathcal{O}_K$, $c_0 \not\equiv 0 \mod \mathfrak{p}$ and $y \in \mathcal{O}_K^{N+1}$. □

We may now inductively construct more vectors $s_\alpha \in \mathcal{O}_{K_\mathfrak{p}}^{N+1}$. For each multi-index α we define $s_\alpha \in \mathcal{O}_{K_\mathfrak{p}}^{N+1}$ by:

$$\nabla \underline{F}(s_0)(s_\alpha) = -\underline{F}_\alpha\big((s_\gamma : \gamma < \alpha)_{\gamma \leqslant \alpha}\big).$$

This definition is unique up to the addition of an element of $\ker(\nabla \underline{F}(s_0))$.

Theorem 5.14 (Generalisation of Theorem 5.10)**.** *The ith set of lifts is given by:*

$$S_i = \left\{ c_0 \left(\sum_{j=0}^{i-1} \sum_{|\alpha|=j} \pi^j c^\alpha \widehat{s}_\alpha \right) + \pi^i y \;\middle|\; \begin{array}{c} c_0 \in \mathcal{O}_K, \\ c_0 \not\equiv 0 \mod \mathfrak{p}, \\ c = (c_1 \ldots, c_D) \in \mathcal{O}_K^D, \\ y \in \mathcal{O}_K^{N+1} \end{array} \right\}.$$

Proof. We know from page 50 and Lemma 5.13 that S_1 and S_2 are of the form given in the statement of the Theorem. We proceed by induction. Assume that the $(i-1)$th set of lifts is given by

$$S_{i-1} = \left\{ c_0 \left(\sum_{j=0}^{i-2} \sum_{|\alpha|=j} \pi^j c^\alpha \widehat{s}_\alpha \right) + \pi^{i-1} y \;\middle|\; \begin{array}{c} c_0 \in \mathcal{O}_K, \\ c_0 \not\equiv 0 \mod \mathfrak{p}, \\ c = (c_1 \ldots, c_D) \in \mathcal{O}_K^D, \\ y \in \mathcal{O}_K^{N+1} \end{array} \right\}.$$

If $x \in S_{i-1}$, then $x \in S_i$ if and only if $\underline{F}(x) \equiv 0 \mod \mathfrak{p}^i$. We perform a Taylor expansion on $\underline{F}$:

$$\begin{aligned} \underline{F}(x) &= \underline{F}\left(c_0 \left(\sum_{j=0}^{i-2} \sum_{|\alpha|=j} \pi^j c^\alpha \widehat{s}_\alpha \right) + \pi^{i-1} y \right) \\ &\equiv \underline{F}\left(c_0 \left(\sum_{j=0}^{i-2} \sum_{|\alpha|=j} \pi^j c^\alpha \widehat{s}_\alpha \right)\right) + \nabla \underline{F}\left(c_0 \left(\sum_{j=0}^{i-2} \sum_{|\alpha|=j} \pi^j c^\alpha \widehat{s}_\alpha \right)\right)(\pi^{i-1} y) \mod \mathfrak{p}^i \\ &\equiv c_0^{\deg(\underline{F})-1} \left(c_0 \underline{F}\left(\sum_{j=0}^{i-2} \sum_{|\alpha|=j} \pi^j c^\alpha \widehat{s}_\alpha \right) + \pi^{i-1} \nabla \underline{F}(\widehat{s}_0)(y) \right) \mod \mathfrak{p}^i. \end{aligned}$$

Therefore $\underline{F}(x) \equiv 0 \mod \mathfrak{p}^i$ if and only if

$$\pi^{i-1} \nabla \underline{F}(\widehat{s}_0)(y) \equiv -c_0 \underline{F}\left(\sum_{j=0}^{i-2} \sum_{|\alpha|=j} \pi^j c^\alpha \widehat{s}_\alpha \right) \mod \mathfrak{p}^i. \tag{5.6}$$

Expanding part of the right hand side using Lemma 5.11, we have

$$\begin{aligned}\underline{F}\left(\sum_{j=0}^{i-2}\sum_{|\alpha|=j}\pi^j c^\alpha \widehat{s}_\alpha\right) &\equiv \sum_{j=0}^{i-1}\sum_{|\alpha|=j} c^\alpha \pi^j \underline{F}_\alpha\big((\widehat{s}_\gamma : |\gamma| \leqslant i-2)_{\gamma\leqslant\alpha}\big) \mod \mathfrak{p}^i \\ &= \sum_{j=0}^{i-2}\sum_{|\alpha|=j} c^\alpha \pi^j \underline{F}_\alpha\big((\widehat{s}_\gamma)_{\gamma\leqslant\alpha}\big) + \\ &\qquad\qquad \sum_{|\alpha|=i-1} c^\alpha \pi^{i-1}\underline{F}_\alpha\big((\widehat{s}_\gamma : \gamma < \alpha)_{\gamma\leqslant\alpha}\big).\end{aligned}$$

By the definition of the s_α and Lemma 5.12 we know that

$$\underline{F}_\alpha\big((s_\gamma)_{\gamma\leqslant\alpha}\big) = 0,$$

for each α. Therefore Congruence 5.6 becomes

$$\nabla\underline{F}(\widehat{s}_0)(y) \equiv -c_0 \sum_{|\alpha|=i-1} c^\alpha \underline{F}_\alpha((\widehat{s}_\gamma : \gamma < \alpha)) \mod \mathfrak{p}.$$

From the definition of the s_α, we know that this congruence holds if and only if

$$y = c_0 \sum_{|\alpha|=i-1} c^\alpha \widehat{s}_\alpha + \sum_{i=0}^{D} a_i \widehat{s}_i + \pi y'$$

for some $y' \in \mathcal{O}_K^{N+1}$ and $a_i \in \mathcal{O}_K$. After relabelling constants, we see that $x \in S_i$ if and only if

$$x = c_0\left(\sum_{j=0}^{i}\sum_{|\alpha|=j} c^\alpha \pi^j \widehat{s}_\alpha + \pi^{i+1} y\right)$$

for some $c_0 \in \mathcal{O}_K, c_0 \not\equiv 0 \mod \mathfrak{p}$, $c \in \mathcal{O}_K^D$ and $y \in \mathcal{O}_K^{N+1}$, as required. □

5.6 Implementation

The vectors s_α have been defined $\mathfrak{p}$-adically, and the $\widehat{s}_\alpha$ have been given as arbitrary truncations of the vectors s_α, where the $\mathfrak{p}$-adic precision (that is, an exponent m so that we work modulo $\mathfrak{p}^m$) depends on the context. In practice, we can only work to a finite $\mathfrak{p}$-adic precision to construct each of the $\widehat{s}_\alpha$. Each $\widehat{s}_\alpha$ will be constructed by solving a congruence modulo $\mathfrak{p}$ and Hensel lifting that solution to the required $\mathfrak{p}$-adic precision. It would be highly preferable to fix the $\mathfrak{p}$-adic precision at the start, for two main reasons.

1. Each s_α depends on all s_γ such that $\gamma < \alpha$. We will need to calculate $\widehat{s}_0$ to the highest precision we use. If we decided to increase the precision after some of the $\widehat{s}_\alpha$ had been calculated, this would require a recalculation of every vector.

2. Fixing the $\mathfrak{p}$-adic precision will aid the calculation of the $\underline{F}_\alpha((y_\gamma)_{\gamma \leqslant \alpha})$. Although we can perform Taylor expansions on power series (see Equation 5.1), finding explicit expressions in terms of $\underline{H}_i$ for each $\underline{F}_\alpha$ will be tricky. It is simple to fix a $\mathfrak{p}$-adic precision m and evaluate $\underline{F}(\sum_{i=0}^{m} \sum_{|\alpha|=i} c^\alpha y_\alpha) \in \mathcal{O}_K[c_1, \ldots, c_D, (y_\alpha)_{|\alpha| \leqslant m}]$. Terms with coefficient c^α will then form $\underline{F}_\alpha$.

In Section 6.3 we will discuss our strategy for choosing an appropriate $\mathfrak{p}$-adic precision. This $\mathfrak{p}$-adic precision will coincide with the label i of S_i; the set S_i contains $\mathfrak{p}^i \mathcal{O}_K^{N+1}$ so no vector in S_i need be defined to greater $\mathfrak{p}$-adic precision than i.

5.7 Interpretation of sets of lifts

The construction of the sets of lifts S_i involves passing to the $\mathfrak{p}$-adic completion $\mathcal{O}_{K_\mathfrak{p}}$ of $\mathcal{O}_K$ via Hensel lifting (Proposition 5.5). The fact that $V(K) \subseteq V(K_\mathfrak{p})$ underpins our method of finding representatives for points of $V(K)$. In this section we will discuss $V(K_\mathfrak{p})$ and relate sets of representatives for points of $V(K_\mathfrak{p})$ to the sets of lifts we have constructed, which are sets of possible representatives for points of $V(K)$. Each representative of a point of $V(K_\mathfrak{p})$ must satisfy the defining polynomials $\underline{F}$ of V modulo every power of $\mathfrak{p}$.

Every point of $V(K_\mathfrak{p})$ can be reduced modulo $\mathfrak{p}$ to a point in $V(\mathbb{F}_\mathfrak{p})$. Reduction modulo $\mathfrak{p}$ on $V(K_\mathfrak{p})$ partitions points of $V(K_\mathfrak{p})$ into certain disjoint residue discs, each one associated to a point of $V(\mathbb{F}_\mathfrak{p})$. For each $\bar{P} \in V(\mathbb{F}_\mathfrak{p})$ we construct a lift $s_0 \in \mathcal{O}_{K_\mathfrak{p}}^{N+1}$ of $\bar{P}$ such that $\underline{F}(s_0) = 0$. The vector s_0 is a representative of a point of $V(K_\mathfrak{p})$ and all other integral representatives in $\mathcal{O}_{K_\mathfrak{p}}^{N+1}$ of this point are given by $c_0 s_0$ for some $c_0 \in \mathcal{O}_{K_\mathfrak{p}}$. The residue disc of $V(K_\mathfrak{p})$ corresponding to $\bar{P}$ is the set of points in $V(K_\mathfrak{p})$ that have a representative x satisfying $v_\mathfrak{p}(x - s_0) \geqslant 1$. We aim to find all $\mathfrak{p}$-primitive representatives of such points. The set of $\mathfrak{p}$-primitive representatives for the residue disc of $\mathbb{P}^N(K_\mathfrak{p})$ at $\bar{P}$ contains the residue disc of $V(K_\mathfrak{p})$ at $\bar{P}$ and is given by

$$\mathcal{S}_1 = \left\{ c_0(s_0 + \pi y) \mid c_0 \in \mathcal{O}_{K_\mathfrak{p}}, c_0 \not\equiv 0 \mod \mathfrak{p}, y \in \mathcal{O}_{K_\mathfrak{p}}^{N+1} \right\}.$$

We note that $\mathcal{S}_1 \cap \mathcal{O}_K^{N+1} = S_1$. The subset of $\mathcal{S}_1$ whose elements satisfy $\underline{F}$ is the set of all $\mathfrak{p}$-primitive representatives in $\mathcal{O}_{K_\mathfrak{p}}^{N+1}$ of points of $V(K_\mathfrak{p})$ that lie in the residue disc represented by $\bar{P}$.

By solving each $\underline{F}_\alpha$ to find the vectors (s_α) we construct sets

$$\mathcal{S}_i = \left\{ c_0 \left(\sum_{j=0}^{i} \sum_{|\alpha|=j} \pi^j c^\alpha s_\alpha \right) + \pi^{i+1} y \;\middle|\; \begin{array}{c} c_0 \in \mathcal{O}_{K_\mathfrak{p}}, \\ c_0 \not\equiv 0 \mod \mathfrak{p}, \\ c \in \mathcal{O}_{K_\mathfrak{p}}^D, \\ y \in \mathcal{O}_{K_\mathfrak{p}}^{N+1} \end{array} \right\},$$

that satisfy

$$\mathcal{O}_{K_\mathfrak{p}}^{N+1} \supset \mathcal{S}_1 \supset \cdots \supset \mathcal{S}_{i-1} \supset \mathcal{S}_i \supset \ldots.$$

The set $\mathcal{S}_i$ is the subset of $\mathcal{S}_1$ ($\mathfrak{p}$-primitive representatives for the residue disc of $\mathbb{P}^N(K_\mathfrak{p})$ given by $\bar{P}$) whose elements satisfy $\underline{F}$ modulo $\mathfrak{p}^{i+1}$.

The set of convergent infinite sums

$$\mathcal{S}_\infty = \left\{ c_0 \left(\sum_{j=0}^{\infty} \sum_{|\alpha|=j} \pi^j c^\alpha s_\alpha \right) \;\middle|\; c_0 \in \mathcal{O}_{K_\mathfrak{p}}, c_0 \not\equiv 0 \mod \mathfrak{p}, c \in \mathcal{O}_{K_\mathfrak{p}}^D \right\},$$

gives an analytic parametrisation of $\mathfrak{p}$-primitive representatives of the residue disc of $V(K_\mathfrak{p})$ given by $\bar{P}$. $\mathcal{S}_\infty$ is the limit of the sequence of $\mathcal{S}_i$; alternatively we could see the $\mathcal{S}_i$ as truncations modulo $\mathfrak{p}^{i+1}$ of $\mathcal{S}_\infty$.

The set of all $\mathfrak{p}$-primitive representatives in $\mathcal{O}_{K_\mathfrak{p}}^{N+1}$ of points on $V(K_\mathfrak{p})$ is easier to describe than for $V(K)$ because, in general, the infinite sums of $\mathcal{S}_\infty$ do not converge in $\mathcal{O}_K^{N+1}$. For each i, the set S_i is $\mathcal{S}_i \cap \mathcal{O}_K^{N+1}$ or the set of $\mathcal{O}_K^{N+1}$ points in the truncation of $\mathcal{S}_\infty$ modulo $\mathfrak{p}^{i+1}$. As we truncate s_α to obtain $\widehat{s}_\alpha$, we discard information about $V(K_\mathfrak{p})$.

Chapter 6

Constructing lattices of lifts from sets

6.1 $\mathcal{O}_K$-lattices

In correspondence with the classical notion of $\mathbb{Z}$-lattices as finitely generated free $\mathbb{Z}$-modules, we define $\mathcal{O}_K$-lattices.

Definition 25. *An $\mathcal{O}_K$-**lattice** M is a finitely generated, torsion-free module over $\mathcal{O}_K$.*

Much of the theory of $\mathcal{O}_K$-lattices that we will see applies more generally to modules over Dedekind domains. The first chapter of [6] provides a good introduction and the standard results given here may be found there.

A lattice over $\mathbb{Z}$ is endowed with an associated quadratic form which determines length and angles for vectors in the lattice; our $\mathcal{O}_K$-lattices will have length defined by the T_2-norm as introduced in Chapter 3. This differs from the classical $\mathbb{Z}$-lattice case as $T_2(x, y)$ is not generally a K-bilinear form on K^n and so the T_2-norm is not a quadratic form on K^n. Because $\mathcal{O}_K$ is itself a finitely generated torsion-free $\mathbb{Z}$-module, an $\mathcal{O}_K$-module may also be viewed as a $\mathbb{Z}$-lattice with the T_2-norm inducing the quadratic form. This is a valid quadratic form because $T_2(x, y)$ is a $\mathbb{Q}$-bilinear form on $(\mathbb{Q}^d)^n \cong K^n$.

Although $\mathbb{Z}$-lattices are always free, this is not the case for $\mathcal{O}_K$-modules, which may be torsion-free without being free if $\mathcal{O}_K$ is not a principal ideal domain. Therefore if M is an $\mathcal{O}_K$-lattice we cannot necessarily provide a basis for M; this motivates the use of a pseudo-basis.

Lemma 6.1 (Corollary 1.2.25 of [6])**.** *If M is an $\mathcal{O}_K$-lattice, there exist elements*

$a_1, \ldots, a_n \in M$ and fractional ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ of $\mathcal{O}_K$ such that

$$M = \mathfrak{a}_1 a_1 \oplus \cdots \oplus \mathfrak{a}_n a_n.$$

Such a set $(a_i, \mathfrak{a}_i)$ is called a **pseudo-basis** for M. We may think of M as an abstract $\mathcal{O}_K$-module $M \simeq \oplus_{i=1}^n \mathfrak{a}_i$ with n equal to the rank of M. The ideal class of $\prod_i \mathfrak{a}_i$ is independent of the choice of pseudo-basis and is called the **Steinitz class** of M. (This is Corollary 1.2.25 of [6].) M is free if and only if its Steinitz class is principal.

Lemma 6.2 (Prop 1.4.2 of [6])**.** *The pseudo-basis of an $\mathcal{O}_K$-lattice is not unique. Let $(a_i, \mathfrak{a}_i)$ and $(b_j, \mathfrak{b}_j)$ be two pseudo-bases for an $\mathcal{O}_K$-lattice M and let U be the matrix giving the b_j in terms of the a_i. Then $\prod_i \mathfrak{a}_i = (\det(U)) \prod_j \mathfrak{b}_j$.*

To state the definition and algorithm of LLL-reduction for $\mathbb{Z}$-lattices, one requires Gram-Schmidt orthogonalisation as described on page 82 of [5]. We extend this definition to $K_\mathbb{R}$-vectors; this will be used when we discuss lattice reduction in Chapter 8.

Definition 26. *Let $(b_i, \mathfrak{b}_i)_i$ be a pseudo-basis for an $\mathcal{O}_K$-lattice $M \subset K_\mathbb{R}^n$. Then the **Gram-Schmidt orthogonalisation** of the pseudo-basis vectors b_i may by defined inductively by*

$$b_i^* = b_i - \sum_{j<i} \mu_{ij} b_j^*,$$

where μ_{ij} is given by

$$\mu_{ij} = \frac{T_2(b_i, b_j^*)}{T_2(b_j^*, b_j^*)}.$$

The vectors b_i^* lie in $K_\mathbb{R}^n$, the $K_\mathbb{R}$-span of $\{b_i^*\}_{1 \leqslant i \leqslant m}$ is equal to that of $\{b_i\}_{1 \leqslant i \leqslant m}$ and they are orthogonal: $T_2(b_i^*, b_j^*) = 0$ for all $i \neq j$.

6.1.1 Index-ideals of sub-lattices

We will use the structure of torsion modules over $\mathcal{O}_K$ to help us to understand the index of a sub-lattice in the setting of $\mathcal{O}_K$-lattices. This material can be found in Section 1.2.2 of [6].

Let T be a finitely generated torsion module over $\mathcal{O}_K$. Then there exist elements $a_1, \ldots, a_n \in T$ and non-zero integral ideals $\mathfrak{d}_1, \ldots, \mathfrak{d}_n$ not equal to $\mathcal{O}_K$ such that

$$T = (\mathcal{O}_K/\mathfrak{d}_1)a_1 \oplus \cdots \oplus (\mathcal{O}_K/\mathfrak{d}_n)a_n,$$

and $\mathfrak{d}_{i-1} \subset \mathfrak{d}_i$ for each $2 \leqslant i \leqslant n$. The $\mathfrak{d}_i$ are unique and depend only on the isomorphism class of T. The product of these ideals $\prod_i \mathfrak{d}_i$ is called the **order-ideal** of T.

Let $M \supset L$ be $\mathcal{O}_K$-lattices with the same rank. Then the quotient module M/L is a torsion $\mathcal{O}_K$-module. The order-ideal of M/L will be called the **index-ideal** of L in M and will be denoted $[M : L]$. If $M \supset L \supset N$ are all of the same rank, then their index-ideals satisfy

$$[M : N] = [M : L][L : N].$$

We can construct a special pseudo-basis to relate an $\mathcal{O}_K$-lattice and a sub-lattice.

Lemma 6.3 (Theorem 1.2.35 of [6]). *Let $M \supset L$ be two $\mathcal{O}_K$-lattices of rank n. Then there exist a pseudo-basis $(a_i, \mathfrak{a}_i)$ for M and integral ideals $\mathfrak{d}_1, \ldots, \mathfrak{d}_n$ such that $(a_i, \mathfrak{d}_i\mathfrak{a}_i)$ is a pseudo-basis for L and $\prod_i \mathfrak{d}_i = [M : L]$.*

Lemma 6.4. *Let $M \subset \mathcal{O}_K^n$ be an $\mathcal{O}_K$-lattice of full rank. If M is given by a pseudo-basis $(b_i, \mathfrak{b}_i)$ and B is the $n \times n$ matrix whose rows are the b_i, then*

$$[\mathcal{O}_K^n : M] = \langle \det(B) \rangle \prod_i \mathfrak{b}_i.$$

Proof. We know from Lemma 6.3 that there exists a pseudo-basis $(a_i, \mathfrak{a}_i)$ of $\mathcal{O}_K^n$ and integral ideals $\mathfrak{d}_i$ such that $(a_i, \mathfrak{d}_i\mathfrak{a}_i)$ is a pseudo-basis for M. Therefore we have that

$$[\mathcal{O}_K^n : M] = \prod_i \mathfrak{d}_i.$$

Let A be the matrix with rows given by the a_i. To prove the statement for $(a_i, \mathfrak{d}_i\mathfrak{a}_i)$ it will be enough to show that $\langle \det(A) \rangle \prod_i \mathfrak{a}_i = \mathcal{O}_K$. $\mathcal{O}_K^n$ has a standard pseudo-basis $(e_i, \mathcal{O}_K)$. A has full rank and its inverse A^{-1} is the change-of-basis matrix between the a_i and e_i. From Lemma 6.2 we see that $\prod_i \mathfrak{a}_i = \langle \det(A^{-1}) \rangle \mathcal{O}_K$ and we can conclude that

$$\langle \det(A) \rangle \prod_i \mathfrak{a}_i = \langle \det(A) \rangle \langle \det(A^{-1}) \rangle \mathcal{O}_K = \mathcal{O}_K.$$

It follows quickly from Lemma 6.2 that the result holds for all pseudo-bases of M. □

6.2 Lattices of lifts

We now construct some particular $\mathcal{O}_K$-lattices which we call lattices of lifts. We first recall what we mean by a set of lifts. Let V be a variety of dimension D defined by polynomials $\underline{F}$ in $\mathcal{O}_K[X_0, \ldots, X_N]$. Let $\mathfrak{p}$ be a good prime for V which has degree one and is principal and let $\bar{P}$ be a smooth point on the reduced curve $\bar{V}(\mathbb{F}_{\mathfrak{p}})$. Then the ith set of lifts, S_i, is the set of vectors $x \in \mathcal{O}_K^{N+1}$ that are lifts of $\bar{P}$ mod $\mathfrak{p}$ and which satisfy $F(x) \equiv 0 \mod \mathfrak{p}^i$. S_i is defined by a sequence of vectors $(\widehat{s}_\alpha)_{|\alpha| \leqslant i-1} \in \mathcal{O}_K^{N+1}$ whose construction is explained in Chapter 5. S_i is given by

$$S_i = \left\{ c_0 \left(\sum_{j=0}^{i-1} \sum_{|\alpha|=j} \pi^j c^\alpha \widehat{s}_\alpha \right) + \pi^i y \,\middle|\, c_0 \in \mathcal{O}_K, c_0 \not\equiv 0 \mod \mathfrak{p}, c \in \mathcal{O}_K^D, y \in \mathcal{O}_K^{N+1} \right\}.$$

We will define lattices of lifts from these sets.

Definition 27. *Let S_i be a set of lifts as defined above. Then the **ith lattice of lifts**, L_i, is the $\mathcal{O}_K$-submodule of $\mathcal{O}_K^{N+1}$ generated by*

$$\left\{ \pi^{|\alpha|} \widehat{s}_\alpha \right\}_{|\alpha| \leqslant i-1} \text{ and } \pi^i \mathcal{O}_K^{N+1}.$$

We will see later that L_i is free. A key part of the the method of finding points via lattice reduction explained in Chapter 8 is to construct a lattice L_i for which the norm of the index-ideal of L_i in $\mathcal{O}_K^{N+1}$ is bounded below. To achieve this, we must find out more about the index-ideal of L_i.

Proposition 6.5. *The index-ideal of L_i in $\mathcal{O}_K^{N+1}$ (also called the index of L_i) is $\mathfrak{p}^{m_i}$ for some $m_i \leqslant i(N+1)$.*

Proof. Because S_i is contained in $\mathcal{O}_K^{N+1}$, we have

$$\mathcal{O}_K^{N+1} \supset L_i \supset \mathfrak{p}^i \mathcal{O}_K^{N+1}.$$

The index of $\mathfrak{p}^i \mathcal{O}_K^{N+1}$ in $\mathcal{O}_K^{N+1}$ is $\left[\mathcal{O}_K^{N+1} : \mathfrak{p}^i \mathcal{O}_K^{N+1}\right] = (\mathfrak{p}^i)^{N+1}$. Multiplicativity of indexes shows that

$$[\mathcal{O}_K^{N+1} : L_i][L_i : \mathfrak{p}^i \mathcal{O}_K^{N+1}] = [\mathcal{O}_K^{N+1} : \mathfrak{p}^i \mathcal{O}_K^{N+1}] = \mathfrak{p}^{i(N+1)}. \tag{6.1}$$

□

When $(b_i, \mathfrak{b}_i)$ is a pseudo-basis for L_i, Lemma 6.4 shows that

$$\langle \det(b_1, \ldots, b_n) \rangle \prod_i \mathfrak{b}_i = [\mathcal{O}_K^n : L_i] = \mathfrak{p}^{m_i}.$$

Since $\langle \det(b_1, \ldots, b_n) \rangle$ is a principal ideal, $\prod_i \mathfrak{b}_i$ is principal and L_i is free.

We now wish to find bounds on m_i. Recall that $\phi_D(j)$ is the number of multi-indices on $\deg(V)$ coefficients of degree j; we shorten this to $\phi(j)$.

Theorem 6.6. *The index-ideal of L_i is $\mathfrak{p}^{m_i}$, where*

$$i(N+1) \geqslant m_i \geqslant i(N+1) - \sum_{j=0}^{i-1} \phi(j)(i-j).$$

Proof. We start with the assumption that the set of $\widehat{s}_\alpha$ for $|\alpha| \leqslant i-1$ form a linearly independent set $\mod \mathfrak{p}$. In particular, each of them is $\mathfrak{p}$-primitive. Consider the image of the module generated by $\{\pi^{|\alpha|}\widehat{s}_\alpha\}_{|\alpha| \leqslant i-1}$ in $\mathcal{O}_K^{N+1}/\mathfrak{p}^i\mathcal{O}_K^{N+1}$. This is the same as $L_i/\mathfrak{p}^i\mathcal{O}_K^{N+1}$ and is generated by the images of the $\pi^{|\alpha|}\widehat{s}_\alpha$.

The span of the image of $\pi^{|\alpha|}\widehat{s}_\alpha$ in $\mathcal{O}_K^{N+1}/\mathfrak{p}^i\mathcal{O}_K^{N+1}$ is a finite $\mathcal{O}_K$-module isomorphic to

$$\pi^{|\alpha|}\mathcal{O}_K/\mathfrak{p}^i \simeq \mathcal{O}_K/\mathfrak{p}^{i-|\alpha|}.$$

Therefore, the index of $\mathfrak{p}^i\mathcal{O}_K^{N+1}$ in L_i is given by

$$\left[L_i : \mathfrak{p}^i\mathcal{O}_K^{N+1}\right] = \prod_{j=0}^{i-1} \prod_{|\alpha|=j} \mathfrak{p}^{i-j} = \prod_{j=0}^{i-1} (\mathfrak{p}^{i-j})^{\phi(j)} = \prod_{j=0}^{i-1} \mathfrak{p}^{\phi(j)(i-j)},$$

and hence we have

$$\left[\mathcal{O}_K^{N+1} : L_i\right] = \frac{\left[\mathcal{O}_K^{N+1} : \mathfrak{p}^i\mathcal{O}_K^{N+1}\right]}{\left[L_i : \mathfrak{p}^i\mathcal{O}_K^{N+1}\right]} = \mathfrak{p}^{i(N+1) - \sum_{j=0}^{i-1}\phi(j)(i-j)}.$$

If the $\widehat{s}_\alpha$ are linearly dependent $\mod \mathfrak{p}$ there may be linear relations amongst the images of the $\pi^{|\alpha|}\widehat{s}_\alpha$ in $\mathcal{O}_K^{N+1}/\mathfrak{p}^i\mathcal{O}_K^{N+1}$. These may reduce the rank of the image of the module generated by $\{\pi^{|\alpha|}\widehat{s}_\alpha\}_{|\alpha| \leqslant i-1}$ or reduce the exponent in the index of a generator. Either of these would reduce the exponent of $\mathfrak{p}$ in the index $[L_i : \mathfrak{p}^i\mathcal{O}_K^{N+1}]$ so that it is less than $\sum_{j=0}^{i-1} \phi(j)(i-j)$. Therefore the minimal possible exponent of $\mathfrak{p}$ in $[\mathcal{O}_K^{N+1} : L_i]$ is $i(N+1) - \sum_{j=0}^{i-1} \phi(j)(i-j)$. Proposition 6.5 gives the upper bound on m_i. □

6.3 Implementation

6.3.1 $\mathfrak{p}$-adic precision

In Section 5.6 we discussed the need to construct the vectors $\widehat{s}_\alpha$ using a fixed finite $\mathfrak{p}$-adic precision and noted that this precision matches the label i of S_i and L_i. Now that we know how the exponent of $\mathfrak{p}$ in the index-ideal of a lattice of lifts arises we are ready to discuss what this $\mathfrak{p}$-adic precision should be.

For a fixed prime $\mathfrak{p}$ it is to our benefit to construct a lattice with as large an exponent of $\mathfrak{p}$ in the index-ideal as possible. If we find points by lattice enumeration as in Chapter 7, a large exponent means a sparse lattice with few points to check.

Let $\psi(j)$ indicate the number of linearly independent vectors added at stage j of the construction of vectors $\widehat{s}_\alpha$. If, at stage j, fewer than N linearly independent vectors $\widehat{s}_\alpha$ have been constructed, by continuing to stage $j+1$ we increase the exponent of $\mathfrak{p}$. The $\mathfrak{p}$-adic precision we wish to use is k, where k is minimal such that

$$\sum_{j=0}^{k} \psi(j) \geqslant N.$$

If we fix this k then in constructing S_k we generate at least N linearly independent vectors $\pi^{|\alpha|}\widehat{s}_\alpha$. To proceed on to stage $k+1$ would add vectors $\pi^k \widehat{s}_\alpha$ for $|\alpha| = k$, but these vectors were already in L_k as they are contained in $\mathfrak{p}^k \mathcal{O}_K^{N+1}$.

For a variety of dimension D there are $\phi_D(j)$ new vectors constructed at stage j. For each j, we know that $\psi(j) \leqslant \phi_D(j)$. We note that $\psi(j) = \phi_D(j)$ for $j = 0$ or 1, as these vectors are chosen to be a basis for $\ker(\nabla \underline{F}(\widehat{s}_0))$ and therefore are linearly independent. Beyond this, we do not know whether there will be any linear dependence between the $\widehat{s}_\alpha$ before we construct them and so we cannot guarantee choosing the optimal precision. We use $\phi_D(j)$ as a substitute for $\psi(j)$ when we attempt to choose our $\mathfrak{p}$-adic precision. The time required to perform extra Hensel lifting steps on each vector is likely to be small compared to other steps in the point-finding algorithm, so an attempt to overestimate k would not be very detrimental to timing and in some cases could have significant benefits. On this basis, we propose using $\mathfrak{p}$-adic precision k, where k is minimal such that

$$\sum_{j=0}^{k} \phi_D(j) \geqslant N + 2.$$

The frequency of linear dependence between the $\widehat{s}_\alpha$ may merit further investigation.

6.3.2 Constructing a lattice from a set

We have defined the L_i by using the vectors $\widehat{s}_\alpha$ that were constructed in Chapter 5. However, to be able to compute further with L_i we need to construct a pseudo-basis of L_i.

One way to generate a basis of a $\mathbb{Z}$-lattice from a generating set is to apply the Hermite normal form (HNF) algorithm to find an upper-triangular basis. We may specify an $\mathcal{O}_K$-lattice over a principal ideal domain using a basis rather than a pseudo-basis—in this case there is a HNF algorithm that works in the same way as the one over $\mathbb{Z}$. If we work carefully we may use this version of HNF to find a basis for L_i even when $\mathcal{O}_K$ is not a principal ideal domain. By including $\mathfrak{p}^i\mathcal{O}_K^{N+1}$ in the generating set of the lattice we ensure that ideals generated from entries in columns of the matrix during the HNF process are principal: such ideals divide $\mathfrak{p}^i$ so they must be powers of the principal prime $\mathfrak{p}$. This overcomes the only way in which such a HNF algorithm may fail for number fields with class number greater than 1 and is an important reason to choose a principal prime ideal (as in Chapter 4).

Chapter 7

Points from lattices via $\mathbb{Z}$-lattice enumeration

In Chapters 5 and 6 we explained how to construct $\mathcal{O}_K$-lattices of lifts L_i for a variety $V \subset \mathbb{P}^N(K)$. These lattices contain representatives for all rational points of V. As explained in Chapter 3, rational points in $\mathbb{P}^N(K)$ of height $\leqslant B_H$ correspond to vectors of length $\leqslant B_L$ in $\mathcal{O}_K^{N+1}$. To find rational points of V we search for such points in L_i.

In this chapter we will consider the problem of finding points of bounded T_2-norm in an arbitrary $\mathcal{O}_K$-lattice $M \subset \mathcal{O}_K^n$. In Section 7.4 we will give a few remarks that apply to the case $M = L_i$, but the majority of this chapter will be quite general.

One way to find points in an $\mathcal{O}_K$-lattice is to "restrict scalars", i.e., to consider an $\mathcal{O}_K$-lattice of rank n as a $\mathbb{Z}$-lattice of rank nd. Efficient enumeration of $\mathbb{Z}$-lattice points has already been implemented in several computer algebra packages. We will explain how to convert our $\mathcal{O}_K$-lattice to a $\mathbb{Z}$-lattice with the same T_2-norm. Although all of the numbers involved are algebraic and may be described exactly in a computer algebra system, to do so would be expensive. Existing $\mathbb{Z}$-lattice enumeration implementations take floating-point real input in which the real numbers involved are given to finite precision. If it is necessary to prove that all points up to a certain height have been found, it is important to deal with matters of precision to ensure that no points are missed.

7.1 A $\mathbb{Z}$-lattice from an $\mathcal{O}_K$-lattice

Let K be a number field of degree d and let M be an $\mathcal{O}_K$-lattice of rank n given by a pseudo-basis $M = \oplus_{i=1}^{n} \mathfrak{b}_i b_i$. Let T_2 be the function on vectors of $K_{\mathbb{R}}^n$ given by $T_2(x, y) = \sum_{i=1}^{n} \sum_{k=1}^{d} \sigma_k(x_i)\bar{\sigma}_k(y_i)$. As ideals of $\mathcal{O}_K$ are clearly $\mathbb{Z}$-modules of rank d, we may write $\mathfrak{b}_\mathfrak{i} = \oplus_{j=1}^{d} \mathbb{Z}\beta_{i,j}$ and so $M = \oplus_{i,j} \mathbb{Z}\beta_{i,j} b_i$ as a $\mathbb{Z}$-module. For clarity in what follows, we relabel these basis vectors so that $M = \oplus_{i=1}^{nd} \mathbb{Z} b_i$. T_2 provides a quadratic form to allow us to view the $\mathbb{Z}$-module M as a $\mathbb{Z}$-lattice. We may think of the $\mathbb{Z}$-lattice M as $\mathbb{Z}^{nd} \subset \mathbb{R}^{nd}$ with an inner product given by the positive-definite, symmetric matrix $T := (T_2(b_i, b_j))_{ij}$. Although T_2 is not an inner product on $K_{\mathbb{R}}^n$ or K^n as it is not $K_{\mathbb{R}}$- or K-bilinear, it is $\mathbb{Q}$-bilinear and does provide an inner product on $\mathbb{R}^{nd}$.

We encounter issues of precision and accuracy in the construction of the matrix T that we need to consider. The images of elements of K under embeddings σ_k of K into $\mathbb{C}$ are algebraic numbers, to be represented with finite precision. We wish to find all $x \in \mathbb{Z}^{nd}$ such that $x^t T x \leqslant B_L$ for a vector length bound B_L. Approximating T without adjusting B_L could mean that some such points are missed. The next section will explain the precision and the length bound adjustment needed so that provably all points of T_2-norm less than or equal to B_L are found. In practice our vector length bound B_L for vectors in a lattice of lifts will be derived from a bound on height as explained in Chapter 3.

7.2 Precision

The aim of this chapter is to show how to explicitly compute T. The algorithm will be presented on page 69 in Algorithm 2 and we will prove the following theorem.

Theorem 7.1. *Let $\eta > 1$. Then there exists an explicitly calculable $\epsilon > 0$ such that if ϵ is the unit roundoff on floating-point operations, Algorithm 2 constructs an approximation S to the matrix $T := (T_2(b_i, b_j))_{ij}$ such that if x satisfies $x^t T x \leqslant B_L$, then $x^t S x < \eta B_L$.*

To make this precise, we will need some facts about floating-point arithmetic.

7.2.1 Unit roundoff, precision and matrix entry precision

This material can be found in the early chapters of [18]. Fix positive integers p and $e_{\max}$ and a negative integer $e_{\min}$. Then we define the **floating-point approximation** $\mathsf{fl}_p(x)$ of $x \in \mathbb{R}$ to be the nearest number of the form $\pm m 2^{e-p}$ to x, where

$0 \leqslant m \leqslant 2^p - 1$ and $e_{\min} \leqslant e \leqslant e_{\max}$. (We assume that ties are dealt with so that every x in the range available has an unique floating-point approximation.) The **precision** p is the number of binary digits used to represent the **mantissa**, m. IEEE double precision arithmetic is a standard format for floating-point arithmetic; here we have $p = 53$, $e_{\min} = -1021$ and $e_{\max} = 1024$. We define the **unit roundoff** in terms of the precision by $\epsilon = 2^{-p}$. Every $x \in \mathbb{R}$ in the range allowed by our floating-point system can be approximated by a floating-point number with relative error no more than ϵ. For $t \in \mathbb{Z}$ we define $\gamma_t = \frac{t\epsilon}{1-t\epsilon}$ and will assume in all cases that $t\epsilon < 1$. This is entirely reasonable as t will always be less than or equal to nd in our applications and IEEE double precision arithmetic has $\epsilon \approx 10^{-16}$.

Lemma 7.2.

1. *([18], Theorem 2.2) For any $a \in \mathbb{R}$ in the range of our floating-point system,*
$$\mathsf{fl}(a) = a(1+c) \textit{ for some } |c| < \epsilon.$$

2. *([18], Section 2.2) If $a, b \in \mathbb{R}$ are exactly floating-point numbers, i.e. $\mathsf{fl}(a) = a$ and $\mathsf{fl}(b) = b$, then*
$$\mathsf{fl}(ab) = ab(1+c') \textit{ for some } |c'| < \epsilon.$$

3. *([18], Problem 4.3) If x_i are given exactly by floating-point numbers and $s_n = \sum_{i=1}^n x_i$, then $\mathsf{fl}(s_n) = \sum_{i=1}^n (1+d_i)x_i$ for some $|d_i| \leqslant \gamma_{n-1}$.*

We will now bound the relative error in matrix entries. If S is an approximation to the matrix T calculated in floating-point arithmetic with unit roundoff ϵ, we wish to bound $|S_{ij} - T_{ij}|/|T_{ij}|$. The entry $T_{ij} \in \mathbb{R}$ is given by $T_2(b_i, b_j) = \sum_k \sum_m \sigma_k(b_{i,m})\bar{\sigma}_k(b_{j,m})$, where $b_{i,m}$ denotes the m-th coordinate of vector b_i.

Lemma 7.3. *A floating-point approximation S of T calculated with unit roundoff ϵ satisfies*
$$\frac{|S_{ij} - T_{ij}|}{|T_{ij}|} < \frac{(1+\epsilon)^3}{(1-\epsilon(d-1))(1-\epsilon(n-1))} - 1.$$

Proof. We will denote error terms by c (for errors bounded by ϵ) and d (for errors bounded by some γ_t) as in Lemma 7.2, with subscripts matching the operation or number to which the error relates.

$$
\begin{aligned}
|S_{ij} - T_{ij}| &= |\mathsf{fl}(T_{ij}) - T_{ij}| \\
&= \left| \mathsf{fl}\left(\sum_k \sum_m \sigma_k(b_{i,m}) \bar{\sigma}_k(b_{j,m}) \right) - \sum_k \sum_m \sigma_k(b_{i,m}) \bar{\sigma}_k(b_{j,m}) \right| \\
&= \left| \sum_k \sum_m (1 + d_m)(1 + d_k) \mathsf{fl}\left(\sigma_k(b_{i,m}) \bar{\sigma}_k(b_{j,m}) \right) \right. \\
&\qquad\qquad \left. - \sum_k \sum_m \sigma_k(b_{i,m}) \bar{\sigma}_k(b_{j,m}) \right| \\
&= \left| \sum_k \sum_m (1 + d_m)(1 + d_k)(1 + c_{k,i,j,m}) \mathsf{fl}(\sigma_k(b_{i,m})) \mathsf{fl}(\bar{\sigma}_k(b_{j,m})) \right. \\
&\qquad\qquad \left. - \sum_k \sum_m \sigma_k(b_{i,m}) \bar{\sigma}_k(b_{j,m}) \right| \\
&= \left| \sum_k \sum_m (1 + d_m)(1 + d_k)(1 + c_{k,i,j,m})(1 + c_{k,i,m})(1 + c_{\bar{k},j,m}) \sigma_k(b_{i,m}) \bar{\sigma}_k(b_{j,m}) \right. \\
&\qquad\qquad \left. - \sum_k \sum_m \sigma_k(b_{i,m}) \bar{\sigma}_k(b_{j,m}) \right| \\
&= \left| \sum_k \sum_m \big((1 + d_m)(1 + d_k)(1 + c_{k,i,j,m})(1 + c_{k,i,m})(1 + c_{\bar{k},j,m}) - 1 \big) \times \right. \\
&\qquad\qquad \left. \sigma_k(b_{i,m}) \bar{\sigma}_k(b_{j,m}) \right| \\
&< \big((1 + \gamma_{n-1})(1 + \gamma_{d-1})(1 + \epsilon)^3 - 1 \big) \left| \sum_k \sum_m \sigma_k(b_{i,m}) \bar{\sigma}_k(b_{j,m}) \right| \\
&= \big((1 + \gamma_{n-1})(1 + \gamma_{d-1})(1 + \epsilon)^3 - 1 \big) |T_{ij}| \\
&= \left(\frac{(1 + \epsilon)^3}{(1 - \epsilon(d-1))(1 - \epsilon(n-1))} - 1 \right) |T_{ij}|
\end{aligned}
$$

□

The bound is small when ϵ is small. This result will allow us to choose a suitable unit roundoff ϵ for a required matrix entry precision $\frac{|S_{ij} - T_{ij}|}{|T_{ij}|} < \delta$.

7.2.2 Adjusted length bounds

We collect some useful results from the theory of matrices. If A is a matrix with real entries A_{ij} then the **Frobenius norm** of A is given by $\|A\| = \left(\sum_i \sum_j |A_{ij}|^2 \right)^{\frac{1}{2}}$. If A

is a symmetric $n \times n$ matrix we denote the eigenvalues of A by $\lambda_1(A) \leqslant \ldots \leqslant \lambda_n(A)$.

Lemma 7.4 (Fact 1.11 and Inequality (1.30) of [25]). *For symmetric matrices A and B,*

$$\max_j |\lambda_j(A) - \lambda_j(B)| \leqslant ||A - B||$$

where $||.||$ denotes the Frobenius norm on matrices.

Parlett describes this result in [25] by saying that eigenvalues are "perfectly conditioned". This is not the case for non-symmetric matrices.

Lemma 7.5. *Let A and B be matrices such that $|A_{ij} - B_{ij}| < \nu |A_{ij}|$ for some $0 < \nu < 1$. Then we have the bound*

$$|A_{ij}| < \frac{|B_{ij}|}{1 - \nu}.$$

If, furthermore, A and B are both symmetric, then

$$\lambda_j(B) - \frac{\nu}{1 - \nu} ||B|| < \lambda_j(A).$$

Proof. The first part is a simple application of the triangle inequality:

$$\begin{aligned} |A_{ij}| &\leqslant |A_{ij} - B_{ij}| + |B_{ij}| \\ &< \nu |A_{ij}| + |B_{ij}|. \end{aligned}$$

As $0 < \nu < 1$,

$$(1 - \nu)|A_{ij}| < |B_{ij}|$$

and the conclusion follows.

For the second part we use Lemma 7.4 to show that

$$\lambda_j(B) - ||A - B|| \leqslant \lambda_j(A) \leqslant \lambda_j(B) + ||A - B||.$$

We apply the matrix entry precision and the first part of the Lemma to the norm of $A - B$:

$$\begin{aligned} ||A - B|| &= \left(\sum_{i,j} |A_{ij} - B_{ij}|^2 \right)^{1/2} \\ &< \left(\sum_{i,j} (\nu |A_{ij}|)^2 \right)^{1/2} \end{aligned}$$

$$
\begin{aligned}
||A-B|| &< \left(\sum_{i,j} (\frac{\nu}{1-\nu}|B_{ij}|)^2\right)^{1/2} \\
&= \frac{\nu}{1-\nu}\left(\sum_{i,j}|B_{ij}|^2\right)^{1/2} \\
&= \frac{\nu}{1-\nu}||B||.
\end{aligned}
$$

Therefore,

$$\lambda_j(B) - \frac{\nu}{1-\nu}||B|| < \lambda_j(B) - ||A-B|| \leqslant \lambda_j(A)$$

□

Lemma 7.6. *Let A be a positive definite symmetric matrix, $B_L > 0$ a real number and x a real vector such that $x^tAx \leqslant B_L$. Then each entry x_j of x satisfies*

$$|x_j|^2 \leqslant \frac{B_L}{\lambda_1(A)}.$$

Proof. We may diagonalise A; there exist a unitary matrix U and a diagonal matrix D such that $A = U^tDU$. Note that because A is positive definite its eigenvalues are all strictly positive; therefore the diagonal entries of D are also strictly positive. Let y be equal to Ux. Because U is unitary, $|x| = |y|$.

Because $x^tAx \leqslant B_L$, we have $(Ux)^tD(Ux) \leqslant B_L$, so y satisfies $y^tDy \leqslant B_L$. This leads us to see that

$$x^tAx = y^tDy = \sum_i D_{ii}y_i^2 \leqslant B_L.$$

The diagonal entries of D are the eigenvalues $D_{ii} = \lambda_i(A)$ of A. We consider the smallest eigenvalue and see that $\lambda_1(A)\sum_i y_i^2 \leqslant B_L$ and that $\sum_i y_i^2 = |y|^2 = |x|^2$. We conclude that $|x|^2 \leqslant \frac{B_L}{\lambda_1(A)}$. This bound applies to each entry of x: $|x_j|^2 \leqslant \frac{B_L}{\lambda_1(A)}$. □

7.3 Approximating the Gram matrix

We can now calculate a floating-point approximation to T and find the resulting error in the T_2-norm.

Theorem 7.7. *Let T be a positive definite symmetric matrix and let B_L satisfy $B_L > 0$. Then for all $\eta > 1$ there exists a $\delta > 0$ such that if $|S_{ij} - T_{ij}| < \delta|T_{ij}|$ for* *all i and j then we have*

$$|x^tSx - x^tTx| < (\eta - 1)B_L,$$

for every x such that $x^tTx \leqslant B_L$.

Proof. For all x, we can estimate the error in terms of T and x:

$$\begin{aligned}
|x^tTx - x^tSx| &= \left|\sum_{i,j} T_{ij}x_ix_j - \sum_{i,j} S_{ij}x_ix_j\right| \\
&= \left|\sum_{i,j}(T_{ij} - S_{ij})x_ix_j\right| \\
&\leqslant \sum_{i,j} |T_{ij} - S_{ij}|\,|x_i||x_j| \\
&< \sum_{i,j} \delta|T_{ij}||x_i||x_j|.
\end{aligned}$$

Choose a positive-definite symmetric matrix S° with entry-wise precision $|S^\circ_{ij} - T_{ij}| < \nu|T_{ij}|$ for some $0 < \nu < 1$. We may always choose S° so that $\lambda_{\min}(S^\circ) - \frac{\nu}{1-\nu}||S^\circ|| > 0$ by choosing ν to be small. We label $l(S^\circ) = \lambda_{\min}(S^\circ) - \frac{\nu}{1-\nu}||S^\circ||$. This S° only needs to satisfy these conditions; it is not our final approximation to T. We use the first part of Lemma 7.5 to bound the error in terms of S°:

$$|x^tTx - x^tSx| < \sum_{i,j} \delta\frac{|S^\circ_{ij}|}{1-\nu}|x_i||x_j| = \frac{\delta}{1-\nu}\sum_{i,j}|S^\circ_{ij}||x_i||x_j|.$$

We may bound the size of $|x_i|$ and $|x_j|$ using Lemma 7.6, concluding that

$$|x^tTx - x^tSx| < \frac{\delta}{1-\nu}\sum_{i,j}|S^\circ_{ij}|\frac{B_L}{\lambda_1(T)} = \frac{\delta}{1-\nu}\frac{B_L}{\lambda_1(T)}\sum_{i,j}|S^\circ_{ij}|,$$

for all x such that $x^tTx \leqslant B_L$. We wish to find a δ that satisfies $\frac{\delta}{(1-\nu)\lambda_1(T)}\sum_{i,j}|S^\circ_{ij}| \leqslant \eta - 1$. Everything on the left-hand-side of this inequality is already known apart from $\lambda_1(T)$. Here, we employ Lemma 7.4, applied to T and S°. Let $\lambda_{\min}$ be a lower bound for the eigenvalues of S°: $\lambda_1(S^\circ) > \lambda_{\min}(S^\circ) > 0$. By Lemma 7.5 we have

$$\lambda_{\min}(S^\circ) - \frac{\nu}{1-\nu}||S^\circ|| < \lambda_1(T).$$

Choose a $\delta > 0$ such that

$$\delta \leqslant (\eta - 1)(1 - \nu)\frac{l(S^\circ)}{\sum_{i,j} |S^\circ_{ij}|}. \tag{7.1}$$

Then the inequality

$$|x^tTx - x^tSx| < \frac{\delta B_L}{(1-\nu)l(S^\circ)} \sum_{i,j} |S^\circ_{ij}| \leqslant (\eta - 1)B_L,$$

holds for all x such that $x^tTx \leqslant B_L$. □

We may find an approximation S to the Gram matrix T that satisfies the matrix entry precision condition of Theorem 7.7 using the following algorithm. We use fl_p to denote a floating-point approximation with precision p.

```
Algorithm 2: Approximation to $T_2$ matrix with bounded length error
  Input:
      - $\mathbb{Z}$-linearly independent vectors $b_1, \ldots, b_n$ with entries in $K$ ,
      - $\eta > 1$, an acceptable proportional increase in the length bound,
      - $p$, default precision (unit roundoff $= 2^{-p}$).
  Output: - a matrix $S$ that approximates $T_2$, so that $x^tSx < \eta x^tT_2x$ for all $x$.

  Procedure:
  For each embedding $\sigma_k : K \hookrightarrow \mathbb{C}$ and entry $b_{i,m}$ of a vector $b_i$:
      calculate exactly and store $\sigma_k(b_{i,m})$ and $\bar{\sigma}_k(b_{i,m})$.
  Set $S^\circ \leftarrow \left(\mathsf{fl}_p\left(\sum_m \sum_k \sigma_k(b_{i,m})\bar{\sigma}_k(b_{j,m})\right)\right)_{ij}$, calculated with precision $p$ from
  exact values.
  While $S^\circ$ is not positive definite or $l(S^\circ) \leqslant 0$:
      increase $p$ and go to previous step.
  Find $\delta > 0$ satisfying inequality 7.1.
  Find $\epsilon > 0$ satisfying inequality 7.2.
  If $-\log_2(\epsilon) \leqslant p$:
      set $S \leftarrow S^\circ$.
  Else:
      set $p \leftarrow \lceil -\log_2(\epsilon) \rceil$,
      set $S \leftarrow (\mathsf{fl}_p(\sum_m \sum_k \sigma_k(b_{i,m})\bar{\sigma}_k(b_{j,m})))_{i,j}$ calculated with precision $p$
      from exact values.
  Return $S$
```

We now restate and prove the main result of this chapter:

Theorem 7.1. *Let $\eta > 1$. Then there exists an explicitly calculable $\epsilon > 0$ such that if ϵ is the unit roundoff on floating-point operations, Algorithm 2 constructs an approximation S to the matrix $T := (T_2(b_i, b_j))_{ij}$ such that if x satisfies $x^tTx \leqslant B_L$, then $x^tSx < \eta B_L$.*

Proof. Use the method outlined in the proof of Theorem 7.7 to find a $\delta > 0$ that satisfies the conclusion of that Theorem. Choose ϵ satisfying $\frac{1}{nd} > \epsilon > 0$ such that

$$0 < \frac{(1+\epsilon)^3}{(1-\epsilon(d-1))(1-\epsilon(n-1))} - 1 \leqslant \delta. \tag{7.2}$$

This is possible because for fixed n and d the expression tends to 0 as $\epsilon \to 0$ and we can use a computer algebra system to solve this inequality. By Lemma 7.6 and Theorem 7.7, the floating-point approximation S of T will have the property that

$$|x^tSx - x^tTx| < (\eta - 1)B_L,$$

for all x such that $x^tTx \leqslant B_L$. We conclude that if $x^tTx \leqslant B_L$ then

$$x^tSx \leqslant x^tTx + |x^tSx - x^tTx| < \eta B_L.$$

□

Theorem 7.1 shows that Algorithm 2 provides a method of constructing a floating-point approximation to T that approximates the T_2-norm to within a prescribed relative error. We will now consider some of the practical issues involved in using Algorithm 2.

7.3.1 Adjusting precision

In Algorithm 2 we describe finding ϵ as in Theorem 7.1 corresponding to our chosen η. We use a unit roundoff less than or equal to ϵ to construct a matrix S which is an approximation to T with known accuracy. We construct the appropriate unit roundoff by defining a precision p. As the precision is integral, we may find that we need to overestimate the precision and therefore end up with a smaller ϵ than expected. Considering Inequality 7.1, we can recalculate our η in view of this explicit ϵ and so potentially reduce the length bound compared to what was expected. It make sense to set p to be the usual double precision of 53 initially, increasing it only if necessary.

In fact, we may go further and consider this process in the other direction. If we fix a precision p we can calculate a suitable η as follows. We still require a S° as constructed in the proof of Theorem 7.7. We use $\epsilon = 2^{-p}$ to find a δ satisfying Inequality 7.2 and then rearrange Inequality 7.1 to define a suitable proportional error bound η. If the reason for fixing the precision is a limitation of the machine, then we may struggle to construct a suitable S° as this may need an arbitrarily high precision.

Although in theory we do not need our final approximation S to be positive definite (the S output by Algorithm 2 satisfies Theorem 7.1 even if it is not), this will be necessary for finding points. If S turns out not to be positive definite, we could attempt to deal with this by increasing the working precision. However, if $\lambda_1(T)$ is very small this could be difficult and require a restrictively high precision. A possible solution would be to construct S using exact algebraic numbers, converting to a floating-point version once the entries have been calculated. A drawback of this would be that such exact arithmetic is likely to be slower in general than floating-point arithmetic. An alternative idea would be to use a ridge adjustment: adding a small quantity to all diagonal entries of S to force the matrix to be positive definite. This would take some care and likely involve an adjustment to η, and has not yet been implemented. We do require S to be positive definite to complete the lattice enumeration step.

7.4 Finding points

After fixing p and η (and a positive-definite S) we know that all points x in our lattice (a sub-lattice of $\mathcal{O}_K^n$) such that $||x|| \leqslant B_L$ satisfy $x^t S x < \eta B_L$. We construct the lattice in Magma [4] from the Gram matrix S and then use the ShortVectors function to find all points with norm up to ηB_L. The Magma function ShortVectors allows the user to specify a minimum as well as a maximum norm for lattice points, so this could be used to extend point searches whilst avoiding unnecessary repetition.

We could also use Pari's [31] qfminim function to enumerate lattice points. To do this in Sage [30] requires a small change from Sage 5.10 (the current version at the time of writing), for which a patch has been created.[1] This method will be implemented soon. Further discussion of the use of lattice enumeration to find rational points of V can be found in Chapter 9.

[1] This patch can be found at `http://trac.sagemath.org/ticket/14867`.

Chapter 8

Points from lattices via lattice reduction

Our aim in this chapter is to generalise a method given by Cremona and Roberts in [11] for finding points on curves from lattices via lattice reduction. We will outline the circumstances under which such a method might be applicable and discuss existing lattice reduction methods. Unfortunately this method is not always applicable and we explore the issues that cause it to fail in certain cases.

Theorem 8.1. *Let K be an imaginary quadratic field (with degree $d = 2$) and L an $\mathcal{O}_K$-sub-lattice of $\mathcal{O}_K^n$ of rank n, with pseudo-basis $(b_i, \mathfrak{b}_i)$ satisfying*

$$Y_1 \leqslant \mathcal{N}(\mathfrak{b}_i) \leqslant Y_2 \tag{8.1}$$

and

$$||b_n^*||^{Z_1} \geqslant Z_2||b_i||, \tag{8.2}$$

for all i and some fixed $Y_1, Y_2, Z_1, Z_2 > 0$, with b_i^* denoting the Gram-Schmidt orthogonalisation of b_i, as in Definition 26 on page 56. If

$$\mathcal{N}([\mathcal{O}_K^n : L]) > Z_2^{-dn} d^{-\frac{(Z_1+1)dn}{2}} Y_2^n B_L^{\frac{Z_1 dn}{2}} Y_1^{-Z_1 n} 2^{\frac{Z_1 nd}{2}}, \tag{8.3}$$

then every $z \in L$ such that $||z||^2 < B_L$ lies in the submodule L_0 of L given by $(b_i, \mathfrak{b}_i)_{i=1}^{n-1}$.

Despite the fact that imaginary quadratic number fields are the only ones considered in this theorem, we retain the variable d as it allows us to see how the theorem might be generalised in future. We will eventually use this result to construct points on curves in a manner analogous to that of Section 3.3 of [11] where it applies. We first collect relevant information relating to norms on K.

Lemma 8.2. *Let K be a number field of degree d. Let $B \in K^{n\times n}$ be of full rank with rows $b_1, \ldots, b_n$. Let $\mathcal{N}(x)$ denote the field norm of x. Then we have*

$$d^{n/2}\mathcal{N}(\det(B))^{1/d} \leqslant \prod_{i=1}^{n} \|b_i\|.$$

Proof. Let the σ_k be the d embeddings of K into $\mathbb{C}$. The definition of norm implies that

$$\mathcal{N}(\det(B))^2 = \prod_{k=1}^{d} \sigma_k(\det(B))\bar{\sigma}_k(\det(B)).$$

We use the notation b_{ij} for the jth coordinate of b_i. The definition of T_2-norm says that $\|b_i\|^2 = \sum_{k=1}^{d}\sum_{j=1}^{n} \sigma_k(b_{ij})\bar{\sigma}_k(b_{ij})$. By Hadamard's inequality for complex matrices (see page 51 of [5]), we may state that, for each embedding σ_k,

$$\sigma_k(\det(B))\bar{\sigma}_k(\det(B)) \leqslant \prod_{i=1}^{n}\sum_{j=1}^{n} \sigma_k(b_{ij})\bar{\sigma}_k(b_{ij}).$$

Multiplying across all embeddings σ_k to bound the norm of $\det(B)$, we have

$$\mathcal{N}(\det(B))^2 = \prod_{k=1}^{d}\prod_{i=1}^{n}\sum_{j=1}^{n} \sigma_k(b_{ij})\bar{\sigma}_k(b_{ij}) = \prod_{i=1}^{n}\prod_{k=1}^{d}\sum_{j=1}^{n} \sigma_k(b_{ij})\bar{\sigma}_k(b_{ij}).$$

We now apply the arithmetic mean-geometric mean inequality to show that

$$\begin{aligned}
\left(\prod_{k=1}^{d}\sum_{j=1}^{n} \sigma_k(b_{ij})\bar{\sigma}_k(b_{ij})\right)^{1/d} &\leqslant \frac{1}{d}\sum_{k=1}^{d}\sum_{j=1}^{n} \sigma_k(b_{ij})\bar{\sigma}_k(b_{ij}),\\
d\left(\prod_{k=1}^{d}\sum_{j=1}^{n} \sigma_k(b_{ij})\bar{\sigma}_k(b_{ij})\right)^{1/d} &\leqslant \sum_{k=1}^{d}\sum_{j=1}^{n} \sigma_k(b_{ij})\bar{\sigma}_k(b_{ij}) = \|b_i\|^2.
\end{aligned}$$

Taking the product over all rows, we have

$$\begin{aligned}\prod_{i=1}^{n} d\left(\prod_{k=1}^{d}\sum_{j=1}^{n}\sigma_k(b_{ij})\bar{\sigma}_k(b_{ij})\right)^{1/d} &= d^n\left(\prod_{i=1}^{n}\prod_{k=1}^{d}\sum_{j=1}^{n}\sigma_k(b_{ij})\bar{\sigma}_k(b_{ij})\right)^{1/d}\\ &\leqslant \prod_{i=1}^{n}\|b_i\|^2.\end{aligned}$$

Therefore, we have

$$d^n\mathcal{N}(\det(B))^{2/d} \leqslant \prod_{i=1}^{n}\|b_i\|^2,$$

and the result follows. □

Lemma 8.3. *Let a be a non-zero element of a fractional ideal $\mathfrak{a}$. Then, $\|a\|^2 \geqslant d\mathcal{N}(\mathfrak{a})^{\frac{2}{d}}$.*

Proof. Note that $\mathcal{N}(x) = \sqrt{\prod_k |\sigma_k(x)\bar{\sigma}_k(x)|}$. If a is non-zero in $\mathfrak{a}$ then $\mathcal{N}(a) \geqslant \mathcal{N}(\mathfrak{a})$. By the arithmetic mean - geometric mean inequality,

$$\mathcal{N}(a)^{\frac{2}{d}} = \left(\prod_k \sigma_k(a)\bar{\sigma}_k(a)\right)^{\frac{1}{d}} \leqslant \frac{1}{d}\sum_k \sigma_k(a)\bar{\sigma}_k(a) = \frac{1}{d}\|a\|^2.$$

The result follows by combining the two inequalities. □

Lemma 8.4. *Let K be an imaginary quadratic field. Then for all $x \in K_{\mathbb{R}}^n$ and $a \in K_{\mathbb{R}}$, we have*

$$||ax||^2 = \frac{1}{2}||a||^2||x||^2.$$

Proof. Let σ_1 and σ_2 be the two embeddings of $K \hookrightarrow \mathbb{C}$, extended to $K_{\mathbb{R}}$. The two embeddings are complex conjugates, so we have

$$\begin{aligned}||a||^2 &= \sum_j \sigma_j(a)\bar{\sigma}_j(a)\\ &= \sigma_1(a)\bar{\sigma}_1(a) + \sigma_2(a)\bar{\sigma}_2(a)\\ &= 2\sigma_1(a)\bar{\sigma_1}(a) = 2\sigma_2(a)\bar{\sigma_2}(a) = 2\mathcal{N}(a).\end{aligned}$$

Therefore, we have

$$\begin{aligned}
||ax||^2 &= \sum_i \sum_j \sigma_j(ax_i)\bar{\sigma}_j(ax_i) \\
&= \sum_i \sum_j \sigma_j(a)\bar{\sigma}_j(a)\sigma_j(x_i)\bar{\sigma}_j(x_i) \\
&= \sum_i \frac{1}{2}||a||^2 \sum_j \sigma_j(x_i)\bar{\sigma}_j(x_i) \\
&= \frac{1}{2}||a||^2 \sum_i \sum_j \sigma_j(x_i)\bar{\sigma}_j(x_i) \\
&= \frac{1}{2}||a||^2||x||^2.
\end{aligned}$$

□

This works because both of the embeddings of any element are of the same size.

We have now collected the results needed to prove Theorem 8.1.

Proof of Theorem 8.1. The combination of Lemma 8.3 and our bound on the norms of ideals implies that $||a||^2 \geqslant dY_1^{\frac{2}{d}}$ for all non-zero $a \in \mathfrak{b}_i$. By Lemma 6.4, it follows that $\mathcal{N}([\mathcal{O}_K^n : L]) \leqslant \mathcal{N}(\langle \det(b_1, \ldots, b_n)\rangle)Y_2^n$.

By Inequality 8.2, we see that $||b_n^*||^{Z_1 n} \geqslant Z_2^n \prod_i ||b_i||$ and therefore $||b_n^*||^2 \geqslant Z_2^{\frac{2}{Z_1}} \left(\prod_i ||b_i||\right)^{\frac{2}{Z_1 n}}$. We then set up a chain of inequalities as follows:

$$\begin{aligned}
\frac{1}{2}dY_1^{\frac{2}{d}}||b_n^*||^2 &\geqslant \frac{1}{2}dY_1^{\frac{2}{d}} Z_2^{\frac{2}{Z_1}} \left(\prod_i ||b_i||\right)^{\frac{2}{Z_1 n}} \\
&\geqslant \frac{1}{2}dY_1^{\frac{2}{d}} Z_2^{\frac{2}{Z_1}} \left(d^{\frac{n}{2}} \left(\mathcal{N}(\det(b_1, \ldots, b_n))\right)^{\frac{1}{d}}\right)^{\frac{2}{Z_1 n}} && \text{(by Lemma 8.2)} \\
&= \frac{1}{2}dY_1^{\frac{2}{d}} Z_2^{\frac{2}{Z_1}} d^{\frac{1}{Z_1}} \left(\mathcal{N}(\det(b_1, \ldots, b_n))\right)^{\frac{2}{Z_1 nd}} \\
&\geqslant \frac{1}{2}dY_1^{\frac{2}{d}} Z_2^{\frac{2}{Z_1}} d^{\frac{1}{Z_1}} \left(\mathcal{N}([\mathcal{O}_K^n : L])Y_2^{-n}\right)^{\frac{2}{Z_1 nd}} \\
&= \frac{1}{2}dY_1^{\frac{2}{d}} Z_2^{\frac{2}{Z_1}} d^{\frac{1}{Z_1}} Y_2^{-\frac{2}{Z_1 d}} \mathcal{N}([\mathcal{O}_K^n : L])^{\frac{2}{Z_1 nd}} \\
&> \frac{1}{2}dY_1^{\frac{2}{d}} Z_2^{\frac{2}{Z_1}} d^{\frac{1}{Z_1}} Y_2^{-\frac{2}{Z_1 d}} \left(Z_2^{-dn} d^{-\frac{(Z_1+1)dn}{2}} Y_2^n B_L^{\frac{Z_1 dn}{2}} Y_1^{-Z_1 n} 2^{\frac{Z_1 nd}{2}}\right)^{\frac{2}{Z_1 nd}} \\
&= \frac{1}{2}dY_1^{\frac{2}{d}} Z_2^{\frac{2}{Z_1}} d^{\frac{1}{Z_1}} Y_2^{-\frac{2}{Z_1 d}} Z_2^{-\frac{2}{Z_1}} d^{-\frac{Z_1+1}{Z_1}} Y_2^{\frac{2}{Z_1 d}} B_L Y_1^{-\frac{2}{d}} 2 \\
&= B_L \\
&\geqslant ||z||^2.
\end{aligned}$$

We have $||z||^2 = ||\sum_i a_i b_i||^2 = ||\sum_i a_i^* b_i^*||^2 = \sum_i ||a_i^* b_i^*||^2 \geqslant ||a_n^* b_n^*||^2 = ||a_n b_n^*||^2 = \frac{1}{2}||a_n||^2||b_n^*||^2$. We know that $a_n = a_n^*$ because the change of basis from b_i to b_i^* is triangular.

Therefore $\frac{1}{2} d Y_1^{\frac{2}{d}} ||b_n^*||^2 > \frac{1}{2}||a_n||^2||b_n^*||^2$, which implies that $a_n = 0$ by Lemma 8.3. Therefore whenever $\|z\|^2 \leqslant B_L$, z is in L_0, the submodule of L given by $(b_i, \mathfrak{b}_i)_{i=1}^{n-1}$. □

8.1 Effective methods over number fields

There are two main differences that cause difficulties in extending Proposition 3.1 of Cremona and Roberts [11] to number fields. The first is the availability of a suitable lattice basis reduction method. Several algorithms have been proposed that attempt to generalise LLL reduction [21] to $\mathcal{O}_K$-lattices but not all of them preserve the aspects of LLL reduction that we require for Theorem 8.1.

The second difference involves the T_2-norm. When working over $\mathbb{Q}$ we use the Euclidean norm: for pairs $\alpha \in \mathbb{R}$, $x \in \mathbb{R}^n$ it is clear that $|\alpha x| = |\alpha||x|$. Over imaginary quadratic fields we can use Lemma 8.4 to relate $\|\alpha x\|$, $\|\alpha\|$ and $\|x\|$. It is unclear whether it is possible to prove such a result in general because the T_2-norm on $K_{\mathbb{R}}^n$ is sub-multiplicative: it is not a true norm.

8.1.1 Lattice reduction methods

We outlined our requirements of lattice reduction in the statement of Theorem 8.1: we need a form of lattice reduction satisfying Inequalities 8.1 and 8.2. There have been several attempts to generalise LLL reduction to the case of $\mathcal{O}_K$-lattices but not all of them are suitable for our needs. We are not aware of any methods that satisfy Inequalities 8.1 and 8.2 for every sub-lattice of $\mathcal{O}_K^{N+1}$ defined over any number field.

The important property of LLL reduction used in Proposition 3.1 of [11] is the "Lovász condition" which bounds the lengths of each b_i^* vector in terms of the next: $|b_i^*|^2 \geqslant (\frac{3}{4} - \mu_{i,i-1}^2)|b_{i-1}^*|^2$, with the $\mu_{i,j}$ bounded. (See Definition 2.6.1 of [5].) This implies (Part 2 of Theorem 2.6.2, [5]) that $|b_j| \leqslant 2^{\frac{(i-1)}{2}}|b_i^*|$ for $1 \leqslant j \leqslant i \leqslant n$, repeated application of which allows us to deduce a lower bound on $|b_n^*|$ in the form of Inequality 8.2. As noted by Cohen in [5], the $\frac{3}{4}$ may be replaced by any constant $c_L \in (\frac{1}{4}, 1)$.

A Lovász-type condition would therefore be sufficient to satisfy Inequality 8.2 in Theorem 8.1. The lattice reduction algorithm outlined by Fieker and Pohst in [14] contains what they call an "LLL condition" of this form. After an adjustment of c_L (though c_L must remain strictly less than 1), this could give an effective Lovász condition if and only if a bound for $\mu_{i,j}$ can be found so that $c_L - \mu_{i,i-1}^2 > 0$ for each i. Fieker and Pohst state that this is not possible in general when $c_L = \frac{3}{4}$. The attempt to minimise $\mu_{i,j}$ is contained in the $\mathsf{Red}(k,l)$ step of Algorithm 2 of [14].

Consider the case in which the initial pseudo-basis has all ideals $\mathfrak{a}_i = \mathcal{O}_K$. This could well fit our situation as the lattices L_i are always free. Then minimising $\mu_{i,j}$ means to adjust $\mu_{i,j} \in K_{\mathbb{R}}$ by an element of $\mathcal{O}_K$. We may therefore bound $|\mu_{i,j}|$ above by the maximum value of $\|x\|$ for x in a fundamental domain for the action of the lattice $\mathcal{O}_K$ on $K_{\mathbb{R}}$. For certain Euclidean fields such a maximum is less than 1, which is necessary for the Lovász condition. The lattice reduction algorithm of [14] does not change the ideals appearing in a pseudo-basis; these are the same in the input and output.

Fieker and Pohst also provide a form of $\mathcal{O}_K$-lattice enumeration in [14]. The main purpose of their lattice reduction algorithm is to improve performance of this enumeration. Because we already have a method of $\mathbb{Z}$-lattice enumeration detailed in Chapter 7, we have not explored the use of this algorithm. Vectors in the $\mathcal{O}_K$-lattice and $\mathbb{Z}$-lattice are in one-to-one correspondence and arithmetic in number fields is in general slower than over $\mathbb{Z}$. The only source of benefit of using this $\mathcal{O}_K$-lattice enumeration could be a reduction in the number of vectors found whose T_2-norm is greater than the bound specified. We do not yet know whether Fieker and Pohst's $\mathcal{O}_K$-lattice enumeration could achieve this kind of improvement.

A more recent form of lattice basis reduction by Fieker and Stehlé described in [15] provides absolute bounds for the norms of ideals and bounds for the lengths of basis vectors based on the successive lattice minima. It uses standard LLL reduction on a full rank submodule of the $\mathbb{Z}$-lattice corresponding to a $\mathcal{O}_K$-lattice but in general does not follow closely the method of LLL. In particular, it has no Lovász-type condition for us to use.

Napias has generalised the LLL algorithm to Euclidean rings in [23]. This algorithm seems to be very similar to that of [14] but far less general. Euclidean rings are always principal ideal domains, which provides an important simplification. This is the only form of lattice basis reduction which we have found that we may be able to use. We will show that this reduction will allow us to leave out the last vector of a reduced basis, when applied to $\mathcal{O}_K$-lattices when K is imaginary quadratic and $\mathcal{O}_K$ is Euclidean. There are exactly five number fields satisfying these conditions: $\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{-7})$ and $\mathbb{Q}(\sqrt{-11})$.

Proposition 8.5. *Let K be an imaginary quadratic Euclidean number field. Then the output of the lattice reduction for $\mathcal{O}_K$-lattices described by Napias in [23] satisfies the conditions of Theorem 8.1.*

Proof. For each of these five fields, the ring of integers is a Euclidean domain. Euclidean domains are always principal ideal domains, so the five fields all have class number 1 and every $\mathcal{O}_K$-lattice has a basis, not just a pseudo-basis. In Section 2 of [23], Napias describes properties of what she calls an "A-LLL-reduced" lattice basis, where A is an Euclidean ring. In our cases we take A to be $\mathcal{O}_K$. Let C_1 be the **Euclidean minimum** of K, defined by

$$C_1 = \sup \{ \inf \{ \mathcal{N}(y - x) \ | \ x \in \mathcal{O}_K \} \mid y \in K_{\mathbb{R}} \} .$$

For each of the fields $K = \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{-7})$ and $\mathbb{Q}(\sqrt{-11})$, the Euclidean minimum of $\mathcal{O}_K$ is strictly less than 1 (see Section 4.1 of [19]). Let C_2 be any real number satisfying $0 < C_1 < C_2 < 1$. Then, part ii) of "Properties" in Section 2 of [23] states that

$$||b_i||^2 \leqslant (C_2 - C_1)^{1-j} ||b_j^*||^2 \text{ for } 1 \leqslant i \leqslant j \leqslant n,$$

for any $b_1, \ldots, b_n$ that form an A-LLL-reduced basis (with parameters C_1 and C_2) for an $\mathcal{O}_K$-lattice. Therefore, $(b_i, \mathcal{O}_K)_{i=1}^n$ forms a pseudo-basis for the $\mathcal{O}_K$-lattice and this satisfies the conditions of Theorem 8.1. □

Corollary 8.6. *Let K be an imaginary quadratic Euclidean number field and let $L \subset \mathcal{O}_K^{N+1}$ be an $\mathcal{O}_K$-lattice such that*

$$\mathcal{N}([\mathcal{O}_K^{N+1} : L]) > B_L^{N+1} (C_2 - C_1)^{-N(N+1)} 2^{-(N+1)}.$$

If $(b_i)_{i=0}^N$ is an "A-LLL-reduced" basis for L in the sense of [23] then every $z \in L$ such that $||z||^2 < B_L$ lies in the submodule L_0 of L given by $(b_i)_{i=0}^{N-1}$.

Proof. By Proposition 8.5, we know that L satisfies the conditions of Theorem 8.1. Therefore, it suffices to show that Inequality 8.3 holds for some $Y_1, Y_2, Z_1, Z_2 > 0$. Let $Y_1 = Y_2 = Z_1 = 1$, $Z_2 = (C_2 - C_1)^{\frac{N}{2}}$ and $d = 2$. Then we see that

$$Z_2^{-d(N+1)} d^{-\frac{(Z_1+1)d(N+1)}{2}} Y_2^{N+1} B_L^{\frac{Z_1(N+1)d}{2}} Y_1^{-Z_1(B+1)} 2^{\frac{Z_1(N+1)d}{2}} = \\ B_L^{N+1} (C_2 - C_1)^{-N(N+1)} 2^{-(N+1)},$$

and Theorem 8.1 provides the result. □

We can therefore conclude that if K is one of the five imaginary quadratic Euclidean number fields, there already exists a form of lattice reduction that allows us to exclude the last vector when searching for points up to a given bound.

The algorithm of Fieker and Pohst described in [14] is similar to that of [23], and we expect that we could apply it to any lattice for which we can find suitable bounds on $\mu_{i,j}$ to construct a Lovász condition. The conditions on number fields or lattices required for this have not yet been fully investigated beyond the idea that Euclidean fields are likely to be suitable: but this is simply the algorithm of [23].

The next section will explain why Theorem 8.1 is limited to imaginary quadratic fields. If this restriction could be lifted, then use of the algorithm of [23] could be extended to all Euclidean fields.

8.1.2 Norms, scalar multiplication and imaginary quadratic fields

Theorem 8.1 was stated only for imaginary quadratic number fields. In this section we will explain why this is the case and discuss the difficulties involved in attempting to extend this result to other fields.

The only part of the proof of Theorem 8.1 that requires K to be an imaginary quadratic number field is the use of Lemma 8.4 to bound $||z||^2$ below by $\frac{1}{2}||a_n||^2||b_n^*||^2$. The proof of Lemma 8.4 relies on the fact that K is an imaginary quadratic field, because imaginary quadratic fields are the only number fields apart from $\mathbb{Q}$ that have a single infinite place. (For LLL reduction on lattices defined over $\mathbb{Q}$, Proposition 3.1 of [11] forms a version of Theorem 8.1.) The proof of Lemma 8.4 relies on the fact that when K is imaginary quadratic, for any $a \in K$ the sizes of both embeddings of a are the same: $|\sigma_1(a)| = |\sigma_2(a)|$. This gives a relationship between the lengths of both of the embeddings of a given field element a, which in turn allows them to be expressed in terms of the norm $||a||$.

The following Lemma shows that such a relationship cannot be constructed for arbitrary $a \in K$ when K is a number field that is not imaginary quadratic. This means that the idea used in the proof of Lemma 8.4 cannot be extended to other number fields.

Lemma 8.7. *Let K be a number field that is not $\mathbb{Q}$ or an imaginary quadratic number field. Then for all $\epsilon > 0$ there exists an embedding $\sigma : K \hookrightarrow \mathbb{C}$ and a non-zero element $x \in \mathcal{O}_K$ such that $|\sigma(x)| < \epsilon$.*

Proof. Choose any $\epsilon > 0$. Let K be a number field and fix $\alpha_1, \ldots, \alpha_d$ an integral basis for K. The set $\{\alpha_i\}_{i=1}^{d}$ is $\mathbb{Q}$-linearly independent.

Let $\sigma : K \hookrightarrow \mathbb{C}$ be any embedding of K. Then σ is an injective $\mathbb{Q}$-linear map, so in particular the set $\{\sigma(\alpha_i)\}_{i=1}^{d}$ must be $\mathbb{Q}$-linearly independent. The complex numbers form a real vector space of dimension 2. So if $d > 2$ or if $d = 2$ and K is real quadratic (so that $\sigma : K \hookrightarrow \mathbb{R}$) then the set of $\{\sigma(\alpha_i)\}_{i=1}^d$ are $\mathbb{R}$-linearly dependent, since d exceeds the dimension of the codomain of σ as a real vector space.

Choose $\delta > \frac{1}{\epsilon}\sum_{i=1}^d |\sigma(\alpha_i)|$. By the $\mathbb{R}$-linear dependence of the $\sigma(x_i)$ there exist $a_1, \ldots, a_d \in \mathbb{R}$, not all zero, satisfying

$$a_1\sigma(\alpha_1) + \cdots + a_d\sigma(\alpha_d) = 0.$$

Using a multi-dimensional version of Dirichlet's Approximation Theorem (see Theorem 201 of [16]), there exist $q, p_1, \ldots, p_d \in \mathbb{Z}$ such that

$$|qa_i - p_i| < \frac{1}{\delta},$$

for each $i = 1, \ldots, d$, with not all of the p_i equal to 0. Therefore, we have

$$\begin{aligned} |\sigma(p_1\alpha_1 + \cdots + p_d\alpha_d)| &= |q(a_1\sigma(\alpha_1) + \cdots + a_d\sigma(\alpha_d)) - \sigma(p_1\alpha_1 + \cdots + p_d\alpha_d)| \\ &= |(qa_1 - p_a)\sigma(\alpha_1) + \cdots + (qa_d - p_d)\sigma(\alpha_d)| \\ &< \frac{1}{\delta}\sum_{i=1}^d |\sigma(\alpha_i)| \\ &< \epsilon. \end{aligned}$$

Taking $x = p_1\alpha_1 + \cdots + p_d\alpha_d$, the claim follows. □

We have shown that, outside of the imaginary quadratic and rational cases, we cannot construct a lower bound for the size of an embedding of an element of $\mathcal{O}_K$. For any ideal $\mathfrak{a}$ of K one cannot construct a lower bound for the size of an embedding of an element of $\mathfrak{a}$; we follow exactly the same argument as Lemma 8.7 applied to an integral basis for the ideal. This means that we cannot use a relationship between embeddings of K to construct a version of Lemma 8.4 to use in the proof of Theorem 8.1.

Chapter 9

Algorithms and examples

In this chapter we will explain in detail how to use the methods described so far in this thesis to find points on varieties over number fields. We will explain the circumstances under which each of these methods is applicable. We also provide some examples of points found using an implementation of Algorithm 4.

9.1 Processing lattice points

In each method we construct $\mathcal{O}_K$-lattices containing vectors that potentially represent rational points on a variety V. In Chapter 7 we described the conversion of such an $\mathcal{O}_K$-lattice to a $\mathbb{Z}$-lattice and how to use existing methods such as those in Magma or Pari to enumerate points in the $\mathbb{Z}$-lattice. We construct lattices so that each rational point in $V(K)$ has a representative in some $\mathbb{Z}$-lattice. However, not all lattice vectors correspond to rational points so we will need to check lattice points to see whether they correspond to rational points of $V(K)$ by evaluating the defining polynomials of V at lattice points. This could be time-consuming, so we wish to do some pre-processing to reduce the number of points which require this treatment. In particular, a point of $\mathbb{P}^N(K)$ will have multiple representatives in the lattice: we wish (as far as possible) to avoid considering the same projective point multiple times. Let L be an $\mathcal{O}_K$-lattice of rank $N+1$ and let M be the corresponding $\mathbb{Z}$-lattice $M \cong \mathbb{Z}^{d(N+1)}$.

9.1.1 Processing in $\mathbb{Z}^{d(N+1)}$

We consider some conditions that could be considered as "projectifying" the affine lattice output, reducing the search for points from $\mathbb{Z}^{d(N+1)}$ to $\mathbb{P}^{d(N+1)-1}(\mathbb{Z})$.

A lattice point $x \in M$ is given by an element of $\mathbb{Z}^{d(N+1)}$. We need only check half of the lattice points since x and $-x$ define the same point in projective space.

If x is not primitive, there exists some $x' \in \mathbb{Z}^{d(N+1)}$ and $a \in \mathbb{Z}$ such that $ax' = x$ and x' and x define the same projective point. The T_2-norm of such an x' will be shorter than the corresponding x so we restrict our search to primitive $x \in \mathbb{Z}^{d(N+1)}$.

A benefit of these methods is that they can be applied to points found in $\mathbb{Z}^{d(N+1)}$ without converting to the corresponding point in $\mathcal{O}_K^{N+1}$.

9.1.2 Processing in $\mathcal{O}_K^{N+1}$

We process the output of our search for lattice points by taking a point $x \in \mathbb{Z}^{d(N+1)}$ and converting it via the $\mathbb{Z}$-basis of M to a point in $L \subseteq \mathcal{O}_K^{N+1}$. Distinct primitive lattice points of M may still determine the same point in $\mathbb{P}^N(K)$. This is because although the lattice basis $(\beta_{i,j} b_i)_{ij}$ is $\mathbb{Z}$-linearly independent, it is not K-linearly independent: in passing to the $\mathbb{Z}$-lattice we have temporarily discarded some of the $\mathcal{O}_K$-lattice structure.

We recall from Chapter 3 that we can restrict our search to points of $\mathcal{O}_K^{N+1}$ whose content ideal is one of a finite list of ideals A, where A contains one ideal from each class in $\mathrm{Cl}(K)$. To process a lattice point we may convert it to an $\mathcal{O}_K^{N+1}$ vector and discard it if its content ideal is not in A. If $\mathcal{O}_K$ is a principal ideal domain this means to discard points of $\mathcal{O}_K^{N+1}$ if they are not primitive.

9.1.3 Processing in $\mathbb{P}^N(K)$

These checks performed on elements of $M \cong Z^{d(N+1)}$ and $L \subseteq \mathcal{O}_K^{N+1}$ are in general not enough to reduce the output to exactly one vector for each projective point represented. If $x \in \mathcal{O}_K^{N+1}$ and u is a unit of $\mathcal{O}_K$ then ux and x represent the same point in $\mathbb{P}^N(K)$ and their coefficients generate the same ideal. Therefore both x and ux would pass the checks on elements of M and L we have described so far. It may therefore be useful to keep track of projective points found, to avoid checking the same point for membership of $V(K)$ multiple times.

This is unlikely to be useful in every case: it could mean storing a large number of projective points that are not points on the variety. The choice of strategy is a trade-off between the time required to check whether a vector x satisfies the defining polynomials of V and the memory and time required to check whether x represents a projective point that has already been seen and to store it if it has not.

If K has unit rank 0 we have a simpler method to discard superfluous unit multiples of a vector. Fix a coherent system to identify the unit, which will be a root of unity, in a factorisation of an element of K. (This is a.factor().unit() for a number field element a in Sage [30].) For a vector x we discard x if the unit in the factorisation of the first non-zero entry of x is not 1. If K is $\mathbb{Q}$, this is achieved by only using one of $\{x, -x\}$ in Section 9.1.1.

9.2 Finding points by $\mathbb{Z}$-lattice enumeration

In this section we present two related algorithms for processing lattice vectors to construct projective points. Algorithm 3 employs the methods of Section 9.1 to find projective points from a lattice and also uses sub-functions which we call $\mathbb{Z}$check, $\mathcal{O}_K$check, and $\mathbb{P}^N$check. These are an opportunity to perform further checking at each stage of the construction of a projective point. We will give examples of the use of $\mathbb{Z}$check and $\mathcal{O}_K$check after stating Algorithm 3. We use ShortVectors to denote a function that constructs all $\mathbb{Z}$-lattice vectors up to a given length, such as the ShortVectors function in Magma [4] or qfminim in Pari [31].

Algorithm 3: Points from an $\mathcal{O}_K$-lattice via restriction of scalars and $\mathbb{Z}$-lattice enumeration

Input:

- $L \subset \mathcal{O}_K^{N+1}$, an $\mathcal{O}_K$-lattice, given by a pseudo-basis
- B_H, a bound on height,

and optionally:

- $\mathbb{Z}$check, a function $\mathbb{Z}^{(N+1)d} \to$ True or False,
- $\mathcal{O}_K$check, a function $\mathcal{O}_K^{N+1} \to$ True or False,
- $\mathbb{P}^N$check, a function $\mathbb{P}^N(K) \to$ True or False.

Output: - Points of $\mathbb{P}^N(K)$ of height less than or equal to B_H with a representative in L.

Note: The points of the output will have a $\mathbb{Z}$-module representative satisfying $\mathbb{Z}$check, have an $\mathcal{O}_K$-module representative satisfying $\mathcal{O}_\mathsf{K}$check and satisfy $\mathbb{P}^\mathsf{N}$check.

Initialisation:

Let A be a set of ideals of minimal norm for each class of $\mathrm{Cl}(K)$, as described in Chapter 3, and let N_K be the maximum norm of an ideal in A.

Let $B_L = (N+1)\exp\left(\frac{2(B_H+\log(N_K))}{d}\right) c_K$, as explained in Chapter 3.

Let M be the $\mathbb{Z}$-lattice generated from L with quadratic form given by the T_2-norm, as explained in Chapter 7.

Procedure:

```
For each $v \in \mathbb{Z}^{nd}$ generated by ShortVectors on $M$ with length bound $B_L$:
    If $v \neq 0$ and the first non-zero coefficient of $v$ is $> 0$ and $v$ is primitive
    and $\mathbb{Z}$check($v$) = True:
        set $w$ to be the vector in $\mathcal{O}_K^{N+1}$ represented by $v$.
        If the content ideal of $w$ is in $A$ and $\mathcal{O}_K$check($w$) = True:
            set $P$ to be the point in $\mathbb{P}^N(K)$ represented by $w$.
            If $\mathbb{P}^N$check($P$) = True:
                yield $P$.
```

A simple application of Algorithm 3 is the enumeration of points in $\mathbb{P}^N(K)$. We can use it to find points on any variety V in the following way. If $L = \mathcal{O}_K^{N+1}$ then every point of $\mathbb{P}^N(K)$ has a representative in L. Then for any $V \subseteq \mathbb{P}^N$ we can find all K-rational points of V of height $\leqslant B_H$ by simply checking whether each projective point of $\mathbb{P}^N(K)$ of height less than or equal to B_H is in $V(K)$. We can do this using Algorithm 3 by adding the requirement that $w \in \mathcal{O}_K^{N+1}$ satisfies the defining polynomials of V to the function $\mathcal{O}_K\mathsf{check}$. This method of finding rational points does not rely on V being smooth or irreducible and so is the most generally applicable.

We can also use Algorithm 3 to find points in a lattice of lifts $L_i \in \mathcal{O}_K^{N+1}$, where L_i has been constructed as in Chapters 5 and 6. In this case we use some information about L_i to further improve $\mathbb{Z}\mathsf{check}$.

Recall that if $L = L_i$ is a lattice of lifts for V at a point $\bar{P}$ then L_i contains all lifts of $\bar{P}$ that are roots of the defining polynomials of V modulo $\mathfrak{p}^i$. These are the lattice vectors that we are interested in as they are possible representatives for points of V. It is worth remembering that L_i contains many other vectors. In particular, the vectors that we want are $\mathfrak{p}$-primitive.

We recall the definition of L_i as the $\mathcal{O}_K$-module generated by $\{\pi^{|\alpha|}\widehat{s}_\alpha\}_{|\alpha|<i}$ and $\mathfrak{p}^i\mathcal{O}_K^{N+1}$. The vector $\widehat{s}_0$ is $\mathfrak{p}$-primitive by construction as it is a representative in $\mathcal{O}_K^{N+1}$ for $\bar{P} \in \mathbb{P}^N(\mathbb{F}_\mathfrak{p})$. (If a vector x is not $\mathfrak{p}$-primitive, every coordinate is in $\mathfrak{p}$ and so it reduces to $(0, \dots, 0) \mod \mathfrak{p}$, which does not define a projective point in $\mathbb{P}^N(\mathbb{F}_\mathfrak{p})$.) It is the only $\mathfrak{p}$-primitive vector in the generating set, as each vector $\widehat{s}_\alpha$ is multiplied by $\pi^{|\alpha|}$. Therefore, we may fix a basis for L_i so that it contains exactly one $\mathfrak{p}$-primitive vector: we call this vector b_0.

When L_i is converted from an $\mathcal{O}_K$-lattice to a $\mathbb{Z}$-lattice, b_0 will be converted to a set of d vectors $\beta_{0,1}b_0, \dots, \beta_{0,d}b_0$. If x in L_i is to represent a lift of $\bar{P}$, it must be $\mathfrak{p}$-primitive, so the coefficient of b_0 (as part of a basis for the $\mathcal{O}_K$-module L_i) must be non-zero modulo $\mathfrak{p}$. If we represent x using coefficients $a_{i,j}$ in $\mathbb{Z}^{d(N+1)}$, we need that $\sum_{j=1}^d a_{0,j}\beta_{0,j} \not\equiv 0 \mod \mathfrak{p}$. We can therefore discount points in $\mathbb{Z}^{d(N+1)}$ for which all $a_{0,j} \equiv 0 \mod p$, where p is the prime above $\mathfrak{p}$ in $\mathbb{Z}$. A small amount of work over K to calculate the sum $\sum_{j=1}^d a_{0,j}\beta_{0,j}$ and check it to make sure that it is not $0 \mod \mathfrak{p}$ would give a more stringent filter on lattice points, whilst still avoiding having to construct the vector in $\mathcal{O}_K^{N+1}$.

We defined $\phi_D(j)$ in Section 5.5 to denote the number of multi-indices of degree j in D variables. We used this to choose a $\mathfrak{p}$-adic precision to use in constructing lattices of lifts for a variety of dimension D. For ease of notation we will use $\phi(j) = \phi_D(j)$ in what follows, except when we need to distinguish between varieties of different dimension.

Algorithm 4 gives an example of how to use Algorithm 3 when L is a lattice of lifts. It may be useful to reverse the order of $\mathcal{O}_K\mathsf{check}$ and $\mathbb{P}^N\mathsf{check}$ or to remove the $\mathbb{P}^N\mathsf{check}$ condition, depending on the particular situation; Algorithm 4 provides one illustration of their use.

```
Algorithm 4: Points on a variety via $\mathbb{Z}$-lattice enumeration
  Input:
      - $V \subset \mathbb{P}^N$, a geometrically smooth, irreducible variety defined over $K$,
      - $B_H$, a bound on height.
  Output: - All points of $V(K)$ with height less than or equal to $B_H$.

  Procedure:
  Set $\mathfrak{p}$ to be a good prime for $V$, constructed from Algorithm 1.
  For each $\bar{P}$ on the reduced variety $\bar{V}(\mathbb{F}_\mathfrak{p})$:
      set $i$ to be the least $i$ such that $\sum_{j=0}^{i} \phi(j) \geqslant N+2$,
      set $L \leftarrow L_i$, lattice of lifts for $\bar{P}$,
      set $\mathbb{Z}$check to return False if $\sum_{j=1}^{d} a_{0,j}\beta_{0,j} \equiv 0 \mod \mathfrak{p}$ and True
      otherwise,
      set $\mathcal{O}_K$check to return True if and only if $w$ satisfies the defining
      polynomials of $V$,
      set $\mathbb{P}^N$check to return False if $P$ has been seen before, otherwise True.
      Return the output of Algorithm 3 with inputs $L$, $B_H$, $\mathbb{Z}$check,
      $\mathcal{O}_K$check and $\mathbb{P}^N$check.
```

We can use Algorithm 4 to find points on a smooth irreducible variety defined over any number field.

9.3 Finding points by lattice reduction

Given a form of lattice basis reduction whose output satisfies the conditions of Theorem 8.1, we can use this lattice reduction to find all points up to some height bound B_H on a variety V. After choosing a suitable prime ideal, for each point on the reduced variety $\bar{V}$ we construct a lattice of lifts L whose pseudo-basis we reduce. Let the reduced pseudo-basis be $(b_i, \mathfrak{b}_i)_{i=0}^{N}$. If the norm of the index of L is large enough then by Theorem 8.1 every vector of L with T_2-norm $\leqslant B_L$ will lie in a submodule L_0 of L given by $(b_i, \mathfrak{b}_i)_{i=0}^{N-1}$.

To force the norm of the index of L to be large, we must choose a prime ideal of large norm.

Lemma 9.1. *Let K be a number field of degree d and $V \subseteq \mathbb{P}^N$ a variety of dimension D defined over K. Let $x > 0$ and let $\mathfrak{p}$ be a prime of K of degree one which is a* *good prime for V, lying above a rational prime p that satisfies*

$$p > x^{(i(N+1)-\sum_{j=0}^{i-1}\phi(j)(i-j))^{-1}}.$$

Then for each point on the reduced variety $\bar{V}(\mathbb{F}_{\mathfrak{p}})$ at $\bar{P}$, the ith lattice of lifts L_i will satisfy

$$\mathcal{N}([\mathcal{O}_K^{N+1} : L_i]) > x.$$

Proof. By Theorem 6.6 we have $[\mathcal{O}_K^{N+1} : L_i] = \mathfrak{p}^{m_i}$, where $m_i \geqslant i(N+1) - \sum_{j=0}^{i-1}\phi(j)(i-j)$. Because $\mathfrak{p}$ has degree 1, $\mathcal{N}(\mathfrak{p}) = p$ and $\mathcal{N}([\mathcal{O}_K^{N+1} : L_i]) = p^{m_i}$. Therefore, we have

$$\mathcal{N}([\mathcal{O}_K^{N+1} : L_i]) = p^{m_i} > (x^{(i(N+1)-\sum_{j=0}^{i-1}\phi(j)(i-j))^{-1}})^{m_i} \geqslant x.$$

□

Our aim is to use Lemma 9.1 in conjunction with Theorem 8.1 to reduce the rank of the lattice or dimension of the variety containing the points we wish to find. We can do this whenever Theorem 8.1 applies, this is currently restricted to the five Euclidean imaginary quadratic fields. In Algorithm 5 we construct a good prime $\mathfrak{p}$ with large norm so that $\mathcal{N}([\mathcal{O}_K^{N+1} : L_i])$ satisfies the condition of Theorem 8.1 and all vectors in L_i with squared T_2-norm $\leqslant B_L$ can be written without use of the final pseudo-basis vector b_N. This allows us to restrict our search to a subvariety V' of V which will usually have smaller dimension. We will then use Algorithms 6 and 7 to find points on V'. Algorithm 5 can be found on page 88.

9.3.1 Finding points from a sublattice or subvariety

We will now discuss methods for finding points of bounded height on the subvariety V' of V; these are needed in Algorithm 5.

The simplest way to find points from a reduced lattice basis is to use Algorithm 4 to find points in L_0. The rank of L_0 as a $\mathbb{Z}$-lattice is Nd, which represents an improvement on the index of L_i which is $(N+1)d$. Finding points in L_0 by $\mathbb{Z}$-lattice enumeration is always an option in cases where other methods cannot be used or are inefficient. However, it is not always the most efficient method.

In some situations, we may use the subvariety $V' \subset V$ to find points. Once a lattice basis has been constructed and reduced, we can use it change coordinates on $\mathbb{P}^N(K)$. If polynomials $\underline{F}$ define V then the polynomials $G_j(x_0, \ldots, x_N) = F_j(\sum_{i=0}^{N} x_i b_i)$ describe V in new coordinates. G_j are homogeneous polynomials with the same degrees as F_j. We use the additional information that the points we are

Algorithm 5: Points on a variety via lattice reduction

Input:

- LatticeRed, a method of lattice reduction that takes an $\mathcal{O}_K$-lattice and outputs a reduced pseudo-basis that satisfies the conditions of Theorem 8.1, with constants as defined in that Theorem,
- $V \subset \mathbb{P}^N$, a variety defined over a number field K for which LatticeRed is known to work, defined by polynomials $\underline{F}$ in $\mathcal{O}_K[X_0, \ldots, X_N]$,
- B_H, a bound on height.

Note: We require K to be imaginary quadratic for LatticeRed to satisfy Theorem 8.1, such a LatticeRed is currently known only for Euclidean fields.

Output: - All points of $V(K)$ with height less than or equal to B_H.

Initialisation:
Let A be a set of ideals of minimal norm for each class of $\mathrm{Cl}(K)$, as described in Chapter 3, and let N_K be the maximum norm of an ideal in A.
Let $B_L = (N+1)\exp\left(\frac{2(B_H+\log(N_K))}{d}\right) c_K$, as explained in Chapter 3.
Let i be the least integer such that $\sum_{j=0}^{i} \phi(j) \geqslant N+2$.
Set $m(i) \leftarrow \left(i(N+1) - \sum_{j=0}^{i-1} \phi(j)(i-j)\right)^{-1}$.
Let $\mathfrak{p}$ be the result of Algorithm 1 with lower bound on the norm of $\mathfrak{p}$ given by

$$\mathcal{N}(\mathfrak{p}) > \left(Z_2^{-d(N+1)} d^{-(Z_1+1)d(N+1)/2} Y_2^{N+1} B_L^{Z_1(N+1)d/2} Y_1^{-Z_1(N+1)} 2^{Z_1(N+1)d/2}\right)^{m(i)}.$$

Procedure:

```
For each $\bar{P}$ on the reduced variety $\bar{V}(\mathbb{F}_\mathfrak{p})$:
    set $L \leftarrow L_i$, lattice of lifts for $\bar{P}$,
    set $(b_j, \mathfrak{b}_j)_{j=o0}^{N}$ be LatticeRed$(L)$,
    set $V'$ to be the variety defined by $\underline{F}$ and $b_N.(X_0, \ldots, X_N)$.
    Yield each point of $L_0$ lying in $V'$ with height $\leqslant B_H$ (using
    Algorithm 6 or 7).
```

searching for do not involve the vector b_N in the old coordinates: this means that $x_N = 0$ in new coordinates. If V is not contained in the hyperplane $x_N = 0$, then $\dim(V') = \dim(V) - 1$. Equivalently, we can consider V' in the old coordinates as being defined by $\underline{F}$ and the linear homogeneous polynomial $b_N.(X_0, \ldots, X_N)$.

We now outline some special cases in which we may use V' to find points without needing to use $\mathbb{Z}$-lattice enumeration on L_0.

If V is a curve and $\dim(V') = 0$ then $V'(K)$ is a finite collection of points, which can be found with relative ease. If V is a plane curve given by a single polynomial $G(x_0, x_1, x_2)$ then this can be achieved simply by factorising $G(x_0, x_1, 0)$ over K: linear factors correspond to points on V. For curves in higher ambient dimensions we use Gröbner basis methods.

If $0 < \dim(V') < \dim(V)$ then there are two particular cases in which we can find all points without constructing any new lattices. If $\bar{P} \notin \bar{V}'(\mathbb{F}_\mathfrak{p})$ then there can be no points of $V'(K)$ which reduce to $\bar{P} \mod \mathfrak{p}$. In this case we can stop computing with $\bar{P}$ altogether as there are no points of $V(K)$ with height $\leqslant B_H$ that reduce to $\bar{P} \mod \mathfrak{p}$.

If $\bar{P}$ is a smooth point of $\bar{V}'(\mathbb{F}_\mathfrak{p})$ then we form a lattice of lifts for V' based at $\bar{P}$. The index of L_i for $\bar{P}$ and V' will exceed that of L_i for $\bar{P}$ and V, because $\phi_{\dim(V)}(j) \geqslant \phi_{\dim(V')}(j)$ for each j. In this case, we may perform the lattice reduction step on the new L_i for V', aiming for a further reduction in the rank of lattice or dimension of variety for the resulting set of possible representatives. It is vital that we are able to use the same prime so that the new lattice is also a lattice of lifts of the particular reduced point $\bar{P}$.

We use these ideas in the following algorithm.

```
Algorithm 6: Points on a subvariety after lattice reduction
Input:
    - $\bar{P} \in \bar{V}(\mathbb{F}_\mathfrak{p})$,
    - $B_H$, a bound on height,
    - $V'$, a subvariety of $V$,
    - $L_0$, a lattice of lifts for $\bar{P}$ on $\bar{V}(\mathbb{F}_\mathfrak{p})$, all as found in Algorithm 5.
Note: As for Algorithm 5, we require the number field $K$ to be Euclidean and
imaginary quadratic.
Output: - All points of $V'(K)$ with height less than or equal to $B_H$ that
          reduce to $\bar{P} \mod \mathfrak{p}$.

Procedure:
If $\dim(V') = 0$:
    yield each point of $V'(K)$ of height $\leqslant B_H$ using a Gröbner basis
    method.
Else if $0 < \dim(V') < \dim(V)$:
    If $\bar{P} \notin \bar{V}'(\mathbb{F}_\mathfrak{p})$:
        exit.
    If $\bar{P}$ is a smooth point on $\bar{V}'$:
        set $L \leftarrow L_i$ for $\bar{P}$ and $V'$ and go to lattice reduction step of
        Algorithm 5.
Else:
    use Algorithm 4 on $L_0$ to find points on $V'$ of height $\leqslant B_H$ that reduce
    to $\bar{P} \mod \mathfrak{p}$.
```

Algorithm 6 uses V' in some special cases; we now explore the idea of using V' in more generality. If V' is smooth we may find points on V' using lattices of lifts and lattice reduction: we may use this method recursively. This recursion only makes sense when $\dim(V') < \dim(V)$. Once $\dim(V') = 0$, we can find points via the substitution method described above.

However, if $\bar{P}$ is a point on $\bar{V}'(\mathbb{F}_\mathfrak{p})$ that is not smooth (this is the only case remaining after excluding the conditions in Algorithm 6) we can no longer construct lattices of lifts based at $\bar{P}$, as $\bar{V}'$ is not smooth at $\bar{P}$. Therefore, a new good prime $\mathfrak{q}$ for V' should be found and lattices of lifts constructed for each reduced point of $\bar{V}'(\mathbb{F}_\mathfrak{q})$. By finding each point of $V'(K)$ of height $\leqslant B_H$, we may find every point of V that reduces to $\bar{P} \mod \mathfrak{p}$ with height $\leqslant B_H$. The major drawback to this method is that we spend time finding points of V' that do not reduce to $\bar{P} \mod \mathfrak{p}$. When

V' is not smooth and the two special cases mentioned before do not hold, we have to resort to lattice enumeration on L_0.

Finally, if $\dim(V') = \dim(V)$ then, because V is irreducible, $V' = V$. This occurs when V lies within the hyperplane defined by $x_N = 0$ in the new coordinates. In this case, by changing variables, we may consider $V \subset \mathbb{P}^{N-1}$, thus reducing the ambient dimension. It may then be a worthwhile strategy to start the whole computation of points on $V' = V$ again. A new prime of larger norm will most likely be required for lattice reduction methods, but the resulting lattices of lifts would have a smaller $\mathbb{Z}$-rank of $(N-1)d$.

Further investigation is needed to establish whether and when the construction of a new prime and new set of lattices of lifts is likely to be more efficient than $\mathbb{Z}$-lattice enumeration. These methods are illustrated in Algorithm 7, which is a development of Algorithm 6.

Currently no examples exist of points found with Algorithms 5, 6 and 7; further work would be required to implement a suitable LatticeRed method.

Algorithm 7: Points on a subvariety after lattice reduction with recursion

```
Input:
    - $\bar{P} \in \bar{V}(\mathbb{F}_{\mathfrak{p}})$,
    - $B_H$, a bound on height,
    - $V'$, a subvariety of $V$,
    - $L_0$, a lattice of lifts for $\bar{P}$ on $\bar{V}(\mathbb{F}_{\mathfrak{p}})$, all as found in Algorithm 5.
Note: As for Algorithm 5, we require the number field $K$ to be Euclidean and
imaginary quadratic.
Output: - All points of $V'(K)$ with height less than or equal to $B_H$ that
          reduce to $\bar{P}$ mod $\mathfrak{p}$.

Procedure:
If $\dim(V') = 0$:
    yield each point of $V'(K)$ of height $\leqslant B_H$ by a Gröbner basis method.
Else if $0 < \dim(V') < \dim(V)$:
    If $\bar{P} \notin \bar{V}'(\mathbb{F}_{\mathfrak{p}})$:
        exit.
    If $\bar{P}$ is a smooth point on $\bar{V}'$:
        set $L \leftarrow L_i$ for $\bar{P}$ and $V'$ and go to lattice reduction step of
        Algorithm 5.
    Else:
        use Algorithm 4 on $L_0$ to find points on $V'$ of height $\leqslant B_H$.
Else:
    yield points on $V(K) \subset \mathbb{P}^{N-1}(K)$ of height $\leqslant B_H$ which reduce to $\bar{P}$
    mod $\mathfrak{p}$ using Algorithm 5.
```

9.4 Examples

We have implemented a version of Algorithm 4 for curves in Sage [30], with the actual enumeration of short vectors in $\mathbb{Z}$-lattices performed by the Magma [4] function ShortVectors. This has been parallelised to allow multiple lattices to be searched simultaneously. We provide some examples of curves and points found on them using this implementation.

Let $\mathcal{C}_1$ be the plane unit circle, given by the polynomial $X^2 + Y^2 - Z^2$ over the quintic number field defined by $x^5 - 2x^4 + 4x^3 - 5x + 1$. We searched for representatives for points on $\mathcal{C}_1$ with squared T_2-norm up to 300 and found 92 points.

By Theorem 3.10, a search with $B_L = 300$ for a curve in $\mathbb{P}^2$ over this number field finds all points of logarithmic height up to -1.7146. Twelve of the points found are the points defined over $\mathbb{Q}$ with logarithmic height up to $\log(5)$. This demonstrates that we may find points of larger height than expected with our method, although we cannot guarantee that all such points are found.

Let $\mathcal{C}_2$ be the genus 3 modular curve $X_{S_4}(13)$ as studied in [2], given as a plane curve by

$$4X^3Y - 3X^2Y^2 + 3XY^3 - X^3Z + 16X^2YZ - 11XY^2Z + 5Y^3Z + \\ 3X^2Z^2 + 9XYZ^2 + Y^2Z^2 + XZ^3 + 2YZ^3$$

over the quadratic number field $\mathbb{Q}(\sqrt{13})$. By searching for representatives of points with squared T_2-norm up to 5000 on $\mathcal{C}_2$ we verified the six points on $\mathcal{C}_2$ defined over $\mathbb{Q}(\sqrt{13})$ in [2]:

$$\{(1:3:-2), (0:0:1), (0:1:0), (1:0:0), (3 \pm \sqrt{13}:0:2)\},$$

and found no other points of $\mathcal{C}_2$. These are all of the points on $\mathcal{C}_2(\mathbb{Q}(\sqrt{13}))$ with logarithmic height up to 5.24.

Let $\mathcal{C}_3$ be the cubic curve defined by the polynomial

$$3X^3 - 13X^2Y + 4X^2Z + 2XY^2 + XYZ - Y^3 - 5Y^2Z - YZ^2 + Z^3$$

over the number field generated by α, where α is a root of $x^3 - 2x^2 + 13x - 3$. $\mathcal{C}_3$ considered as a curve defined over $\mathbb{Q}$ is an example from [9] of a representative of a non-trivial element of $\text{Ш}(E/Q)[3]$ for the elliptic curve E defined over $\mathbb{Q}$ by $y^2 + xy = x^3 + x^2 - 1154x - 15345$. The cubic field has been chosen so as to guarantee the existence of a rational point of $\mathcal{C}_3$ over this field. After a search for representatives of points with square T_2-norm up to 50, the points $(\alpha^2 - 2\alpha + 13 : 3 : 0)$ and $(\alpha - 4 : -\alpha^2 + 2\alpha - 10 : 9)$ were found. By performing this calculation we have demonstrated that there are no other rational points on $\mathcal{C}_3(\mathbb{Q}(\alpha))$ with logarithmic height less than or equal to 1.16.

Let $\mathcal{C}_4$ be the elliptic curve defined by $-X^3 - X^2Z + Y^2Z - XZ^2 + YZ^2$ over the field $\mathbb{Q}(\sqrt[3]{5})$. The Mordell-Weil rank of this curve defined over $\mathbb{Q}$ is 0. The suggestion of this curve came from Vladimir Dokchitser, who showed in [12] that if the Birch and Swinnerton-Dyer conjecture holds for elliptic curves over number fields then this curve has a point of infinite order over the field $\mathbb{Q}(\sqrt[3]{m})$ for every cube-free $m > 1$. However, we have not found any examples of such points. The points found so far from a search (ongoing at the time of writing) for representatives with T_2-norm up to 1000 has yielded only the three known torsion points of $\mathcal{C}_4$, defined over $\mathbb{Q}$: $(0:-1:1),(0:0:1),(0:1:0)$. This calculation will find all points on $\mathcal{C}_4$ over $\mathbb{Q}(\sqrt[3]{5})$ with logarithmic height up to 1.247.

Let $\mathcal{C}_5$ be the elliptic curve defined by

$$-X^3+X^2Z+XYZ+Y^2Z+292XZ^2-4241Z^3.$$

This curve is known to have rank 0 over $\mathbb{Q}$. Because it is a quadratic twist of the elliptic curve with Cremona label 605c1, which has rank 1 over $\mathbb{Q}$, $\mathcal{C}_5$ has a point of infinite order over $\mathbb{Q}(\sqrt{5})$. A search for representatives with squared T_2-norm up to 1000, which guarantees finding all points on $\mathcal{C}_5$ of logarithmic height up to 4.63, returned the point $(0:1:0)$.

Let $\mathcal{C}_6$ be the intersection of quadrics in $\mathbb{P}^3$ defined by $XW+YZ+YW+W^2$ and $XY+XZ+2Z^2-3ZW$. This curve arises from a second 2-descent on the elliptic curve over $\mathbb{Q}$ with Cremona label 27382a1 which was performed in Magma [4]. A search for points of squared T_2-norm up to 1000 over the quadratic field $\mathbb{Q}(\sqrt{5})$ yielded the $\mathbb{Q}$-rational points $(-9/5:2:-3/5:1),(-2:0:1:0),(4/3:-1:4/3:1),(11/4:-3/2:3/2:1),(0:-2/5:3/2:1),(-1:0:2:1),(0:-1:0:1),(0:1:0:0),(6:-7/3:2:1),(-1:6:-1:1),(-1:0:0:1)$ and $(1:0:0:0)$: this includes all points on $\mathcal{C}_6(\mathbb{Q}(\sqrt{5}))$ of logarithmic height $\leqslant 4.34$.

Let $\omega=\sqrt{26521}$. Let $\mathcal{C}_7$ be the elliptic curve defined over $\mathbb{Q}(\omega)$ by

$$\begin{aligned}-37128125X^3+(81003\omega+13179867)X^2Z+(-57225\omega+27522500)XYZ+\\ 37128125Y^2Z+(-81003\omega-13179867)YZ^2.\end{aligned}$$

This curve was suggested to the author by Johan Bosman. It conjecturally has rank 2 over $\mathbb{Q}(\omega)$, with a torsion subgroup of order 18. A search for representatives with T_2-norm up to 100000 found only the torsion points $(0:1:0)$ and $(0:0:1)$; with this calculation we have shown that any other points must have logarithmic height greater than -288.31. The two real embeddings of a fundamental unit of this field are about 10^{128} and 10^{-128}, and so $c_{\mathbb{Q}(\omega)}$ is around 10^{128}! The disparity in the size of the two embeddings of a unit accounts for the very small height bound attained, relative to the bound on T_2-norm used.

All computations were performed on machines at the University of Warwick with AMD Opteron™processors 6174 and 8378, with speeds of 2200 and 2400 MHz respectively. All machines were running Ubuntu 12.04 (LTS) server edition. The following table contains indications of total timings for each of the three main parts of the algorithm: finding points on the reduced curve, constructing lattices of lifts and searching for points in these lattices of lifts. All examples were performed using small primes that were chosen by hand. The time should depend on the norm of the prime, number of reduced points (which is related to the norm of the prime), the degree of the number field, the ambient dimension and of course the length bound.

Except in the smallest of the examples, almost all of the time is spent on finding points in lattices by exhaustive search. We could hope to improve this by changing the size of the prime used (an increase would yield more lattices, each with fewer points with length $\leqslant B_L$) and optimising the way that points are found and processed. An implementation of Algorithm 5 would remove this step entirely and might provide an improvement in speed.

Curve	Norm of prime	Number of reduced points	Degree of field	Ambient dimension	Length bound	Time to find reduced points	Time to construct lattices	Time to find points from lattices
$\mathcal{C}_1$	23	24	5	2	300	0.0359s	677s	296509s
$\mathcal{C}_2$	17	20	2	2	5000	0.0450s	12.7s	5599s
$\mathcal{C}_3$	19	16	3	2	50	0.0269s	14.1s	16.1s
$\mathcal{C}_4$	29	24	3	2	1000	0.0451s	19.3s	714393s
$\mathcal{C}_5$	31	34	2	2	1000	0.0556s	20.8s	8739s
$\mathcal{C}_6$	11	18	2	3	1000	0.936s	17.1s	59157s
$\mathcal{C}_7$	11	20	2	2	100000	0.0392s	107s	1574s

Bibliography

[1] George B. Arfken, Hans J. Weber, and Frank E. Harris. *Mathematical Methods for Physicists.* Academic Press, Boston, seventh edition, 2013.

[2] B. S. Banwait and J. E. Cremona. Tetrahedral Elliptic Curves and the local-to-global principle for Isogenies. *ArXiv e-prints*, August 2013, 1306.6818.

[3] Z.I. Borevich and I.R. Shafarevich. *Number Theory.* Academic Press, 1966.

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

[5] Henri Cohen. *A Course in Computational Algebraic Number Theory.* Springer-Verlag, 1993.

[6] Henri Cohen. *Advanced Topics in Computational Number Theory, GTM 138*, volume 193 of *Graduate Texts in Mathematics.* Springer, 2000.

[7] Brian Conrad. L-functions and Dirichlet Density for Global Fields. `math.stanford.edu/~conrad/249BPage/handouts/dirdensity.pdf`. Lecture notes, online.

[8] David A. Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra, 3/e (Undergraduate Texts in Mathematics).* Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2007.

[9] J. E. Cremona, T. Fisher, C. O'Neil, D. Simon, and M. Stoll. Explicit n-descent on elliptic curves. III. Algorithms. *ArXiv e-prints*, July 2011, 1107.3516.

[10] J. E. Cremona, D. A. Roberts, and C. L. Turner. Report MD8 for the European Marie Curie Research Training Network GTEM: Lattice-based methods for point-finding over number fields and function fields, 2010.

[11] J. E. Cremona and D.A. Roberts. Preliminary Report MD7 for the European Marie Curie Research Training Network GTEM: Applications of polynomial lattices to point-finding over rational function fields. 2008.

[12] Vladimir Dokchitser. Root numbers of non-abelian twists of elliptic curves. *Proceedings of the London Mathematical Society*, 91(2):300–324, 2005.

[13] N. Elkies. Rational points near curves and small nonzero $|x^3 - y^2|$ via lattice reduction. Lecture Notes in Computer Science 1838 (proceedings of ANTS-IV), pages 33–63, 2000.

[14] C. Fieker and M.E. Pohst. On Lattices over Number Fields. In *Algorithmic Number Theory: Second International Symposium, ANTS-II, Talence, France, May 18 - 23, 1996, Proceedings*, volume 1122 of *Lecture Notes in Computer Science*, pages 133–140. Springer, 1996.

[15] Claus Fieker and Damien Stehlé. Short bases of lattices over number fields. In *Algorithmic number theory*, volume 6197 of *Lecture Notes in Comput. Sci.*, pages 157–173. Springer, Berlin, 2010.

[16] G.H. Hardy and E.M. Wright. *An Introduction to the Theory of Numbers.* Oxford science publications. Oxford University Press, fifth edition, 1979.

[17] D. R. Heath-Brown. Personal communication to John Cremona, November 1999.

[18] Nicholas J. Higham. *Accuracy and Stability of Numerical Algorithms.* Society for Industrial and Applied Mathematics, 1996.

[19] F. Lemmermeyer. The Euclidean Algorithm in Algebraic Number Fields. `http://www.rzuser.uni-heidelberg.de/%7Ehb3/publ/survey.pdf`, 2004. Online, accessed August 2013.

[20] F. Lemmermeyer. Class Field Theory. `http://www.fen.bilkent.edu.tr/~franz/cft.html`, 2007. Online, accessed January 2012.

[21] A.K. Lenstra, Jr. Lenstra, H.W., and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261(4):515–534, 1982.

[22] R. Long. *The Algorithmic Solution of Simultaneous Diophantine Equations.* PhD thesis, Oxford Brookes University, 2005.

[23] Huguette Napias. A generalization of the LLL-algorithm over euclidean rings or orders. *Journal de Théorie des Nombres de Bordeaux*, 8:387–396, 1996.

[24] Jürgen Neukirch. *Algebraic Number Theory (Grundlehren der mathematischen Wissenschaften).* Springer, 1999.

[25] Beresford N. Parlett. *The Symmetric Eigenvalue Problem.* Society for Industrial and Applied Mathematics, 1998.

[26] D. A. Roberts. *Explicit Descent On Elliptic Curves Over Function Fields.* PhD thesis, University of Nottingham, 2007.

[27] R. Tyrrell Rockafellar. *Convex analysis.* Princeton Mathematical Series, No. 28. Princeton University Press, Princeton, N.J., 1970.

[28] J.H. Silverman. *The Arithmetic of Elliptic Curves, GTM 106.* 1985.

[29] W.A. Stein. *Algebraic Number Theory, a Computational Approach.* 2005. Available online at `modular.math.washington.edu/books/ant/ant.pdf`.

[30] W. A. Stein et al. *Sage Mathematics Software (Version 5.10).* The Sage Development Team, 2013. `http://www.sagemath.org`.

[31] The PARI Group, Bordeaux. *PARI/GP, version* `2.5.4`, 2013. available from `http://pari.math.u-bordeaux.fr/`.

[32] Mark Watkins. Searching for Points with the Elkies ANTS-IV Algorithm. `http://magma.maths.usyd.edu.au/~watkins/papers/padic.ps`, Unknown date.

[33] T. Womack. *Explicit Descent on Elliptic Curves.* PhD thesis, University of Nottingham, 2003.