A computational method for the construction of Siegel sets in complex hyperbolic space

A thesis submitted to University College London
for the degree of Doctor of Philosophy

Brian Michael Tyler

March 2010

Department of Mathematics
University College London

I, Brian Michael Tyler, confirm that the work presented in this thesis is my own. Where information has been derived from other sources, I confirm that this has been indicated in the thesis.

Abstract

This thesis presents a computational method for constructing Siegel sets for the action of $\Gamma = \mathrm{SU}(n,1;\mathfrak{O})$ on $\mathbb{H}^n_{\mathbb{C}}$, where $\mathfrak{O}$ is the ring of integers of an imaginary quadratic field with trivial class group. The thesis first presents a basic algorithm for computing Siegel sets and then considers practical improvements which can be made to this algorithm in order to decrease computation time. This improved algorithm is implemented in a C++ program called `siegel`, the source code for which is freely available at `http://code.google.com/p/siegel/`, and this program is used to compute explicit Siegel sets for the action of all applicable groups Γ on $\mathbb{H}^2_{\mathbb{C}}$ and $\mathbb{H}^3_{\mathbb{C}}$.

Acknowledgements

Principally I would like to extend my most sincere thanks to Dr. Andrei Yafaev, not just for his continued academic support over the four and something years that I've taken to complete this PhD., but also for his friendship and for not giving up on me during the tough times that are an almost inevitable part of such a program of study and research.

In a world of such stark and growing disparity between those with opportunity and those without as that which we inhabit, a man who has been as fortunate as I would do well to remember that his life is one filled with opportunity by virtue of the people who have given him those opportunities and supported him throughout his entire life. For me those people have been and continue to be my parents. As I grow older I realise the sacrifices that they have made for me and for them I shall be eternally grateful.

UCL has given me a first rate education; perhaps not necessarily the education I would have asked for, but nonetheless I couldn't fault it. Being given the chance to live amongst the intellectual elite in the heart of what is perhaps the greatest and freest city in the world for three years entirely at the taxpayer's expense is a privilege afforded to very few and I am deeply thankful to those people who deemed me worthy of such a privilege.

I would like to add a special mention for Dr. Vassili Corbas of Reading University as he was the person who really got me interested in mathematics beyond the box-ticking exam-centric mindset of the modern university student. It was his passion for the subject that inspired me and I'm sure that without his help I would probably now be working as a middle ranking accountant at the Carphone Warehouse (a fate to which I once came perilously close).

Contents

Chapter 1

Results

The following results were obtained from a C++ application called `siegel` which implements an algorithm based on Algorithm 5.10.1. The source code is released under the GPL v3.0 license and can be found here: `http://code.google.com/p/siegel/`. The application consists of approximately 10,000 lines of code and its design and implementation comprised the majority of the work involved in this PhD. thesis.

1.1 Siegel Sets in 2 and 3 Dimensions

Theorem 1.1.1 *Let $K = \mathbb{Q}\left(\sqrt{d}\right)$ be an imaginary quadratic field with ring of integers $\mathfrak{O}$, suppose that $Cl(K) = 1$ and let S_∞ be a Siegel container for $\Gamma = \mathrm{SU}(2,1;\mathfrak{O})$. Then $\mathrm{S}_\infty(L)$ is a Siegel set for Γ, where:*

$d = -1$	$L = 0.999978433493$	$\lvert \mathcal{C}_K \rvert \leq 23$
$d = -2$	$L = 0.499996205477$	$\lvert \mathcal{C}_K \rvert \leq 181$
$d = -3$	$L = 0.999992068197$	$\lvert \mathcal{C}_K \rvert \leq 17$
$d = -7$	$L = 0.791053494930$	$\lvert \mathcal{C}_K \rvert \leq 27$
$d = -11$	$L = 0.331422584272$	$\lvert \mathcal{C}_K \rvert \leq 451$
$d = -19$	$L = 0.249830466184$	$\lvert \mathcal{C}_K \rvert \leq 827$
$d = -43$	$L = 0.113480677567$	$\lvert \mathcal{C}_K \rvert \leq 9253$
$d = -67$	$L = 0.074467903908$	$\lvert \mathcal{C}_K \rvert \leq 33466$
$d = -163$	$L = 0.009440545740$	$\lvert \mathcal{C}_K \rvert \leq 36096934$

Theorem 1.1.2 *Let $K = \mathbb{Q}\left(\sqrt{d}\right)$ be an imaginary quadratic field with ring of integers $\mathfrak{O}$, suppose that $Cl(K) = 1$ and let S_∞ be a Siegel container for $\Gamma = \mathrm{SU}(3,1;\mathfrak{O})$. Then $\mathrm{S}_\infty(L)$ is a Siegel set for Γ, where:*

$d = -1$	$h = 0.987391129157$	$\lvert \mathcal{C}_K \rvert \leq 108$
$d = -2$	$h = 0.577540291822$	$\lvert \mathcal{C}_K \rvert \leq 2258$
$d = -3$	$h = 0.999085879138$	$\lvert \mathcal{C}_K \rvert \leq 47$
$d = -7$	$h = 0.493756821420$	$\lvert \mathcal{C}_K \rvert \leq 1601$

$d=-11$	$h=0.536411563086$	$\mid \mathcal{C}_K \mid \leq 773$
$d=-19$	$h=0.196138009090$	$\mid \mathcal{C}_K \mid \leq 104813$
$d=-43$	$h=0.059149067053$	$\mid \mathcal{C}_K \mid \leq 46224490$
$d=-67$	$h=0.010418787475$	
$d=-163$	$h=0.000040212980$	

When computing a lower height bound for $n=3, d=-43$ and $n=3, d=-67$ the computer was told to accept a sub-optimal height bound in order to speed up computation; this means that the results are not as good as they could be. When computing the lower height bound for $n=3, d=-163$ the computer was told to accept a highly sub-optimal height bound, this means that this result is most likely very far from the actual height bound, however computation time was still around two and a half months; due to modifications made to the algorithm since this computation was performed, it would probably now be somewhat faster than this to compute this value.

An upper bound on the number of cusps for $n=3, d=-67$ is definitely computable in practise with the current library and technology, however it is likely to take a few months of computation time based on the computation time for $n=3, d=-43$ which was approximately two days. An upper bound for $n=3, d=-163$ is not realistically computable without either greatly improving the height bound, or using a very powerful supercomputer.

Lemma 1.1.3 *Let $\underline{\mathbf{v}} \in \mathbb{H}^n_{\mathbb{C}}$, let $\mathbf{q} \in \mathcal{C}_K$ be a cusp of dilation factor δ and suppose that $\mathrm{h}(\underline{\mathbf{v}}) > 2\delta^{-1}$. Then $\mathrm{e}_{\mathbf{q}}(\underline{\mathbf{v}}) \geq 1$.*

PROOF Expanding out the effect function $\mathrm{e}_{\mathbf{q}}(\underline{\mathbf{v}}) = \mid \langle \underline{\mathbf{v}}, \mathbf{q} \rangle \mid^2 \geq \left| \frac{\delta \mathrm{h}(\underline{\mathbf{v}})}{2} \right|^2 \geq \left| \frac{\delta 2\delta^{-1}}{2} \right|^2 = 1.$ ∎

Corollary 1.1.4 *Let $K = \mathbb{Q}\left(\sqrt{d}\right)$ be an imaginary quadratic field with ring of integers $\mathfrak{O}$, suppose that $Cl(K) = 1$, let S_∞ be a Siegel container for $\Gamma = \mathrm{SU}(2,1;\mathfrak{O})$, let L be as in Theorem 1.1.1, take Δ as*

$d=-1$	$\Delta=4$
$d=-2$	$\Delta=16$
$d=-3$	$\Delta=4$
$d=-7$	$\Delta=6$
$d=-11$	$\Delta=36$
$d=-19$	$\Delta=64$
$d=-43$	$\Delta=310$
$d=-67$	$\Delta=721$
$d=-163$	$\Delta=44881$

Then whenever $\delta > \sqrt{\Delta}$, $\mathcal{C}_{K_\delta}(\mathrm{S}_\infty(L)) = \emptyset$.

Corollary 1.1.5 *Let $K = \mathbb{Q}\left(\sqrt{d}\right)$ be an imaginary quadratic field with ring of integers $\mathfrak{O}$, suppose that*

$Cl(K) = 1$, let S_∞ be a Siegel container for $\Gamma = \mathrm{SU}(3,1;\mathfrak{O})$, let L be as in Theorem 1.1.2, take Δ as

$d = -1$	$\Delta = 4$
$d = -2$	$\Delta = 11$
$d = -3$	$\Delta = 4$
$d = -7$	$\Delta = 16$
$d = -11$	$\Delta = 13$
$d = -19$	$\Delta = 103$
$d = -43$	$\Delta = 1143$
$d = -67$	$\Delta = 36848$
$d = -163$	$\Delta = 2473588627$

Then whenever $\delta > \sqrt{\Delta}$, $\mathcal{C}_{K_\delta}(\mathrm{S}_\infty(L)) = \emptyset$.

Chapter 2

Introduction

This thesis presents an algorithmic approach to the problem of constructing Siegel sets for the action of $\mathrm{SU}(n,1;\mathfrak{O})$ on $\mathbb{H}^n_{\mathbb{C}}$ where $\mathfrak{O}$ is the ring of integers of some imaginary quadratic field. The problem is solved for the case of fields with trivial class group in Algorithm 4.6.2. This first algorithm is quite naïve; this makes it easy to analyse from a theoretical perspective, but contains too many inefficiencies to be a practical candidate for implementation, as such computational improvements to Algorithm 4.6.2 are considered and an improved algorithm is given in Algorithm 5.10.1. The improved algorithm is implemented as a C++ application and this application is used to compute explicit Siegel sets for all fields with trivial class group in dimensions 2 and 3, these results are presented in Chapter 1.

Both the basic and computationally improved algorithms implement the same control flow; this is described in Figure 2. The algorithm takes three inputs; n the complex hyperbolic dimension of the space to work in, d a Heegner number (an integer d such $\mathbb{Q}(\sqrt{-d})$ has trivial class group) and $\alpha \in (0,1)$ an error tolerance, the closer α is to 1 the more accurate the result. The algorithm then proceeds as follows:

1. A Siegel set for the stabilizer of the point at infinity is computed analytically using a formula, see Lemma 4.2.6 and Lemma 5.1.2. Call this set X.

2. Cusps are generated which are candidates for raising the height of points in X.

3. The set X is iterated through to see if every point in it can be raised above a certain threshold level by the current set of cusps.

4. If the threshold height is reached the algorithm terminates and outputs a height which determines a Siegel set. Otherwise more cusps are generated and the process is repeated until the threshold height is attained.

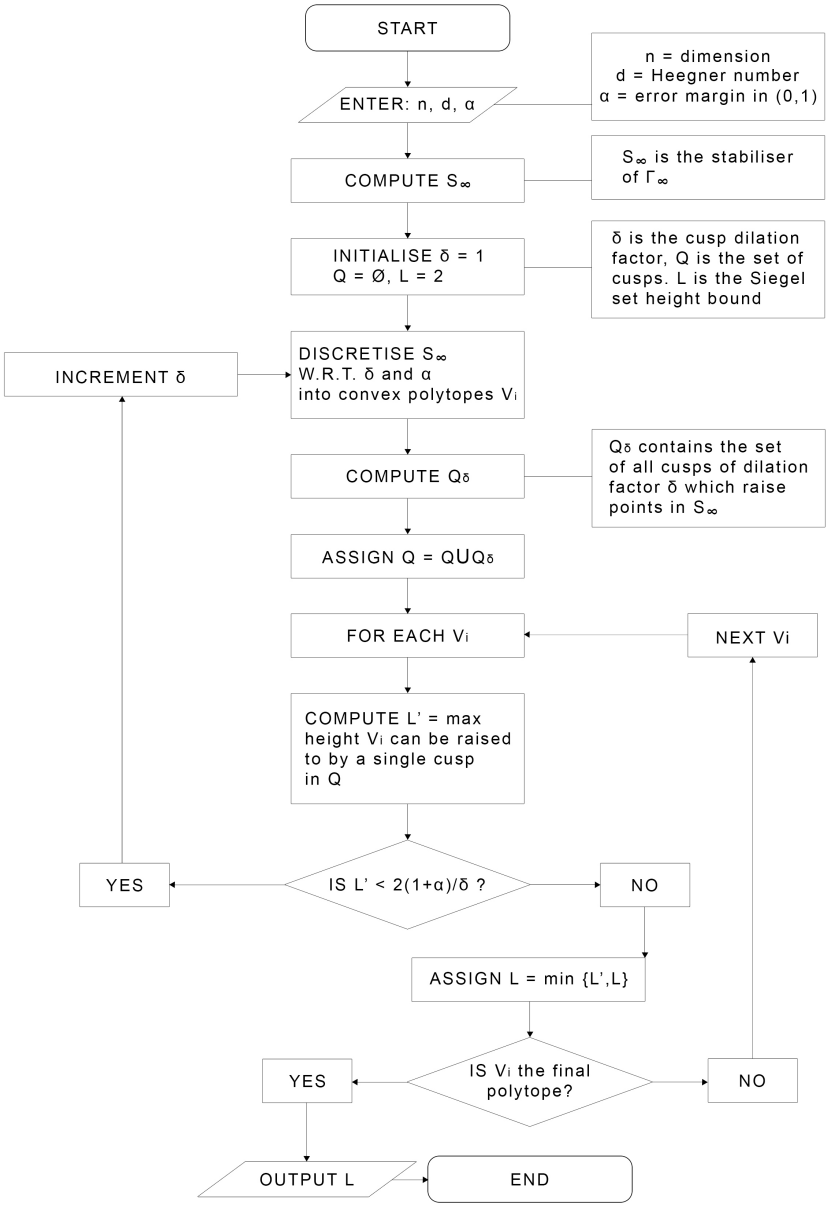


Figure 2.1: Control Flow of the Siegel Set Generating Algorithm

2.1 The current state of knowledge

At the point of commencing this work analytic solutions to the problem were known in the cases of $\mathrm{SU}(2,1;\mathbb{Z}[\imath])$ and $\mathrm{SU}\left(2,1;\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]\right)$; in the first case two proofs were known and in the second one; see [FL03] and [Yas05] ($\mathbb{Z}[\imath]$) and [FP06] ($\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$). To the best of the author's knowledge no computational work had been carried out in the field. In all of these works fundamental domains are computed for their respective groups and not just Siegel sets. The paper [FP06] is a very elegant piece of mathematics that makes explicit use of the special geometry inherited from the sixth roots of unity in the ring of integers, the authors compute a fundamental domain without going via a Siegel set, however due to this the proof it is not clear that their proof can be generalised to other groups or dimensions. In contrast [FL03] and [Yas05] adopt a more traditional approach, first computing a Siegel set and then using this to compute a fundamental domain; in fact under a change of basis the computation of a Siegel set in [FL03] for $\mathrm{SU}(2,1;\mathbb{Z}[\imath])$ generalises immediately to the computation of a Siegel set for $\mathrm{SU}\left(2,1;\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]\right)$.

This thesis builds primarily on [FL05] which considers the construction of a Siegel set for $\mathrm{SU}(2,1;\mathbb{Z}[\imath])$ and was the precursor to [FL03] (the date order is explained by the fact that [FL03] is a pre-print, whereas [FL05] is a published paper). There are two key modifications that need to be made to this paper in order to generalise the method to all fields with trivial class group in all dimensions:

1. The basis needs to be changed so that all groups can be represented.
2. The method needs to be adapted to deal with the action of more than one automorphism. This is achieved in this thesis by the introduction of the effect function.

The paper [FL05] does not use cusps to proxy the height changing properties of automorphisms, but instead uses the actual automorphisms themselves; whilst this creates no problems in the case that they work in, in the general case computing automorphisms is an expensive task which is considerably more complicated than constructing cusps alone. And in general it is not necessary to work with automorphisms as is shown in [Yas05] where the author develops a method for computing fundamental domains and calculating cohomology by using only cusps and never considering the actual automorphisms themselves; this method starts from the position of knowing a Siegel set for the group action along with a set of cusps which generates this Siegel set; although no theory of Siegel set or cusp construction is discussed in [Yas05].

As such this thesis sits somewhere in between [FL05] and [Yas05]. Firstly [FL05] lay the building blocks for Siegel set construction with one explicit example and [Yas05] describes how to construct a fundamental domain given a Siegel set and a set of candidate cusps which generate it. This thesis bridges the gap by developing a computational method for constructing Siegel sets along with a set of candidate cusps which generate this set.

2.2 Results obtained

The following results were obtained from a C++ application called `siegel` which implements an algorithm based on Algorithm 5.10.1. Let $\mathbb{Q}\left(\sqrt{d}\right)$ be an imaginary quadratic number field and write $\mathfrak{O}$ for the ring of integers of $\mathbb{Q}\left(\sqrt{d}\right)$, denote the set of cusps that generate a Siegel set as Q, then the following sets are Seigel

sets for Γ:

$$S_\infty = \left\{ \underline{\mathbf{v}} \in \overline{\mathbb{H}^n_{\mathbb{C}}} \;\middle|\; \left|\Re \underline{z}_i\right| \leq \frac{1}{2},\ 0 \leq \Im \underline{z}_i \leq \frac{\sqrt{-d}}{4},\ |x| \leq \frac{\sqrt{-d}}{2},\ \mathrm{h}(\underline{\mathbf{v}}) \geq h \right\}$$

when $d \equiv 1 \mod 4$;

$$S_\infty = \left\{ \underline{\mathbf{v}} \in \overline{\mathbb{H}^2_{\mathbb{C}}} \;\middle|\; |\Re \underline{z}| \leq 1,\ 0 \leq \Im \underline{z} \leq \frac{\sqrt{-d}}{2},\ |x| \leq \frac{\sqrt{-d}}{2},\ \mathrm{h}(\underline{\mathbf{v}}) \geq h \right\}$$

when $d \not\equiv 1 \mod 4$ and $n = 2$;

$$S_\infty = \left\{ \underline{\mathbf{v}} \in \overline{\mathbb{H}^3_{\mathbb{C}}} \;\middle|\; \left|\Re \underline{z}_1\right| \leq 1,\ \left|\Re \underline{z}_2\right| \leq \frac{1}{2}\ (i \neq 1),\ \left|\Im \underline{z}_i\right| \leq \frac{\sqrt{-d}}{2},\ |x| \leq \frac{\sqrt{-d}}{2},\ \mathrm{h}(\underline{\mathbf{v}}) \geq h \right\}$$

when $d \not\equiv 1 \mod 4$ and $n = 3$

Dimension $n = 2$:

$d = -1$	$h = 0.999978433493$	$\lvert Q \rvert \leq 23$
$d = -2$	$h = 0.499996205477$	$\lvert Q \rvert \leq 181$
$d = -3$	$h = 0.999992068197$	$\lvert Q \rvert \leq 17$
$d = -7$	$h = 0.791053494930$	$\lvert Q \rvert \leq 27$
$d = -11$	$h = 0.331422584272$	$\lvert Q \rvert \leq 451$
$d = -19$	$h = 0.249830466184$	$\lvert Q \rvert \leq 827$
$d = -43$	$h = 0.113480677567$	$\lvert Q \rvert \leq 9253$
$d = -67$	$h = 0.074467903908$	$\lvert Q \rvert \leq 33466$
$d = -163$	$h = 0.009440545740$	$\lvert Q \rvert \leq 36096934$

Dimension $n = 3$:

$d = -1$	$h = 0.987391129157$	$\lvert Q \rvert \leq 108$
$d = -2$	$h = 0.577540291822$	$\lvert Q \rvert \leq 2258$
$d = -3$	$h = 0.999085879138$	$\lvert Q \rvert \leq 47$
$d = -7$	$h = 0.493756821420$	$\lvert Q \rvert \leq 1601$
$d = -11$	$h = 0.536411563086$	$\lvert Q \rvert \leq 773$
$d = -19$	$h = 0.196138009090$	$\lvert Q \rvert \leq 104813$
$d = -43$	$h = 0.059149067053$	$\lvert Q \rvert \leq 46224490$
$d = -67$	$h = 0.010418787475$	
$d = -163$	$h = 0.000040212980$	

2.3 Outline of the Thesis

Chapter 3 follows [Gol99], Section 3.1 introduces complex hyperbolic n-space as the space of negative lines in $\mathbb{P}^n_{\mathbb{C}}$ with respect to an Hermitian form of signature $(n,1)$ and the group of automorphisms of this space is $\mathrm{PU}(n,1)$ although the group $\mathrm{SU}(n,1;\mathbb{C})$ can be considered in its place; the ball model is then shown to be equivalent to this definition and is also shown to be a valid model for the symmetric space and; the paraboloid model is shown to be isomorphic to the ball model and thus also a valid model via the Cayley transform. In Section 3.2 a change is made from the standard basis in order to ease computation later on and notation for describing points in the space is set up. Section 3.3 decomposes the stabilizer of infinity in $\mathrm{SU}(n,1;\mathbb{C})$ into the semidirect product of a translation group and a rotation-dilation group, it describes what this decomposition looks like under restriction to certain subrings of $\mathbb{C}$; amongst these subrings are imaginary quadratic fields and the rings of integers of such fields. The chapter concludes in Section 3.4 with another structural result, giving the Brûhat decomposition of $\mathrm{SU}(n,1;\mathbb{C})$ under restriction to certain subfields of $\mathbb{C}$ including imaginary quadratic fields.

Chapter 4 develops the theoretical tools required to algorithmically construct Siegel sets for the action of $\Gamma = \mathrm{SU}(n,1;\mathfrak{O})$ on $\mathbb{H}^n_{\mathbb{C}}$ where $\mathfrak{O}$ is the ring of integers of an imaginary quadratic field K with trivial class group. Section 4.1 introduces objects called cusps Definition 4.1.1; through a deep result of Zink [Zin79] it is shown that when the class group of K is trivial then the cusps define a family of functions which perfectly proxy the height changing properties of the automorphisms in Γ; the effect function of a cusp at a point in $\mathbb{H}^n_{\mathbb{C}}$ is introduced Definition 4.1.8, it determines whether or not a point is raised by the action of a particular cusp and is one of the main tools used throughout the rest of this thesis. One of the key properties of the effect function is that it is convex under the standard Euclidean metric, this is proved in Proposition 4.1.9. Section 4.2 introduces the Siegel container as a Siegel set for Γ_∞; the importance of Siegel containers in Siegel set construction is given by Proposition 4.2.2 which states "*Let* $\mathrm{S}_\infty \subset \mathbb{H}^n_{\mathbb{C}}$ *be a Siegel container for* Γ*, let* $L > 0$*, and suppose that for all* $\underline{\mathbf{v}} \in \mathbb{H}^n_{\mathbb{C}}$ *there exists an automorphism* $\gamma \in \Gamma$ *such that* $\gamma \circ \underline{\mathbf{v}} \in \mathrm{S}_\infty(L)$*. Then* $\mathrm{S}_\infty \cap \left\{\underline{\mathbf{v}} \in \overline{\mathbb{H}^n_{\mathbb{C}}} \mid \text{height of } \underline{\mathbf{v}} \geq L\right\}$ *is a Siegel set for* Γ." In Lemma 4.2.6 an analytic formula for writing down a Siegel container depending only on the imaginary quadratic field and the dimension of the space is given. With an explicit formula for Siegel containers, in Section 4.3 attention is turned to the part of Proposition 4.2.2 which describes how to turn Siegel containers into Siegel sets, the first key result is Lemma 4.3.2 which describes how to verify that a set of cusps generates a Siegel set. A new function called the Phi function is introduced Definition 4.3.3 and this function is used in Lemma 4.3.5 to reinterpret Lemma 4.3.2 in a form which asks not just if a set of cusps generates a Siegel set, but determines the lower height bound of the Siegel set generated given a set of cusps. Up until this stage questions have been asked from the point of view of being able to operate without restriction on a continuous space, however of course computation is only possible in a discrete approximation of a continuous space and as such Section 4.4 investigates how to extend these continuous results to a discretised approximation; Corollary 4.4.4 extends Lemma 4.3.5 from a continuous space, to a space discretised into the union of convex polytopes and this now provides a practical method of algorithmically computing a Siegel set; in addition a strategy for bounding the error in discretisation is presented in Lemma 4.4.7. Having worked out in theory how to construct a Siegel set from a Siegel container in a discrete model given the existence of a set of cusps, it remains to consider how to construct the set of cusps. A cusp has an important invariant associated to it called its dilation factor; the dilation factor of a cusp is a strictly positive real number and the square of

a dilation factor is an integer; furthermore the smaller the dilation factor of a cusp the larger the region of effect is around that cusp in which the cusp can raise points in $\mathbb{H}^n_{\mathbb{C}}$. In Section 4.5 it is shown that the number of cusps of a fixed dilation factor which can raise the height of points in a compact region in $\mathbb{H}^n_{\mathbb{C}}$ is finite and two algorithms (Algorithm 4.5.5 and Algorithm 4.5.6) for constructing all cusps in such a region are described, in fact these algorithms construct many cusps which cannot raise any points in the region of interest into the bargain, but this is theoretically unimportant; the choice of algorithm depends solely on the congruence class of the generator of the field. The final section in the chapter pulls all of these ideas together into a single algorithm, Algorithm 4.6.2, which takes as input; a dimension, a Heegner number and an error tolerance and returns a Siegel set for the group determined by these parameters, the Siegel set lies within an error bound based on the error tolerance; this algorithm is shown in Proposition 4.6.3 to be guaranteed to terminate.

Chapter 5 considers improvements that can be made to Algorithm 4.6.2 to make it practical for implementation. In Section 5.1 Lemma 5.1.2 and Lemma 5.1.3 improve on the Siegel container computed in Lemma 4.2.6 by considering the action of rotational automorphisms in the integral stabilizer subgroups; in all but two cases the measure of the Siegel container is considerably decreased; a smaller Siegel container means a smaller space to discretise and as such either greater speed or higher accuracy. In Section 5.2 it is shown that there are two types of cusp; primitive and non-primitive and; for any non-primitive cusp, there is a primitive cusp which is at least as good at raising the height of all points in $\mathbb{H}^n_{\mathbb{C}}$ than the non-primitive one, Corollary 5.2.3. As such non-primitive cusps play no part in the construction of Siegel sets and as such they do not need to be output by a cusp generating algorithm; checking for primitivity is a simple operation which involves computing the K-norm of the coordinates of a cusp.

Due to the projective nature of $\mathbb{H}^n_{\mathbb{C}}$ cusps corresponding to the same line in $\mathbb{P}^n_{\mathbb{C}}$ have equivalent actions, Section 5.3 determines how to identify and remove all but one cusp from each equivalence class early on in the process of cusp construction.

The number of cusps generated by the original cusp algorithms is heavily influenced by bounds on the coordinates derived in Corollary 4.4.6, however these bounds are rather loose and lead to a large number of superfluous cusps being generated. Section 5.4 improves on these bounds by considering the coordinates on an individual basis; the difficulty in achieving these improvements is not mathematical but practical and comes primarily in the form of an algorithm for iterating through a lattice which changes during the process of iteration, Algorithm 5.4.8.

Removing non-primitive and equivalent cusps and improving the bounds on the cusp coordinates significantly reduces the number of superfluous cusps which are generated, however some percentage of the generated cusps will still not be able to raise any points in the Siegel container, Section 5.5 provides a method for removing all such cusps from the set of generated cusps, however this method involves performing a multidimensional minimisation which is an expensive computational operation, whereas all other cusp pruning operations are either inexpensive, or actually speed up construction time, and as such this should be considered as a final stage in the process of cusp generation.

Section 5.6 combines the ideas in Sections 5.2 - 5.5 to create an improved cusp generation algorithm. Section 5.7 considers an alternative way of discretising the search space compared to that described in Section 4.4; the first method of discretising is derived in order to provide definitive bounds on the error introduced due to discretisation, the second method is heuristic based and is designed to provide a compromise between speed and accuracy more appropriate to a practical implementation, however the definitive

error bounds are given up to achieve this compromise.

The computation time not spent constructing cusps is used almost exclusively to compute the Phi function on the discretised search space; Section 5.8 provides an algorithm for performing these calculations in an efficient way, 5.8.1. And since the Phi functions are determined at cusps then the order in which the cusps are chosen to compute Phi at is important; Section 5.9 discusses a strategy for ordering cusps so that they can be chosen in a way which is better than random. The final section in this chapter, Section 5.10 pulls all of these ideas together into a single algorithm, Algorithm 5.10.1, and it is shown that this algorithm is guaranteed to terminate and output a Siegel set.

Chapter 3

Preliminaries

3.1 Complex Hyperbolic Space

The definition of n-dimensional complex hyperbolic space, $\mathbb{H}^n_{\mathbb{C}}$, in this thesis follows [Gol99]: in [Gol99, 3.1] the space $\mathbb{H}^n_{\mathbb{C}}$ is defined to be the negative lines in $\mathbb{P}^n_{\mathbb{C}}$, the set of 1-dimensional complex linear subspaces through the origin in $\mathbb{C}^{n+1}$, with respect to an Hermitian form of signature $(n,1)$; also in [Gol99, 3.1] the ball model of complex hyperbolic space is shown to be equivalent to this projective definition and then; in [Gol99, 4.1] the paraboloid model, which is the most appropriate model from the point of view of computation and is the model used throughout this thesis, is shown to be equivalent to the ball model and as such the to original projective definition; this section reviews this theory.

The Projective Definition

This section follows [Gol99, 3.1]. Let

$$V = \begin{bmatrix} V' \\ V_{n+1} \end{bmatrix} \in \mathbb{C}^{n+1}$$

where $V' \in \mathbb{C}^n$ and $V_{n+1} \in \mathbb{C}$ and define the Hermitian pairing

$$\begin{aligned} \langle V, W \rangle &= \langle\langle V', W' \rangle\rangle - V_{n+1}\overline{W}_{n+1} \\ &= V_1\overline{W}_1 + \cdots + V_n\overline{W}_n - V_{n+1}\overline{W}_{n+1} \end{aligned} \tag{3.1}$$

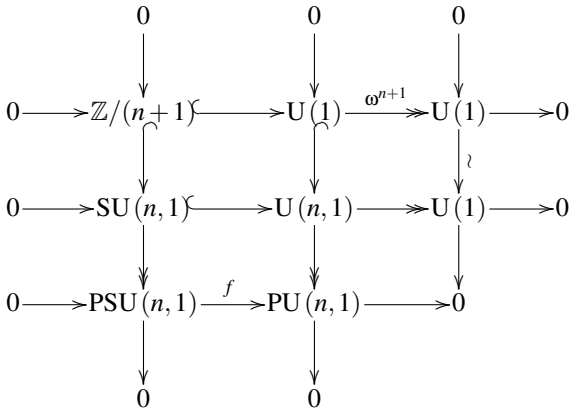
A vector V is said to be *negative (respectively null, positive)* if and only if the Hermitian inner product $\langle V, W \rangle$ is negative (respectively null, positive). *Complex hyperbolic n-space* $\mathbb{H}^n_{\mathbb{C}}$ is defined to be the subset of $\mathbb{P}^n_{\mathbb{C}}$ consisting of negative lines in $\mathbb{C}^{n+1}$. The *boundary* of $\mathbb{H}^n_{\mathbb{C}}$ is the subset $\partial\mathbb{H}^n_{\mathbb{C}}$ of $\mathbb{P}^n_{\mathbb{C}}$ consisting of null lines in $\mathbb{C}^{n+1}$.

Automorphisms

The image $\mathrm{PU}(n,1)$ of $\mathrm{U}(n,1)$ in $\mathrm{PGL}(\mathbb{C}^{n+1})$ is the full group of biholomorphisms of $\mathbb{H}^n_{\mathbb{C}}$, [Gol99, 3.1]. Recall that the projectivisation of a group is the quotient of a group by its centre:

$$\begin{aligned}\mathrm{PU}(n,1) &= \mathrm{U}(n,1)/Z(\mathrm{U}(n,1)) \\ &\simeq \mathrm{U}(n,1)/\mathrm{U}(1)\end{aligned}$$

The centre of $\mathrm{SU}(n,1)$ is isomorphic to $\mathbb{Z}/(n+1)$, the group of $(n+1)^{\text{th}}$ roots of unity. This gives a commutative diagram



where ω is some primitive n^{th} root of unity. Thus by the 9-lemma, the map f is a bijection;

$$\mathrm{PSU}(n,1) \xrightarrow{\sim} \mathrm{PU}(n,1)$$

and in particular

$$\mathrm{PU}(n,1) \simeq \mathrm{SU}(n,1)/\mathbb{Z}/(n+1)$$

So up to a finite group of rotations the groups $\mathrm{PU}(n,1)$ and $\mathrm{SU}(n,1)$ are isomorphic, and as such when studying the automorphisms of complex hyperbolic n-space, the group $\mathrm{SU}(n,1)$ may be studied instead.

The Ball Model

This section follows [Gol99, 3.1]. Let $\mathbb{C}^n$ be complex n-space with the standard positive definite Hermitian inner product

$$\langle\langle v,w\rangle\rangle = v_1\overline{w}_1 + \cdots + v_n\overline{w}_n$$

and let $\mathrm{U}(n)$ denote its group of unitary automorphisms. Complex hyperbolic space shall be identified with the unit ball

$$\mathbb{B}^n = \{z \in \mathbb{C}^n \mid \langle\langle v,w\rangle\rangle < 1\}$$

as follows. Let

$$\begin{array}{rcl} \mathbf{A}:\mathbb{C}^n & \longrightarrow & \mathbb{P}^n_{\mathbb{C}} \\ z' & \mapsto & \left[\begin{smallmatrix} z' \\ 1 \end{smallmatrix}\right] \end{array}$$

be the biholomorphic embedding of $\mathbb{C}^n$ onto the affine patch of $\mathbb{P}^n_{\mathbb{C}}$ defined by $Z_{n+1} \neq 0$ in homogeneous coordinates. Since any vector in $\mathbb{C}^{n+1}$ with homogeneous coordinate $Z_{n+1} = 0$ is positive, $\mathbb{H}^n_{\mathbb{C}} \subset \mathbf{A}(\mathbb{C}^n)$ and $\mathbf{A}$ identifies $\mathbb{B}^n$ with $\mathbb{H}^n_{\mathbb{C}}$ and $\partial\mathbb{B}^n = S^{2n-1} \subset \mathbb{C}^n$ with $\partial\mathbb{H}^n_{\mathbb{C}}$. The hyperplane at infinity $\mathbb{P}^n_{\mathbb{C}} - \mathbf{A}(\mathbb{C}^n)$ is the orthogonal complement $O^\perp$ where the vector

$$O = \left[\begin{smallmatrix} 0' \\ 1 \end{smallmatrix}\right] \in \mathbb{C}^{n+1}$$

corresponds to the origin in $\mathbb{C}^n$.

Lemma 3.1.1 *The stabilizer of O in $\mathrm{SU}(n,1;\mathbb{C})$ is isomorphic to the unitary group $\mathrm{U}(n)$ of $\mathbb{C}^n$.*

PROOF This can be seen easily by direct calculation. Let $g \in \mathrm{SU}(n,1;\mathbb{C})$ and suppose that $gO = O$. Write

$$g = \begin{pmatrix} U & v_1 \\ {v_2}^{\mathrm{t}} & u \end{pmatrix}$$

where $U \in \mathrm{M}_n(\mathbb{C})$, $v_i \in \mathbb{C}^n$ and $u \in \mathbb{C}$. The stability condition implies that $v_1 = 0'$ and the Hermitian stability condition $g^* \left(\begin{smallmatrix} I_n & \\ & -1 \end{smallmatrix}\right) g = \left(\begin{smallmatrix} I_n & \\ & -1 \end{smallmatrix}\right)$ implies that $v_2 = 0'$ whence

$$g = \left(\begin{smallmatrix} U & \\ & u \end{smallmatrix}\right)$$

Since $g \in \mathrm{SU}(n,1;\mathbb{C})$ then $1 = u \det U$ so $u = \det U^{-1}$ and hence u is completely determined by U. Again by the Hermitian stability condition it is necessary that $U \in \mathrm{U}(n)$ as U must stabilise the identity matrix, and since this implies that u is on the unit circle, then this condition is also sufficient. Therefore

$$\begin{array}{rcl} \mathrm{U}(n) & \longleftrightarrow & \mathrm{SU}(n,1;\mathbb{C})_O \\ U & & \left(\begin{smallmatrix} U & \\ & \det U^{-1} \end{smallmatrix}\right) \end{array}$$

is an isomorphism. ∎

Lemma 3.1.2 $\mathrm{SU}(n,1;\mathbb{C})$ *acts transitively on the set $\mathbb{H}^n_{\mathbb{C}}$ of negative lines in $\mathbb{C}^{n+1}$.*

PROOF See [Gol99, Lemma 3.1.3] ∎

The Paraboloid Model

This section follows [Gol99, 4.1]. The paraboloid model arises from viewing $\mathbb{H}^n_{\mathbb{C}}$ from a point $\mathbf{q}_\infty$ on the boundary, it generalises the upper half-plane model of $\mathbb{H}^1_{\mathbb{C}}$. The unit ball is symmetric under the stabilizer $\mathrm{U}(n)$ of the origin, the paraboloid model is invariant under the stabilizer of $\mathbf{q}_\infty$.

Choose a point $\mathbf{q} \in \partial\mathbb{H}^n_{\mathbb{C}}$; such a point corresponds to a null line spanned by a null vector $Q \in \mathbb{C}^{n+1}$. A unique $\mathbb{C}$-hyperplane $H(\mathbf{q})$ is tangent to $\partial\mathbb{H}^n_{\mathbb{C}}$ at $\mathbf{q}$; it corresponds to the linear hyperplane $Q^\perp \subset \mathbb{C}^{n+1}$ which is orthogonal to Q with respect to the Hermitian form defined in (3.1). The affine patch on $\mathbb{P}^n_{\mathbb{C}}$ complementary to $H(\mathbf{q})$ contains $\mathbb{H}^n_{\mathbb{C}}$ as an unbounded domain and this embedding is denoted $\mathbf{B}:\mathbb{H}^n_{\mathbb{C}} \to$

$\mathbb{P}^n_{\mathbb{C}} - H(\mathbf{q})$. Specifically let Q be the vector $\mathbf{q}_\infty = \begin{bmatrix} -1 \\ 0' \\ 1 \end{bmatrix} \in \mathbb{C}^{n+1}$ whence $H(\mathbf{q}_\infty)$ consists of all points having homogeneous coordinates $\begin{bmatrix} z_n \\ z' \\ -z_n \end{bmatrix}$. The map

$$\begin{array}{rcl} \mathbf{B} : \mathbb{H}^n_{\mathbb{C}} & \to & \mathbb{P}^n_{\mathbb{C}} - H(\mathbf{q}) \\ \begin{pmatrix} \mathbf{v}' \\ \mathbf{v}_n \end{pmatrix} & \mapsto & \begin{bmatrix} 1/2 - \mathbf{v}_n \\ \mathbf{v}' \\ 1/2 + \mathbf{v}_n \end{bmatrix} \end{array}$$

is the desired affine embedding; $\mathbb{H}^n_{\mathbb{C}}$ corresponds to the Siegel domain $\mathfrak{H}^n$, referred to here as the paraboloid model, consisting of points $\mathbf{v} \in \mathbb{C}^n$ satisfying

$$2\Re(\mathbf{v}_n) - \langle\langle \mathbf{v}', \mathbf{v}' \rangle\rangle > 0$$

The two sets of inhomogeneous (affine) coordinates in the paraboloid and ball models respectively are related by the *Cayley transform*:

$$\begin{array}{ccccc} & z \in \mathbb{B}^n & \longleftrightarrow & \mathbf{v} \in \mathfrak{H}^n & \\ z_j & = \frac{2\mathbf{v}_j}{1+2w_n} & & \mathbf{v}_j & = \frac{z_j}{1+z_n} \quad (1 \le j < n) \\ z_n & = \frac{1-2\mathbf{v}_n}{1+2w_n} & & \mathbf{v}_n & = \frac{1}{2}\frac{1-z_n}{1+z_n} \end{array}$$

Under the Cayley transform the boundary $\partial\mathfrak{H}^n$ corresponds to the real hypersurface

$$\partial\mathfrak{H}^n = \left\{ \mathbf{v} \in \mathbb{C}^n \mid 2\Re(\mathbf{v}_n) - \langle\langle \mathbf{v}', \mathbf{v}' \rangle\rangle = 0 \right\}$$

together with the ideal point $\mathbf{q}_\infty$.

3.2 A Change of Basis

Goldman defines $\mathbb{H}^n_{\mathbb{C}}$ with respect to the Hermitian form $\langle V, W \rangle = \langle\langle V', W' \rangle\rangle - V_{n+1}\overline{W}_{n+1}$, which is represented by the standard Hermitian matrix of signature $(n,1)$; this being $H' = \begin{pmatrix} I_n & \\ & -1 \end{pmatrix}$. However for computational reasons it is preferable to make a change of basis. The unitary matrix

$$U = \begin{pmatrix} 1/\sqrt{2} & & 1/\sqrt{2} \\ & I_{n-1} & \\ 1/\sqrt{2} & & -1/\sqrt{2} \end{pmatrix}$$

acts on H' by Hermitian conjugation and induces a basis change:

$$U^* H' U = \begin{pmatrix} & & 1 \\ & I_{n-1} & \\ 1 & & \end{pmatrix} = H$$

with respect to this new basis matrix the ideal point $\mathbf{q}_\infty$ becomes

$$\mathbf{q}_\infty = U \begin{bmatrix} -1 \\ 0' \\ 1 \end{bmatrix} = \begin{bmatrix} 0' \\ \frac{1}{2\sqrt{2}} \end{bmatrix}$$

and the non-ideal points in $\mathbb{H}^n_{\mathbb{C}}$ become

$$\underline{\mathbf{v}} = U \begin{bmatrix} 1/2-\mathbf{v}_n \\ \mathbf{v}' \\ 1/2+\mathbf{v}_n \end{bmatrix} = \begin{bmatrix} \frac{1}{2\sqrt{2}} \\ \mathbf{v}' \\ \frac{-\mathbf{v}_n}{2\sqrt{2}} \end{bmatrix}$$

Furthermore, since these points are representatives of lines in $\mathbb{C}^{n+1}$, it makes sense to normalise to remove the factor of $\frac{1}{2\sqrt{2}}$ in the constant coordinates; whence these points may be written equivalently as

$$\mathbf{q}_\infty = \begin{bmatrix} 0' \\ 1 \end{bmatrix} \qquad\qquad \underline{\mathbf{v}} = \begin{bmatrix} 1 \\ 2\sqrt{2}\mathbf{v}' \\ -\mathbf{v}_n \end{bmatrix} = \begin{bmatrix} 1 \\ \tilde{\mathbf{v}}' \\ \tilde{\mathbf{v}}_n \end{bmatrix}$$

where $\tilde{\mathbf{v}}' = 2\sqrt{2}\mathbf{v}'$ and $\tilde{\mathbf{v}}_n = -\mathbf{v}_n$. Therefore the isomorphism between points under the original basis and the new basis is

$$\begin{array}{ccc} \mathbf{w} = \begin{bmatrix} 1/2-\mathbf{w}_n \\ \mathbf{w}' \\ 1/2+\mathbf{w}_n \end{bmatrix} \in \mathfrak{H}^n(H') & \longleftrightarrow & \mathbf{v} = \begin{bmatrix} 1 \\ \mathbf{v}' \\ \mathbf{v}_n \end{bmatrix} \in \mathfrak{H}^n(H) \\ \mathbf{w} = \begin{bmatrix} \frac{1-\mathbf{v}_n}{2} \\ \frac{\mathbf{v}'}{\sqrt{2}} \\ \frac{1+\mathbf{v}_n}{2} \end{bmatrix} & & \mathbf{v} = \begin{bmatrix} 1 \\ 2\sqrt{2}\mathbf{w}' \\ -\mathbf{w}_n \end{bmatrix} \end{array}$$

The new basis matrix H induces Hermitian and quadratic forms on $\mathbb{C}^{n+1} \times \mathbb{C}^{n+1}$ and $\mathbb{C}^{n+1}$ by:

$$\begin{array}{rcl} \langle -,- \rangle : \mathbb{C}^{n+1} \times \mathbb{C}^{n+1} & \longrightarrow & \mathbb{C} \\ (\underline{\mathbf{v}}, \underline{\mathbf{w}}) & \longmapsto & \underline{\mathbf{w}}^* H \underline{\mathbf{v}} \end{array} \qquad \begin{array}{rcl} \mathrm{Q} : \mathbb{C}^{n+1} & \longrightarrow & \mathbb{C} \\ \underline{\mathbf{v}} & \longmapsto & \underline{\mathbf{v}}^* H \underline{\mathbf{v}} \end{array}$$

and the identity matrix I_{n-1} defines an Hermitian form on $\mathbb{C}^{n-1} \times \mathbb{C}^{n-1}$ and a positive definite quadratic form on $\mathbb{C}^{n-1}$:

$$\begin{array}{rcl} \langle -,- \rangle_+ : \mathbb{C}^{n+1} \times \mathbb{C}^{n+1} & \longrightarrow & \mathbb{C} \\ (\underline{\mathbf{v}}, \underline{\mathbf{w}}) & \longmapsto & \underline{\mathbf{w}}^* H \underline{\mathbf{v}} \end{array} \qquad \begin{array}{rcl} \mathrm{Q}_+ : \mathbb{C}^{n+1} & \longrightarrow & \mathbb{C} \\ \underline{\mathbf{v}} & \longmapsto & \underline{\mathbf{v}}^* H \underline{\mathbf{v}} \end{array}$$

It is necessary and sufficient that a point $\underline{\mathbf{v}} \in \mathbb{H}^n_{\mathbb{C}}$ satisfies $\mathrm{Q}(\underline{\mathbf{v}}) < 0$ and $\underline{\mathbf{v}} \in \partial\mathbb{H}^n_{\mathbb{C}}$ satisfies $\mathrm{Q}(\underline{\mathbf{v}}) = 0$ and thus this leads to the following definition.

Definition 3.2.1 (The Paraboloid Model) *Let $n \in \mathbb{N}$ such that $n \geq 2$. Then the paraboloid model of n-dimensional complex hyperbolic space is*

$$\mathbb{H}^n_{\mathbb{C}} = \left\{ \begin{pmatrix} 1 \\ \underline{z} \\ \frac{-\mathrm{Q}_+(\underline{z})-h}{2} + \imath x \end{pmatrix} \;\middle|\; \underline{z} \in \mathbb{C}^{n-1},\ x \in \mathbb{R} \text{ and } h \in \mathbb{R}^{>0} \right\}$$

$$\partial\mathbb{H}^n_{\mathbb{C}} = \left\{ \begin{pmatrix} 1 \\ \underline{z} \\ \frac{-\mathrm{Q}_+(\underline{z})}{2} + \imath x \end{pmatrix} \;\middle|\; \underline{z} \in \mathbb{C}^{n-1} \text{ and } x \in \mathbb{R} \right\} \cup \left\{ \begin{pmatrix} 0 \\ \underline{0} \\ 1 \end{pmatrix} \right\}$$

where the point $\begin{pmatrix} 0 \\ \underline{0} \\ 1 \end{pmatrix}$ is the point at infinity and is denoted $\mathbf{q}_\infty$. The following notation shall be used: $\overline{\mathbb{H}^n_{\mathbb{C}}} = \mathbb{H}^n_{\mathbb{C}} \cup \partial\mathbb{H}^n_{\mathbb{C}}$, $\partial\mathbb{H}^{n\,\times}_{\mathbb{C}} = \partial\mathbb{H}^n_{\mathbb{C}} - \{\mathbf{q}_\infty\}$ and $\overline{\mathbb{H}^{n\,\times}_{\mathbb{C}}} = \overline{\mathbb{H}^n_{\mathbb{C}}} - \{\mathbf{q}_\infty\}$. □

Let $\underline{\mathbf{v}} \in \overline{\mathbb{H}^n_{\mathbb{C}}}^{\times}$, write $\underline{\mathbf{v}} = \begin{pmatrix} 1 & v_1 & \cdots & v_n \end{pmatrix}^{\mathrm{t}}$ put $\underline{z} = \begin{pmatrix} v_1 & \cdots & v_{n-1} \end{pmatrix}^{\mathrm{t}}$ and define the function;

$$\begin{array}{rcl} f : \overline{\mathbb{H}^n_{\mathbb{C}}}^{\times} & \longrightarrow & \mathbb{C}^{n-1} \times \mathbb{R} \times \mathbb{R}^{\geq 0} \\ \underline{\mathbf{v}} & \longmapsto & (\underline{z}, \Im v_n, -\mathrm{Q}(\underline{\mathbf{v}})) \end{array}$$

Since $\mathrm{Q}(\underline{\mathbf{v}}) = 2\Re(v_n) + \mathrm{Q}_+(\underline{z})$, it follows that f is an isomorphism and this leads to the definition of the horospherical model of complex hyperbolic space.

Definition 3.2.2 (Horospherical Model) *Let $n \in \mathbb{N}$ such that $n \geq 2$. Then the horospherical model of n-dimensional complex hyperbolic space is*

$$\begin{aligned} \mathbb{H}^n_{\mathbb{C}} &= \left\{ (\underline{z}, x, h) \mid \underline{z} \in \mathbb{C}^{n-1},\ x \in \mathbb{R} \text{ and } h \in \mathbb{R}^{>0} \right\} \\ \partial\mathbb{H}^n_{\mathbb{C}} &= \left\{ (\underline{z}, x, 0) \mid \underline{z} \in \mathbb{C}^{n-1} \text{ and } x \in \mathbb{R} \right\} \cup \{\infty\} \end{aligned}$$ □

Horospherical coordinates are notationally more compact than paraboloid coordinates, however explicit calculations must, in general, be carried out in paraboloid coordinates.

Definition 3.2.3 (Hyperbolic Notation) *Unless explicitly stated, all points in $\overline{\mathbb{H}^n_{\mathbb{C}}}^{\times}$ shall be denoted $\underline{\mathbf{v}}$ and if further points are required they shall be denoted $\underline{\mathbf{v}}', \underline{\mathbf{v}}'', \ldots$ etceteras. Given points $\underline{\mathbf{v}}, \underline{\mathbf{v}}', \ldots \in \overline{\mathbb{H}^n_{\mathbb{C}}}^{\times}$ the paraboloid vector forms of $\underline{\mathbf{v}}, \underline{\mathbf{v}}', \ldots$ will always be written as*

$$\underline{\mathbf{v}} = \begin{pmatrix} 1 \\ \underline{z} \\ \frac{-\mathrm{Q}_+(\underline{z}) - h}{2} + \imath x \end{pmatrix} \qquad \underline{\mathbf{v}}' = \begin{pmatrix} 1 \\ \underline{z}' \\ \frac{-\mathrm{Q}_+(\underline{z}') - h'}{2} + \imath x' \end{pmatrix} \qquad \cdots$$

and the horospherical tuple forms of $\underline{\mathbf{v}}, \underline{\mathbf{v}}', \ldots$ will always be written as $\underline{\mathbf{v}} = (\underline{z}, x, h)$, $\underline{\mathbf{v}}' = (\underline{z}', x', h'), \ldots$. Under these equivalent coordinate systems the complex vector $\underline{z} \in \mathbb{C}^{n-1}$ is called the complex component of $\underline{\mathbf{v}}$, the $x \in \mathbb{R}$ coordinate is called the real component of $\underline{\mathbf{v}}$, the pair $(\underline{z}, x) \in \mathbb{C}^{n-1} \times \mathbb{R}$ is called the Heisenberg component of $\underline{\mathbf{v}}$ and the $h \in \mathbb{R}^{\geq 0}$ coordinate is called the height component of $\underline{\mathbf{v}}$. The complex component can be thought of as being an element in a $n-1$ dimensional complex space, or a $2n-2$ dimensional real space. The Heisenberg component can be thought of as being an element in the space $\mathbb{C}^{n-1} \times \mathbb{R}$, or an element in a $2n-1$ dimensional real space. □

This section concludes with a proof that with respect to the Hermitian pairing, complex hyperbolic n-space has no orthogonal subspaces.

Lemma 3.2.4 *Let $\underline{\mathbf{v}} \in \overline{\mathbb{H}^n_{\mathbb{C}}}$ and let $X = \left\{ \underline{\mathbf{v}}' \in \overline{\mathbb{H}^n_{\mathbb{C}}} \mid \langle \underline{\mathbf{v}}, \underline{\mathbf{v}}' \rangle = 0 \right\}$. Then either $X = \emptyset$, or $\underline{\mathbf{v}} \in \partial\mathbb{H}^n_{\mathbb{C}}$ and $X = \{\underline{\mathbf{v}}\}$.*

PROOF Let $\underline{\mathbf{v}}, \underline{\mathbf{v}}' \in \overline{\mathbb{H}^n_{\mathbb{C}}}^{\times}$, then

$$\begin{aligned} 2\left\langle \underline{\mathbf{v}}, \underline{\mathbf{v}}' \right\rangle &= 2 \begin{pmatrix} 1 & \underline{z}' & \frac{-\mathrm{Q}_+(\underline{z}') - h'}{2} - \imath x' \end{pmatrix} H \begin{pmatrix} 1 \\ \underline{z} \\ \frac{-\mathrm{Q}_+(\underline{z}) - h}{2} + \imath x \end{pmatrix} \\ &= 2\left\langle \underline{z}, \underline{z}' \right\rangle_+ - \mathrm{Q}_+(\underline{z}) - \mathrm{Q}_+(\underline{z}') - h - h' + 2\imath\left(x - x'\right) \\ &= 2\Re\left\langle \underline{z}, \underline{z}' \right\rangle_+ - \left\langle \underline{z}, \underline{z} \right\rangle_+ - \left\langle \underline{z}', \underline{z}' \right\rangle_+ - h - h' + 2\imath\left(\Im\left\langle \underline{z}, \underline{z}' \right\rangle_+ + x - x'\right) \\ &= \left\langle \underline{z}, \underline{z}' \right\rangle_+ + \overline{\left\langle \underline{z}, \underline{z}' \right\rangle_+} - \left\langle \underline{z}, \underline{z} \right\rangle_+ - \left\langle \underline{z}', \underline{z}' \right\rangle_+ - h - h' + 2\imath\left(\Im\left\langle \underline{z}, \underline{z}' \right\rangle_+ + x - x'\right) \\ &= -\left\langle \underline{z} - \underline{z}', \underline{z} - \underline{z}' \right\rangle_+ - h - h' + 2\imath\left(\Im\left\langle \underline{z}, \underline{z}' \right\rangle_+ + x - x'\right) \end{aligned}$$

$$= -\mathrm{Q}_+\left(\underline{z}-\underline{z}'\right) - h - h' + 2\imath\left(\Im\left\langle \underline{z},\underline{z}'\right\rangle_+ + x - x'\right)$$

Suppose that $\langle \underline{\mathbf{v}}, \underline{\mathbf{v}}'\rangle = 0$, so both $\Re\langle \underline{\mathbf{v}}, \underline{\mathbf{v}}'\rangle = 0$ and $\Im\langle \underline{\mathbf{v}}, \underline{\mathbf{v}}'\rangle = 0$. Considering the real part; $0 = 2\Re\langle \underline{\mathbf{v}}, \underline{\mathbf{v}}'\rangle = -\mathrm{Q}_+(\underline{z}-\underline{z}') - h - h'$, the quadratic form $\mathrm{Q}_+(-)$ is positive definite and $h, h' \geq 0$, so $\mathrm{Q}_+(\underline{z}-\underline{z}'), h, h' = 0$ and $\underline{z} = \underline{z}'$, thus both $\underline{\mathbf{v}}$ and $\underline{\mathbf{v}}'$ are on the boundary. Considering the imaginary part; $0 = \Im\langle \underline{\mathbf{v}}, \underline{\mathbf{v}}'\rangle = \Im\langle \underline{z}, \underline{z}'\rangle_+ + x - x'$, now $\underline{z} = \underline{z}'$, so $\langle \underline{z}, \underline{z}'\rangle_+ \in \mathbb{R}$ whence $\Im\langle \underline{z}, \underline{z}'\rangle_+ = 0$ and so $x = x'$. But then $\underline{\mathbf{v}} = \underline{\mathbf{v}}'$ and $\underline{\mathbf{v}} \in \partial\mathbb{H}^n_{\mathbb{C}}$. If $\underline{\mathbf{v}} = \mathbf{q}_\infty$ then it can be seen by inspection that $\langle \mathbf{q}_\infty, \underline{\mathbf{v}}'\rangle = 1$. ■

3.3 The Stabiliser of Infinity

This section recalls the structure of the parabolic subgroup $\mathrm{SU}(n,1;\mathbb{C})_\infty$; elements which stabilise infinity are called parabolic. There are four important subgroups inside $\mathrm{SU}(n,1;\mathbb{C})_\infty$; the translation, rotation, dilation and AM-subgroups, the AM-subgroup being a direct product of the rotation and dilation subgroups; of these the translation and AM-subgroups have natural restrictions to coordinates which lie in subrings of $\mathbb{C}$ and these restrictions determine the Langlands decomposition of $\mathrm{SU}(n,1;\mathbb{C})_\infty$ under the same restriction.

Let R be a subring of $\mathbb{C}$, then

$$\mathrm{SU}(n,1;R)_\infty = \{g \in \mathrm{SU}(n,1;R) \mid g \circ \mathbf{q}_\infty = \mathbf{q}_\infty\}$$

Contained within $\mathrm{SU}(n,1;\mathbb{C})_\infty$ are the following subgroups:

Definition 3.3.1 (Heisenberg Translation Group)

$$\mathrm{N}(R) = \left\{ \begin{pmatrix} 1 & & \\ \zeta & I_{n-1} & \\ -\frac{\mathrm{Q}(\zeta)}{2} + \imath r & -\zeta^* & 1 \end{pmatrix} \in \mathrm{SL}_{n+1}(R) \;\middle|\; \zeta \in R^{n-1},\ r \in \mathbb{R} \right\}$$

Elements of $\mathrm{N}(R)$ *are denoted* $\mathrm{v}(\zeta, r)$. □

Definition 3.3.2 (Heisenberg Rotation Group)

$$\mathrm{M} = \left\{ \begin{pmatrix} \beta & & \\ & u & \\ & & \beta \end{pmatrix} \in \mathrm{SL}_{n+1}(\mathbb{C}) \;\middle|\; u \in \mathrm{U}(n-1;\mathbb{C}),\ \beta \in \mathbb{C} \right\}$$

Elements of M *are denoted* $m(u,\beta)$. □

Definition 3.3.3 (Heisenberg Dilation Group)

$$\mathrm{A} = \left\{ \begin{pmatrix} \delta & & \\ & I_{n+1} & \\ & & \delta^{-1} \end{pmatrix} \in \mathrm{SL}_{n+1}(\mathbb{R}) \;\middle|\; \delta \in \mathbb{R}^{>0} \right\}$$

Elements of A *are denoted* $a(\delta)$. □

Definition 3.3.4 (Heisenberg AM-Group)

$$\mathrm{AM}(R) = \{a(\delta)m(u,\beta) \in \mathrm{SL}_{n+1}(R) \mid a(\delta) \in \mathrm{A},\ m(u,\beta) \in \mathrm{M}\}$$

Elements of AM *are denoted* $am(\delta,u,\beta)$. □

Let $\underline{\mathbf{v}} \in \overline{\mathbb{H}^n_{\mathbb{C}}}^{\times}$, let $\nu(\zeta, r) \in \mathrm{N}(\mathbb{C})$, let $m(u,\beta) \in \mathrm{M}$ and let $a(\delta) \in \mathrm{A}$. Then it is seen by direct computation that

$$\nu(\zeta,r)\circ\underline{\mathbf{v}} = \begin{pmatrix} 1 \\ \underline{z}+\zeta \\ \frac{-\mathrm{Q}_+(\underline{z}+\zeta)}{2}+\imath\left(x+r-\Im\langle \underline{z},\zeta\rangle_+\right) \end{pmatrix}$$
$$m(u,\beta)\circ\underline{\mathbf{v}} = \begin{pmatrix} 1 \\ \beta^{-1}u\zeta \\ \frac{-\mathrm{Q}_+\left(\beta^{-1}u\zeta\right)}{2}+\imath x \end{pmatrix}$$
$$a(\delta)\circ\underline{\mathbf{v}} = \begin{pmatrix} 1 \\ \delta^{-1}\zeta \\ \frac{-\mathrm{Q}_+\left(\delta^{-1}\zeta\right)}{2}+\imath\delta^{-2}x \end{pmatrix}$$

Lemma 3.3.5 *Let $R \subseteq \mathbb{C}$ be a ring which is stable by complex conjugation, let $h \geq 0$. Then $\mathrm{N}(R)$ acts transitively on the set*

$$X = \left\{ \begin{pmatrix} 1 \\ \underline{z} \\ \frac{-\mathrm{Q}_+(\underline{z})-h}{2}+\imath x \end{pmatrix} \in \mathbb{C}^{n+1} \;\middle|\; \underline{z} \in R^{n-1} \text{ and } x \in \mathbb{R} \text{ s.t. } \frac{-\mathrm{Q}_+(\underline{z})}{2}+\imath x \in R \right\}$$

PROOF Let $\underline{\mathbf{v}}, \underline{\mathbf{v}}' \in X$. Since R is stable by complex conjugation then $\nu = \nu(-\underline{z}, -x) \in \mathrm{N}(R)$ and $\nu \circ \underline{\mathbf{v}} = (1\ \underline{0}\ 0)^{\mathrm{t}}$. Again, as R is stable by complex conjugation, $\nu' = \nu(\underline{z}', x') \in \mathrm{N}(R)$ and $\nu' \circ (1\ \underline{0}\ 0)^{\mathrm{t}} = \underline{\mathbf{v}}'$. Putting $\nu'' = \nu\nu'$, $\nu'' \circ \underline{\mathbf{v}} = \underline{\mathbf{v}}'$, and hence $\mathrm{N}(R)$ acts transitively on X. ∎

Lemma 3.3.6 *Let $R \subseteq \mathbb{C}$ be an integral domain which is stable by complex conjugation; typically R will be $\mathbb{C}$, $\mathbb{Q}\left(\sqrt{d}\right)$ where d is a negative squarefree integer or $\mathfrak{O}$ the ring of integers of $\mathbb{Q}\left(\sqrt{d}\right)$. Then the Langlands decomposition of the group $\mathrm{SU}(n,1;R)_\infty$ is*

$$\mathrm{SU}(n,1;R)_\infty = \mathrm{AM}(R) \ltimes \mathrm{N}(R)$$

Where

$$\mathrm{AM}(R) = \left\{ a(\delta,u,\beta) \mid \delta \in \mathbb{R}^{>0},\ u \in \mathrm{U}(n-1;R),\ \beta \in \mathbb{C} \text{ s.t. } \beta^2 = \det u^{-1},\ \delta\beta,\ \frac{\beta}{\delta} \in R \right\}$$
$$\mathrm{N}(R) = \left\{ \nu(\zeta,r) \mid \zeta \in R^{n-1},\ r \in \mathbb{R} \text{ s.t. } -\frac{\mathrm{Q}_+(\zeta)}{2}+\imath r \in R \right\}$$

PROOF Let $g \in \mathrm{AM}(R) \cup \mathrm{N}(R)$; in the $(n+1)^{\text{th}}$ column of g only the $g_{(n+1,n+1)}$ coordinate is non-zero, therefore $g\mathbf{q}_\infty = (0\ \underline{0}\ g_{(n+1,n+1)})^{\mathrm{t}}$ and $\mathrm{AM}(R)\mathrm{N}(R)$ is a subgroup of $\mathrm{SU}(n,1;R)_\infty$. To show that $\mathrm{SU}(n,1;R)_\infty$ is a subgroup of $\mathrm{AM}(R)\mathrm{N}(R)$ let $g \in \mathrm{SU}(n,1;R)_\infty$ and write:

$$g = \begin{pmatrix} z_1 & \zeta_3{}^{\mathrm{t}} & z_3 \\ \zeta_1 & u & \zeta_4 \\ z_4 & \zeta_2{}^{\mathrm{t}} & z_2 \end{pmatrix}$$

where $u \in \mathrm{GL}_{n-1}(R)$, $\zeta_i \in R^{n-1}$ and $z_i \in R$. The stability condition requires that

$$g\mathbf{q}_\infty = \begin{pmatrix} z_3 \\ \zeta_4 \\ z_2 \end{pmatrix} \sim \begin{pmatrix} 0 \\ \underline{0} \\ 1 \end{pmatrix}$$

thus $z_3 = 0$, $\zeta_4 = \underline{0}$ and $z_2 \neq 0$. Substituting these values back into g and using the Hermitian conjugacy

condition gives

$$\begin{aligned} H &= g^* H g \\ &= \begin{pmatrix} \overline{z_1} & \zeta_1^* & \overline{z_4} \\ \overline{\zeta_3} & u^* & \overline{\zeta_2} \\ & & \overline{z_2} \end{pmatrix} \begin{pmatrix} & & 1 \\ & I_{n-1} & \\ 1 & & \end{pmatrix} \begin{pmatrix} z_1 & {\zeta_3}^{\mathrm{t}} & \\ \zeta_1 & u & \\ z_4 & {\zeta_2}^{\mathrm{t}} & z_2 \end{pmatrix} \\ &= \begin{pmatrix} \overline{z_4} & \zeta_1^* & \overline{z_1} \\ \overline{\zeta_2} & u^* & \overline{\zeta_3} \\ \overline{z_2} & & \end{pmatrix} \begin{pmatrix} z_1 & {\zeta_3}^{\mathrm{t}} & \\ \zeta_1 & u & \\ z_4 & {\zeta_2}^{\mathrm{t}} & z_2 \end{pmatrix} \end{aligned} \tag{3.2}$$

Considering only multiplication by the bottom row of the lefthand matrix in (3.2)

$$\begin{aligned} \begin{pmatrix} 1 & \underline{0} & 0 \end{pmatrix} &= \begin{pmatrix} \overline{z_2} & \underline{0} & 0 \end{pmatrix} \begin{pmatrix} z_1 & {\zeta_3}^{\mathrm{t}} & \\ \zeta_1 & u & \\ \gamma & {\zeta_2}^{\mathrm{t}} & z_2 \end{pmatrix} \\ &= \begin{pmatrix} \overline{z_2} z_1 & \overline{z_2} {\zeta_3}^{\mathrm{t}} & 0 \end{pmatrix} \end{aligned}$$

so $\overline{z_2} z_1 = 1$ and $\zeta_3 = \underline{0}$. Therefore $\overline{z_2} = z_1^{-1}$ and (3.2) becomes

$$\begin{aligned} H &= \begin{pmatrix} \overline{z_4} & \zeta_1^* & \overline{z_1} \\ \overline{\zeta_2} & u^* & \\ z_1^{-1} & & \end{pmatrix} \begin{pmatrix} z_1 & & \\ \zeta_1 & u & \\ z_4 & {\zeta_2}^{\mathrm{t}} & \overline{z_1^{-1}} \end{pmatrix} \\ &= \begin{pmatrix} z_1\overline{z_4} + \mathrm{Q}_+(\zeta_1) + \overline{z_1} z_4 & \zeta_1^* u + \overline{z_1} {\zeta_2}^{\mathrm{t}} & 1 \\ z_1\overline{\zeta_2} + u^*\zeta_1 & u^* u & \\ 1 & & \end{pmatrix} \end{aligned}$$

And so,

$$u^* u = I_{n-1} \implies u \in \mathrm{U}(n-1, R)$$

$$z_1\overline{z_4} + \mathrm{Q}_+(\zeta_1) + \overline{z_1} z_4 = 0 \implies \Re \overline{z_1} z_4 = -\frac{\mathrm{Q}_+(\zeta_1)}{2} \tag{3.3}$$

$$z_1\overline{\zeta_2} + u^*\zeta_1 = \underline{0} \implies z_1\overline{\zeta_2} = -u^*\zeta_1 \tag{3.4}$$

$$\zeta_1^* u + \overline{z_1}{\zeta_2}^{\mathrm{t}} = 0 \implies \overline{z_1}{\zeta_2}^{\mathrm{t}} = -\zeta_1^* u \tag{3.5}$$

Taking the adjoint of (3.4)

$$(\overline{z_1}{\zeta_2}^{\mathrm{t}})^* = (-\zeta_1^* u)^* \implies z_1\overline{\zeta_2} = -u^*\zeta_1$$

shows that (3.5) and (3.4) are equivalent statements, so satisfying one automatically satisfies the other and ${\zeta_2}^{\mathrm{t}} = -\overline{z_1^{-1}}\zeta_1^* u$.

Let $\delta \in \mathbb{R}^{>0}$ and let $\beta \in \{z \in \mathbb{C} \mid |z| = 1\}$ be the the polar coordinates of z_1, so $z_1 = \delta\beta$, then (3.3) can be rewritten as $\delta \Re \frac{z_4}{\beta} = -\frac{\mathrm{Q}_+(\zeta_1)}{2}$ which implies that $\Re \frac{z_4}{\beta} = -\frac{\mathrm{Q}_+(\zeta_1)}{2\delta}$ and; let $r \in \mathbb{R}$ be the unique real number such that $\Im \frac{z_4}{\beta} = \frac{r}{\delta}$, then

$$z_4 = \frac{\beta}{\delta}\left(-\frac{\mathrm{Q}_+(\zeta_1)}{2} + \imath r\right)$$

Calculating the determinant of g shows that

$$1 = \det g = \det \begin{pmatrix} \delta\beta & & \\ * & u & \\ * & * & \delta^{-1}\beta \end{pmatrix} = \beta^2 \det u$$

so $\beta^2 = \det u^{-1}$, therefore;

$$g = \begin{pmatrix} \delta\beta & & \\ \zeta & u & \\ \frac{\beta}{\delta}\left(-\frac{Q_+(\zeta)}{2}+\imath r\right) & -\frac{\beta}{\delta}(\zeta^* u) & \frac{\beta}{\delta} \end{pmatrix} \tag{3.6}$$

where $u \in \mathrm{U}(n-1;R)$, $\beta \in \mathbb{C}$, $\delta \in \mathbb{R}^{>0}$ such that $\beta^2 = \det u^{-1}$, $\delta\beta$ and $\frac{\beta}{\delta} \in \mathbb{R}$. Furthermore $\zeta \in R^{n-1}$ and $r \in \mathbb{R}$ and since $\delta\beta \in \mathbb{R}$ then $\beta^2\left(-\frac{Q_+(\zeta)}{2}+\imath r\right) \in R$, but since $\beta^2 = \det u^{-1}$, β^2 is a unit in R, therefore this is equivalent to requiring that $-\frac{Q_+(\zeta)}{2}+\imath r \in \mathbb{R}$. Therefore $g \in \mathrm{SU}(1,n;R)_\infty$ if and only if; $u \in \mathrm{U}(n-1;R)$, $\beta \in \mathbb{C}$, $\delta \in \mathbb{R}^{>0}$ such that $\beta^2 = \det u^{-1}$, $\delta\beta$ and $\frac{\beta}{\delta} \in R$, $\zeta \in R^{n-1}$ and $r \in \mathbb{R}$ such that $-\frac{Q_+(\zeta)}{2}+\imath r \in R$.

Take $am(\delta,u,\beta) \in \mathrm{AM}(R)$ and $\nu(u^{-1}\zeta,r) \in \mathrm{N}(R)$, then

$$am(\delta,u,\beta)\nu(u^{-1}\zeta,r) = \begin{pmatrix} \delta\beta & & \\ \zeta & u & \\ \frac{\beta}{\delta}\left(-\frac{Q_+(\zeta)}{2}+\imath r\right) & -\frac{\beta}{\delta}(\zeta^* u) & \frac{\beta}{\delta} \end{pmatrix}$$

and comparing with (3.6) shows that $\mathrm{SU}(n,1;R)_\infty \leq \mathrm{AM}(R)\mathrm{N}(R)$.

Finally, it remains to prove that $\mathrm{N}(R)$ is normal in $\mathrm{SU}(n,1;R)_\infty$ so; let $am \in \mathrm{AM}(R)$ and $\nu_1,\nu_2 \in \mathrm{N}(R)$, if $m^{-1}a^{-1}\nu_1 am \in \mathrm{N}(R)$ then $\nu_2^{-1}m^{-1}a^{-1}\nu_1 am\nu_2 \in \mathrm{N}(R)$, and after multiplying out

$$\begin{aligned} am^{-1}\nu_1 am &= \begin{pmatrix} 1 & & \\ \frac{\overline{\beta}}{\delta}u\zeta & I_{n-1} & \\ \frac{1}{\delta^2}\left(-\frac{Q_+(\zeta)}{2}+\imath r\right) & -\frac{\beta}{\delta}(\zeta^* u) & 1 \end{pmatrix} \\ &= \nu\left((\beta\delta)^{-1}u\zeta,\ r\delta^{-2}\right) \in \mathrm{N}(R) \end{aligned}$$

showing that $\mathrm{N}(R)$ is indeed normal in $\mathrm{SU}(n,1;R)_\infty$. ∎

3.4 The Involution and Brûhat Decomposition

The non-parabolic automorphisms are more complicated to write down than those which are parabolic, however the non-parabolic automorphisms can be expressed in terms of a product of parabolic automorphisms and a single non-parabolic automorphism called the involution. This section introduces the involution and describes how to write non-parabolic elements via the Brûhat decomposition of the special unitary group under restriction to a field of characteristic zero which is stable by complex conjugation.

The involution is denoted ω and $\omega \in \mathrm{SU}(n,1;\mathbb{Z})$, its explicit matrix form depends on the congruence class of n modulo 4;

$$\omega = \begin{cases} \begin{pmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{pmatrix} & \text{if } n \equiv 0,3 \mod 4 \\ \begin{pmatrix} & & -1 \\ & \iddots & \\ -1 & & \end{pmatrix} & \text{if } n \equiv 2 \mod 4 \\ \begin{pmatrix} -1 & & \\ & I_{n-2} & \\ & & 1 \end{pmatrix} & \text{if } n \equiv 1 \mod 4 \end{cases}$$

The involution ω has two important properties: firstly it interchanges the origin with the point at infinity $\omega \circ \mathbf{q}_\infty = \left(1 \; \underline{0} \; 0\right)^{\mathrm{t}}$ and secondly it is self-inverse $\omega^2 = 1$.

Proposition 3.4.1 *Let $K \subseteq \mathbb{C}$ be a field of characteristic zero which is stable by complex conjugation. Then Brûhat decomposition of* $\mathrm{SU}(n,1;K)$ *is*

$$\mathrm{SU}(n,1;K) = \mathrm{SU}(n,1;K)_\infty \bigsqcup \mathrm{SU}(n,1;K)_\infty \, \omega \mathrm{N}(K)$$

PROOF Let $g \in \mathrm{SU}(n,1;K)$, if $g \in \mathrm{SU}(n,1;K)_\infty$ then there is nothing to do, so assume $g \in \mathrm{SU}(n,1;K) - \mathrm{SU}(n,1;K)_\infty$. Since $g \circ \mathbf{q}_\infty \neq \mathbf{q}_\infty$, then $g^{-1} \circ \mathbf{q}_\infty \neq \mathbf{q}_\infty$ and as K is a field of characteristic zero

$$g^{-1} \circ \mathbf{q}_\infty = \begin{pmatrix} 1 \\ \underline{z} \\ \frac{-\mathrm{Q}+(\underline{z})-h}{2} + \imath x \end{pmatrix} \in K^{n+1}$$

Furthermore, since K is closed under complex conjugation Lemma 3.3.5 applies and there exists a $\nu \in \mathrm{N}(K)$ such that $\nu g^{-1} \circ \mathbf{q}_\infty = \left(1 \; \underline{0} \; 0\right)$. For all fields K, $\omega \in \mathrm{SU}(n,1;K)$, so $\omega\nu g^{-1} \in \mathrm{SU}(n,1;K)$ and $\omega\nu g^{-1} \circ \mathbf{q}_\infty = \mathbf{q}_\infty$, thus $\omega\nu g^{-1} \in \mathrm{SU}(n,1;K)_\infty$. Therefore putting $\omega\nu g^{-1} = g_\infty \in \mathrm{SU}(n,1;K)_\infty$ one concludes that $g = g_\infty^{-1}\omega\nu$. ∎

Chapter 4

Siegel Set Construction

Let $(X, |\cdot|)$ be a metric space and let G be a discrete subgroup of the isometry group of X, then a Siegel set for the action of G on X is a closed subset $\mathcal{S} \subset X$ with the following two properties:

1. for all $x \in X$ there is a $g \in G$ such that $g \circ x \in \mathcal{S}$ and;
2. the set $\{g \in G \mid \mathcal{S} \cap g \circ \mathcal{S} \neq \emptyset\}$ is finite.

From now on assume that $K = \mathbb{Q}\left(\sqrt{d}\right)$ is an imaginary quadratic field with ring of integers $\mathfrak{O}$ and adopt the notation $\Gamma = \mathrm{SU}(n, 1; \mathfrak{O})$, then the aim of this thesis is to compute Siegel sets for $X = \mathbb{H}^n_{\mathbb{C}}$ and $G = \Gamma$ when the class group of K is trivial.

This chapter describes a method for constructing such Siegel sets and presents this method in the form of an algorithm. The algorithm is quite naïve and not practical from a computational point of view, however it comprehensively describes the important steps in Siegel set construction, it is guaranteed to terminate and it is mathematically easy to verify its validity along with certain important bounds on the output. An improved version of this algorithm, which deals with computational concerns, is described in Chapter 5. In the most simple terms the flow of the algorithm is as follows:

1. Analytically compute a Siegel set for the action of Γ_∞, call this set S_∞. This set S_∞ is compact in every dimension but the height dimension, where it extends from the boundary at zero height, to the boundary at infinite height.
2. Construct integral vectors called cusps which satisfy certain bounds. These cusps proxy the height changing properties of elements of Γ and are much less computationally expensive to construct than integral automorphisms.
3. Use the cusps which have been constructed to attempt to raise all points in S_∞ above some fixed height L. If this cannot be done then go back and make some more cusps. If this can be done then letting $\varepsilon > 0$, the set $\mathrm{S}_\infty \cap \left\{\underline{\mathbf{v}} \in \mathbb{H}^n_{\mathbb{C}} \mid \mathrm{h}(\underline{\mathbf{v}}) \geq L - \varepsilon\right\}$ is a Siegel set.

4.1 Cusps

Cusps are integral vectors which proxy the height altering properties of integral automorphisms and are much more simple to construct than elements of Γ. This section describes how to explicitly write cusps down and introduces the effect function at a cusp which determines whether a cusp increases the height of a point it acts on; it is shown that this function is convex under the standard Euclidean metric, this proves to be a very useful property from a computational point of view.

Definition 4.1.1 (Cusp) *A cusp for K is a vector $\mathbf{q} \in \mathfrak{O}^{n+1}$ such that $\mathrm{Q}(\mathbf{q}) = 0$. The set of all cusps for K is denoted by $\mathcal{C}_K$.* □

Theorem 4.1.2 (Zink) *The number of orbits for the action of Γ on the points in $\partial\mathbb{H}^n_{\mathbb{C}}$ with coordinates in K is equal to the class number of K.*

PROOF See [Zin79]. ■

Corollary 4.1.3 *When the class number of K is 1, then for each cusp $\mathbf{q} \in \mathcal{C}_K$ there exists a $\gamma \in \Gamma$ such that $\mathbf{q} = \gamma^{-1}\mathbf{q}_\infty$.*

Lemma 4.1.4 *Suppose that $Cl(K) = 1$ and let $\mathbf{q} \in \mathcal{C}_K$. Then*

$$\mathbf{q} = \begin{pmatrix} \delta\beta \\ \zeta \\ \frac{\beta}{\delta}\left(-\frac{\mathrm{Q}_+(\zeta)}{2} + \imath r\right) \end{pmatrix}$$

where $\delta \in \mathbb{R}^{>0}$ such that $\delta^2 \in \mathbb{N}$; $\beta \in \mathbb{C}$ such that $|\beta| = 1$ and $\delta\beta \in \mathfrak{O}$; $\zeta \in \mathfrak{O}^{n-1}$ and $r \in \mathbb{R}$ such that $\frac{\beta}{\delta}\left(-\frac{\mathrm{Q}_+(\zeta)}{2} + \imath r\right) \in \mathfrak{O}$.

PROOF By Corollary 4.1.3, for all cusps $\mathbf{q} \in \mathcal{C}_K$ there exists a $\gamma \in \Gamma$ such that $\mathbf{q} = \gamma^{-1}\mathbf{q}_\infty$. By Proposition 3.4.1, since $\gamma \notin \Gamma_\infty$ and $\Gamma \subset \mathrm{SU}(n,1;K)$, it follows that there exist elements δ, β, u, ζ and r such that $\gamma^{-1} = am(\delta,u,\beta)\nu(u^{-1}\zeta,r)\omega\nu(\zeta',r')$ where $a(\delta,u,\beta) \in \mathrm{AM}(K)$ and $\nu(u^{-1}\zeta,r), \nu(\zeta',r') \in \mathrm{N}(K)$, thus

$$\mathbf{q} = a(\delta,u,\beta)\nu(u^{-1}\zeta,r)\omega\nu(\zeta',r')\mathbf{q}_\infty = a(\delta,u,\beta)\nu(u^{-1}\zeta,r)\begin{pmatrix}1\\0\\0\end{pmatrix} = \begin{pmatrix} \delta\beta \\ \zeta \\ \frac{\beta}{\delta}\left(-\frac{\mathrm{Q}_+(\zeta)}{2} + \imath r\right) \end{pmatrix}$$

and necessarily $\mathbf{q} \in \mathfrak{O}^{n+1}$. Considering the first coordinate, if $\delta\beta \in \mathfrak{O}$, then $\overline{\delta\beta} \in \mathfrak{O}$, thus $\overline{\delta\beta}\delta\beta = |\delta\beta|^2 = \delta^2$ and therefore $\delta^2 \in \mathbb{Z}$. ■

Definition 4.1.5 (Cusp Notation) *Suppose that $Cl(K) = 1$. Unless explicitly stated, all cusps shall be denoted $\mathbf{q}$ and if further cusps are required they shall be denoted $\mathbf{q}', \mathbf{q}'', \ldots$ etceteras. Given a cusp $\mathbf{q} \in \mathcal{C}_K$ the vector form of $\mathbf{q}$ will always be written as*

$$\mathbf{q} = \begin{pmatrix} \delta\beta \\ \zeta \\ \frac{\beta}{\delta}\left(-\frac{\mathrm{Q}_+(\zeta)}{2} + \imath r\right) \end{pmatrix}$$

where the variables are as in Lemma 4.1.4. The element δ is called the dilation factor of $\mathbf{q}$, β is called the rotation factor of $\mathbf{q}$, ζ is called the zeta factor of $\mathbf{q}$ and r is called the r factor of $\mathbf{q}$. And for cusps $\mathbf{q}', \mathbf{q}'', \ldots$ the dilation factors will be denoted $\delta', \delta'', \ldots$, the rotation factors will be denoted $\beta', \beta'', \ldots$, the zeta factors will be denoted $\zeta', \zeta'', \ldots$ and the r factors will be denoted $r', r'', \ldots$. □

Let $\underline{\mathbf{v}} \in \overline{\mathbb{H}^n_{\mathbb{C}}}^{\times}$, then $-\mathrm{Q}(\underline{\mathbf{v}}) = h$. The height function encodes how this height is altered by elements of $\mathrm{SU}(n,1;\mathbb{C})$.

Definition 4.1.6 (The Height Function) *Suppose that $Cl(K) = 1$, let $g \in \mathrm{SU}(n,1;\mathbb{C})$ and let $\underline{\mathbf{v}} \in \overline{\mathbb{H}^n_{\mathbb{C}}}$ such that $g \circ \underline{\mathbf{v}} \neq \mathbf{q}_\infty$. Then the height function is defined to be*

$$\mathrm{h}(g \circ \underline{\mathbf{v}}) = \frac{-\mathrm{Q}(\underline{\mathbf{v}})}{|\langle \underline{\mathbf{v}}, g^{-1}\mathbf{q}_\infty \rangle|^2} \qquad \square$$

Lemma 4.1.7 *Let $\underline{\mathbf{v}} \in \overline{\mathbb{H}^n_{\mathbb{C}}}$, let $g \in \mathrm{SU}(n,1;\mathbb{C})$ and suppose that $\gamma \circ \underline{\mathbf{v}} = \underline{\mathbf{v}}' \in \overline{\mathbb{H}^n_{\mathbb{C}}}^{\times}$. Then $\mathrm{h}(g \circ \underline{\mathbf{v}}) = h'$.*

PROOF See [Gol99, 5.4]. ■

By Corollary 4.1.3, whenever the class number of K is 1, for all $\gamma \in \Gamma$ there exists a cusp $\mathbf{q} \in \mathcal{C}_K$ such that

$$\mathrm{h}(\gamma \circ \underline{\mathbf{v}}) = \frac{-\mathrm{Q}(\underline{\mathbf{v}})}{|\langle \underline{\mathbf{v}}, \mathbf{q} \rangle|^2} \tag{4.1}$$

and conversely, for all cusps $\mathbf{q} \in \mathcal{C}_K$ there exists a $\gamma \in \Gamma$ which satisfies (4.1). Therefore the cusps in $\mathcal{C}_K$ perfectly proxy the effect on the change of height of points in $\mathbb{H}^n_{\mathbb{C}}$ under the action of automorphisms in Γ. This leads to the following definition.

Definition 4.1.8 (The Effect Function) *Let $\mathbf{q} \in \mathcal{C}_K$ and let $\underline{\mathbf{v}} \in \overline{\mathbb{H}^n_{\mathbb{C}}}$. Then the effect function of $\underline{\mathbf{v}}$ at $\mathbf{q}$ is defined to be*

$$\mathrm{e}_{\mathbf{q}}(\underline{\mathbf{v}}) = |\langle \underline{\mathbf{v}}, \mathbf{q} \rangle|^2$$

Let $X \subset \overline{\mathbb{H}^n_{\mathbb{C}}}$, then $\mathbf{q}$ is said to be effective on X whenever there exists a $\underline{\mathbf{v}} \in X$ such that $\mathrm{e}_{\mathbf{q}}(\underline{\mathbf{v}}) < 1$. $\square$

Proposition 4.1.9 *Let $\mathbf{q} \in \mathcal{C}_K$ and suppose that $Cl(K) = 1$. Then under horospherical coordinates and under the standard Euclidean metric, the effect function is convex in the set*

$$\mathbb{C}^{n-1} \times \mathbb{R} \times \mathbb{R}^{\geq 0} \equiv \overline{\mathbb{H}^n_{\mathbb{C}}}^{\times}$$

PROOF Let $\underline{\mathbf{v}} \in \overline{\mathbb{H}^n_{\mathbb{C}}}^{\times}$, then in horospherical coordinates $\underline{\mathbf{v}}$ can be written

$$\mathbf{v} \equiv (\underline{z}, x, h) \in \mathbb{C}^{n-1} \times \mathbb{R} \times \mathbb{R}^{\geq 0}$$

and by Corollary 4.1.3 $\mathbf{q} = \gamma^{-1}\mathbf{q}_\infty$, where $\gamma \in \Gamma$. Since $\gamma \in \mathrm{SU}(n,1;\mathbb{C})$, then by Proposition 3.4.1 and Lemma 3.3.6 γ may be written

$$\mathbf{q} = \nu(\zeta, r)\, m(\beta, u)\, a(\delta)\omega\mathbf{q}_\infty$$

where $\zeta \in \mathbb{C}^{n-1}$, $r \in \mathbb{R}$, $u \in \mathrm{U}(n-1)$, $\beta^2 = \det u^{-1}$ and $\delta \in \mathbb{R}^{>0}$, thus $\mathrm{e}_{\mathbf{q}}(\underline{\mathbf{v}})$ becomes:

$$\begin{aligned} \mathrm{e}_{\mathbf{q}}(\mathbf{v}) &= |\langle (\underline{z}, x, h), \nu(\zeta, r)\, m(u)\, a(\delta)\omega\mathbf{q}_\infty \rangle|^2 \\ &= \delta^2 |\langle (\underline{z}, x, h), \nu(\zeta, r)(0,0,0) \rangle|^2 \end{aligned}$$

$$= \delta^2 \left| \langle \nu(-\zeta,-r)(\underline{z},x,h),(0,0,0)\rangle \right|^2$$

Multiplication by a strictly positive real constant preserves convexity, thus it is sufficient to show that $\left| \langle \nu(-\zeta,-r)(\underline{z},x,h),(0,0,0)\rangle \right|^2$ is convex with respect to the Euclidean metric. Moreover, Heisenberg translation is a linear function and as such preserves convexity, so in fact it is only necessary to show that $\left| \langle (\underline{z},x,h),(0,0,0)\rangle \right|^2$ is convex. Multiplying out; $\left| \langle (\underline{z},x,h),(0,0,0)\rangle \right|^2 = \left(\frac{\mathrm{Q}_+(z)+h}{2}\right)^2 + x^2$. Since the sum of two convex functions is convex, and x^2 is convex, the convexity of the effect function follows from the convexity of $\left(\frac{\mathrm{Q}_+(\underline{\mathbf{z}})+h}{2}\right)^2$.

By definition, a function f is convex if and only if $f((1-t)X+tY) \leq (1-t)f(X)+tf(Y)$ where $t \in [0,1]$, and if f is a positive function then this implies that $f(X)^2$ is convex if $f((1-t)X+tY)^2 \leq (1-t)f(X)^2+tf(Y)^2$ holds. Using the Cauchy-Schwartz inequality

$$\begin{aligned}(1-t)f(X)^2+tf(Y)^2 &= \left(\left(\sqrt{1-t}f(X)\right)^2+\left(\sqrt{t}f(Y)\right)^2\right)\left(\left(\sqrt{1-t}\right)^2+\left(\sqrt{t}\right)^2\right)\\ &\geq ((1-t)f(X)+tf(Y))^2\end{aligned}$$

this is indeed seen to be the case. The function $\frac{\mathrm{Q}_+(\underline{\mathbf{Z}})+h}{2}$ is convex as $\mathrm{Q}_+(-)$ is the square of a norm and $h \geq 0$, therefore $\left(\frac{\mathrm{Q}_+(\underline{\mathbf{Z}})+h}{2}\right)^2$ is convex and as such so is $\mathrm{e}_{\mathbf{q}}(-)$. ■

Lemma 4.1.10 *Let $h > 0$, let $\underline{\mathbf{v}} \in \mathbb{H}^n_{\mathbb{C}}$ be a point of height h and let $\mathbf{q} \in \mathcal{C}_K$. Then $\mathrm{e}_{\mathbf{q}}(\underline{\mathbf{v}}) \geq \frac{h^2}{4}$.*

PROOF Let $q_0 \in \mathfrak{O}$ be the first coordinate in $\mathbf{q}$ and let $\tilde{\mathbf{q}} \in \partial\mathbb{H}^{n\,\times}_{\mathbb{C}}$ such that $\tilde{\mathbf{q}} = q_0^{-1}\mathbf{q}$. By definition $\mathrm{e}_{\mathbf{q}}(\underline{\mathbf{v}}) = \left| \langle \underline{\mathbf{v}},\mathbf{q}\rangle \right|^2 = \left| q_0 \right|^2 \left| \langle \underline{\mathbf{v}},\mathbf{q}'\rangle \right|^2$, and given that q_0 is a non-zero algebraic integer, $\left| q_0 \right|^2 \geq 1$. Thus $\mathrm{e}_{\mathbf{q}}(\underline{\mathbf{v}}) \geq \left| \langle \underline{\mathbf{v}},\tilde{\mathbf{q}}\rangle \right|^2$. By Proposition 4.1.9 and Lemma 3.2.4, the effect function is convex and there are no orthogonal subspaces in $\mathbb{H}^n_{\mathbb{C}}$ with respect to $\langle -,-\rangle$, implying that $\left| \langle \underline{\mathbf{v}},\tilde{\mathbf{q}}\rangle \right|^2$ is minimal when the Heisenberg components of $\underline{\mathbf{v}}$ and $\tilde{\mathbf{q}}$ are equal and in this case $\left| \langle \underline{\mathbf{v}},\tilde{\mathbf{q}}\rangle \right|^2 = \frac{h^2}{4}$, therefore $\mathrm{e}_{\mathbf{q}}(\underline{\mathbf{v}}) \geq \frac{h^2}{4}$. ■

4.2 Siegel Containers

The first stage in the computation of a Siegel set for Γ is to compute a Siegel set for Γ_∞, such a set is called a Siegel container. In this section a formula which gives a Siegel container for all groups Γ is derived.

Definition 4.2.1 (Siegel Container) *A Siegel container $\mathrm{S}_\infty \subset \mathbb{H}^n_{\mathbb{C}}$ is a set such that S_∞ is a Siegel set for Γ_∞. For $L \geq 0$, define*

$$\mathrm{S}_\infty(L) = \mathrm{S}_\infty \cap \left\{\underline{\mathbf{v}} \in \overline{\mathbb{H}^n_{\mathbb{C}}} \mid \mathrm{h}(\underline{\mathbf{v}}) \geq L\right\}$$ □

Proposition 4.2.2 *Let $\mathrm{S}_\infty \subset \mathbb{H}^n_{\mathbb{C}}$ be a Siegel container for Γ, let $L > 0$, and suppose that for all $\underline{\mathbf{v}} \in \mathbb{H}^n_{\mathbb{C}}$ there exists an automorphism $\gamma \in \Gamma$ such that $\gamma \circ \underline{\mathbf{v}} \in \mathrm{S}_\infty(L)$. Then $\mathrm{S}_\infty(L)$ is a Siegel set for Γ.*

PROOF The proof follows [FL03, Proposition 2]. By definition $\mathrm{S}_\infty(L)$ is contained within a Siegel set for Γ_∞, so if there are an infinite number of automorphisms γ such that $\gamma \circ \mathrm{S}_\infty(L) \cap \mathrm{S}_\infty(L)$, then all but a finite number must be non-parabolic. Thus it suffices to show that the non-parabolic automorphisms with such a

property are finite. So suppose that γ is non-parabolic and that both $\underline{\mathbf{v}} \in \mathrm{S}_\infty(L)$ and $\gamma \circ \underline{\mathbf{v}} \in \mathrm{S}_\infty(L)$ hold and let $\mathbf{q} \in C_K$ such that $\gamma^{-1}\mathbf{q} = \mathbf{q}_\infty$, then by Lemma 4.1.10;

$$\mathrm{h}(\gamma \circ \mathbf{v}) \leq \frac{4}{\mathrm{h}(\mathbf{v})} \tag{4.2}$$

so $L \leq \mathrm{h}(\gamma \circ \mathbf{v}) \leq \frac{4}{L}$. Furthermore, (4.2) also implies that if $\mathrm{h}(\mathbf{v}) > \frac{4}{L}$, then $\mathrm{h}(\gamma \circ \mathbf{v}) < L$, which by assumption is not true. Therefore $\underline{\mathbf{v}}, \gamma \circ \underline{\mathbf{v}} \in X = \mathrm{S}_\infty(L) - \mathrm{S}_\infty\left(\frac{4}{L}\right)$ and so

$$\{\gamma \in \Gamma \mid \gamma \circ \mathrm{S}_\infty(L) \cap \mathrm{S}_\infty(L) \neq \emptyset\} \subset \{\gamma \in \Gamma \mid \gamma \circ X \cap X \neq \emptyset\}$$

The set $\{\gamma \in \Gamma \mid \gamma \circ X \cap X \neq \emptyset\}$ is compact, therefore since Γ is discrete and hence discontinuous it is finite and $\mathrm{S}_\infty(L)$ is a Siegel set. ∎

In order to compute a Siegel container S_∞ for Γ it is necessary to understand the structure of Γ_∞; by Lemma 3.3.6 the integral stabilizer of infinity decomposes as $\Gamma_\infty = \mathrm{AM}(\mathfrak{O}) \ltimes \mathrm{N}(\mathfrak{O})$, the following lemma describes these groups.

Lemma 4.2.3 *For all fields $K = \mathbb{Q}\left(\sqrt{d}\right)$*

$$\mathrm{N}(\mathfrak{O}) = \begin{cases} \left\{\mathrm{v}(\zeta, r) \mid \zeta \in \mathfrak{O}^{n-1},\ r \in \frac{\sqrt{-d}}{2}\mathbb{Z},\ \mathrm{Q}_+(\zeta) \equiv \frac{2r}{\sqrt{-d}} \mod 2\right\} & \text{if } d \equiv 1 \mod 4 \\ \left\{\mathrm{v}(\zeta, r) \mid \zeta \in \mathfrak{O}^{n-1},\ r \in \sqrt{-d}\mathbb{Z},\ \mathrm{Q}_+(\zeta) \equiv 0 \mod 2\right\} & \text{if } d \not\equiv 1 \mod 4 \end{cases} \tag{4.3}$$

$$\mathrm{AM}(\mathfrak{O}) = \left\{m(u, \beta) \mid u \in \mathrm{U}(n-1; \mathfrak{O}),\ \beta \in \mathfrak{O}^* \text{ s.t. } \beta^2 = \det u^{-1}\right\} \tag{4.4}$$

PROOF First consider the integral Heisenberg translation group $\mathrm{N}(\mathfrak{O})$; by Lemma 3.3.6

$$\mathrm{N}(\mathfrak{O}) = \left\{\mathrm{v}(\zeta, r) \;\middle|\; \zeta \in \mathfrak{O}^{n-1},\ r \in \mathbb{R} \text{ s.t. } -\frac{\mathrm{Q}_+(\zeta)}{2} + \imath r \in \mathfrak{O}\right\}$$

The integrality condition on $\frac{\mathrm{Q}_+(\zeta)}{2} + \imath r$ depends on the congruence class of d modulo 4: when $d \equiv 1 \mod 4$, then the elements in $\mathfrak{O}$ are those of the form $\frac{a+b\sqrt{d}}{2}$ where $a, b \in \mathbb{Z}$ such that $a \equiv b \mod 2$; when $d \not\equiv 1 \mod 4$, then the elements in $\mathfrak{O}$ are those of the form $a + b\sqrt{d}$ where $a, b \in \mathbb{Z}$. Thus $\frac{\mathrm{Q}_+(\zeta)}{2} + \imath r \in \mathfrak{O}$ if and only if

$$\begin{array}{llll} r \in \frac{\sqrt{-d}}{2}\mathbb{Z} & \text{and} & \mathrm{Q}_+(\zeta) \equiv \frac{2r}{\sqrt{-d}} \mod 2 & \text{if } d \equiv 1 \mod 4 \\ r \in \sqrt{-d}\mathbb{Z} & \text{and} & \mathrm{Q}_+(\zeta) \equiv 0 \mod 2 & \text{if } d \not\equiv 1 \mod 4 \end{array}$$

showing that $\mathrm{N}(\mathfrak{O})$ is as given in (4.3). Second consider the integral AM-group $\mathrm{AM}(\mathfrak{O})$; by Lemma 3.3.6

$$\mathrm{AM}(\mathfrak{O}) = \left\{a(\delta, u, \beta) \mid \delta \in \mathbb{R}^{>0},\ u \in \mathrm{U}(n-1; \mathfrak{O}),\ \beta \in \mathbb{C} \text{ s.t. } \beta^2 = \det u^{-1},\ \delta\beta,\ \frac{\beta}{\delta} \in \mathfrak{O}\right\}$$

Since $\beta^2 = \det u^{-1}$ and u is a unitary matrix, then $|\beta|^2 = 1$, therefore taking norms; $|\delta\beta|^2 = \delta^2 \in \mathbb{Z}$ and $\left|\delta^{-1}\beta\right|^2 = \delta^{-2} \in \mathbb{Z}$, whence $\delta = 1$ so that

$$\mathrm{AM}(\mathfrak{O}) = \left\{m(u, \beta) \mid\ u \in \mathrm{U}(n-1; \mathfrak{O}),\ \beta \in \mathfrak{O} \text{ s.t. } \beta^2 = \det u^{-1}\right\}$$

but since $|\beta|^2 = 1$, then $\beta \in \mathfrak{O}^*$ showing that $\mathrm{AM}(\mathfrak{O})$ is as given in (4.4). ∎

Corollary 4.2.4 *Let* $\underline{\mathbf{v}} \in \mathbb{H}^n_{\mathbb{C}}$ *and let* $\gamma \in \Gamma_\infty$. *Then* $\mathrm{h}(\gamma \circ \underline{\mathbf{v}}) = \mathrm{h}(\underline{\mathbf{v}})$.

PROOF Write $\gamma = m(\beta,u)\nu(\zeta,r)$ and apply the height function to $\gamma \circ \underline{\mathbf{v}}$;

$$\mathrm{h}(\gamma \circ \underline{\mathbf{v}}) = \frac{-\mathrm{Q}(\underline{\mathbf{v}})}{|\langle \underline{\mathbf{v}}, \gamma^{-1}\mathbf{q}_\infty\rangle|^2} = \frac{-\mathrm{Q}(\underline{\mathbf{v}})}{|\langle \underline{\mathbf{v}}, \nu(\zeta,r)^{-1}m(\beta,u)^{-1}\mathbf{q}_\infty\rangle|^2} = \frac{-\mathrm{Q}(\underline{\mathbf{v}})}{|\beta|^2|\langle \underline{\mathbf{v}}, \mathbf{q}_\infty\rangle|^2} = \frac{-\mathrm{Q}(\underline{\mathbf{v}})}{|\langle \underline{\mathbf{v}}, \mathbf{q}_\infty\rangle|^2} = \mathrm{h}(\underline{\mathbf{v}}) \quad (4.5)$$

■

Corollary 4.2.5 *Let* $S \subset \mathbb{H}^n_{\mathbb{C}}$ *and suppose that S a Siegel set for* $\mathrm{N}(\mathfrak{O})$*, then S is a Siegel container for* Γ.

PROOF Let $u \in \mathrm{U}(n-1;\mathfrak{O})$. By definition u satisfies the relation $u^*u = I_{n-1}$, therefore for $i = 1 \ldots n-1$ the equality $\sum_{j=1}^{n-1} |u_{ij}|^2 = 1$ holds. The coordinates $u_{ij} \in \mathfrak{O}$ and as such if $u_{ij} \neq 0$ then $|u_{ij}|^2 \geq 1$ with equality if and only if $u_{ij} \in \mathfrak{O}^*$. Since the group of units of $\mathfrak{O}$ is finite, $\mathrm{U}(n-1;\mathfrak{O})$ is a finite group. Each element $u \in \mathrm{U}(n-1;\mathfrak{O})$ generates either zero or two elements $m(u,\beta) \in \mathrm{AM}(\mathfrak{O})$ depending upon whether $\det u^{-1} = \beta^2$ is soluble, thus $|\mathrm{AM}(\mathfrak{O})| \leq 2|\mathrm{U}(n-1;\mathfrak{O})|$, hence $\mathrm{AM}(\mathfrak{O})$ is also a finite group. Lemma 4.2.3 states that $\Gamma_\infty = \mathrm{AM}(\mathfrak{O}) \ltimes \mathrm{N}(\mathfrak{O})$, therefore since the number of automorphisms in $\mathrm{AM}(\mathfrak{O})$ is finite, if S is a Siegel set for $\mathrm{N}(\mathfrak{O})$, S is a Siegel set for Γ_∞. ■

Lemma 4.2.6 *The set*

$$\mathrm{S}_\infty = \begin{cases} \left\{ \underline{\mathbf{v}} \in \overline{\mathbb{H}^n_{\mathbb{C}}} \,\middle|\, |\Re \underline{z}_i| \leq \frac{1}{2},\ |\Im \underline{z}_i| \leq \frac{\sqrt{-d}}{4},\ |x| \leq \frac{\sqrt{-d}}{2} \right\} & \text{if } d \equiv 1 \mod 4 \\ \left\{ \underline{\mathbf{v}} \in \overline{\mathbb{H}^n_{\mathbb{C}}} \,\middle|\, |\Re \underline{z}_1| \leq 1,\ |\Re \underline{z}_i| \leq \frac{1}{2}\ (i \neq 1),\ |\Im \underline{z}_i| \leq \frac{\sqrt{-d}}{2},\ |x| \leq \frac{\sqrt{-d}}{2} \right\} & \text{if } d \not\equiv 1 \mod 4 \end{cases}$$

is a Siegel container for Γ.

PROOF By Corollary 4.2.5 it is sufficient to construct a Siegel set for $\mathrm{N}(\mathfrak{O})$, so let $\underline{\mathbf{v}} \in \overline{\mathbb{H}^n_{\mathbb{C}}}$ and let $\nu(\zeta,r) \in \mathrm{N}$; $\nu(\zeta,r)$ acts on $\underline{\mathbf{v}}$ by

$$\nu(\zeta,r) \circ \underline{\mathbf{v}} = (\underline{z} + \zeta, x + r - \Im\langle \underline{z}, \zeta\rangle, h)$$

Write $\underline{z}_i = w_i + \imath y_i$ where $w_i, y_i \in \mathbb{R}$. There are two cases to consider dependent on the congruence class of d modulo 4:

Suppose that $d \equiv 1 \mod 4$, in this case $\zeta_i = \frac{s_i + t_i\sqrt{d}}{2}$ where $s_i, t_i \in \mathbb{Z}$ such that $s_i \equiv t_i \mod 2$ and $r \in \frac{\sqrt{-d}}{2}\mathbb{Z}$ such that $\mathrm{Q}_+(\zeta) \equiv \frac{2r}{\sqrt{-d}} \mod 2$. Choose

- $t_i \in \mathbb{Z}$ such that $\left| \frac{t_i\sqrt{-d}}{2} + y_i \right| \leq \frac{\sqrt{-d}}{4}$;
- $s_i \in \mathbb{Z}$ such that $s_i \equiv t_i \mod 2$ and $\left| \frac{s_i}{2} + w_i \right| \leq \frac{1}{2}$ and having chosen all t_i and s_i;
- $r \in \frac{\sqrt{-d}}{2}\mathbb{Z}$ such that $\mathrm{Q}_+(\zeta) \equiv \frac{2r}{\sqrt{-d}} \mod 2$ and $|r + x - \Im\langle \underline{z}, \zeta\rangle| \leq \frac{\sqrt{-d}}{2}$.

so that $\nu(\zeta,r) \circ \underline{\mathbf{v}} \in \mathrm{S}_\infty$, thus for all $\underline{\mathbf{v}} \in \mathbb{H}^n_{\mathbb{C}}$ there exists a $\nu(\zeta,r) \in \mathrm{N}(\mathfrak{O})$ such that $\nu(\zeta,r) \circ \underline{\mathbf{v}} \in \mathrm{S}_\infty$. Now suppose that $\nu(\zeta,x) \in \mathrm{N}(\mathfrak{O})$ is a Heisenberg translation with the property that $X = \mathrm{S}_\infty \cap \nu(\zeta,x) \circ \mathrm{S}_\infty \neq \emptyset$ and let $\underline{\mathbf{v}} \in X$. By assumption $\nu(\zeta,x) \circ \underline{\mathbf{v}} \in X$, therefore for $i = 1 \ldots n-1$

$$\underline{z}_i,\ \zeta_i + \underline{z}_i \in \left\{ z \in \mathbb{C} \;\middle|\; |\Re z| \leq \frac{1}{2}, |\Im z| \leq \frac{\sqrt{-d}}{4} \right\}$$

Considering the real part, $\left|\frac{s_i}{2}+w_i\right| \leq \frac{1}{2}$ implies $\left|\frac{s_i}{2}\right| \leq \frac{1}{2}+|w_i| \leq 1$, thus $|s_i| \leq 2$; considering the imaginary part, $\left|\frac{t_i\sqrt{-d}}{2}+y_i\right| \leq \frac{\sqrt{-d}}{4}$ implies $\left|\frac{t_i\sqrt{-d}}{2}\right| \leq \frac{\sqrt{-d}}{4}+|y_i| \leq \frac{\sqrt{-d}}{2}$, thus $|t_i| \leq 1$. Hence ζ lies in a compact set and as ζ also lies in a discrete set then there is only a finite number of ζ for which $\nu(\zeta,r)\circ\underline{\mathbf{v}} \in X$ holds. Considering the r variable, the assertion is that

$$x,\ r+x-\Im\left\langle \underline{z},\zeta\right\rangle \in \left\{ x\in\mathbb{R} \;\middle|\; |x| \leq \frac{\sqrt{-d}}{2} \right\}$$

thus $|r+x-\Im\left\langle \underline{z},\zeta\right\rangle| \leq \frac{\sqrt{-d}}{2}$ and so $|r| \leq \frac{\sqrt{-d}}{2}+|x|+|\Im\left\langle \underline{z},\zeta\right\rangle| \leq \sqrt{-d}+|\Im\left\langle \underline{z},\zeta\right\rangle|$. It remains to bound $|\Im\left\langle \underline{z},\zeta\right\rangle|$:

$$|\Im\left\langle \underline{z},\zeta\right\rangle| = \left|\sum_{i=1}^{n-1}\frac{y_is_i-x_it_i\sqrt{-d}}{2}\right| \leq \frac{1}{2}\sum_{i=1}^{n-1}|y_is_i|+\left|x_it_i\sqrt{-d}\right| \leq \frac{1}{2}\sum_{i=1}^{n-1}1-\frac{d}{4} = \frac{n-1}{2}\left(1-\frac{d}{4}\right)$$

Thus $|r| \leq \sqrt{-d}+\frac{n-1}{2}\left(1-\frac{d}{4}\right)$, so r lies in a compact set and since it also lies in a discrete set then there are a finite number of choices for r. Therefore there exists a finite number of $\nu\in \mathrm{N}(\mathfrak{O})$ such that $\mathrm{S}_\infty \cap \nu\circ\mathrm{S}_\infty \neq \emptyset$ and as such S_∞ is a Siegel set for $\mathrm{N}(\mathfrak{O})$.

Suppose now $d \not\equiv 1 \mod 4$, in this case $\zeta_i = s_i+t_i\sqrt{d}$ where $s_i,t_i\in\mathbb{Z}$ such that $\mathrm{Q}_+(\zeta) = \sum_{i=1}^{n-1}|s_i|^2 - d|t_i|^2 \equiv 0 \mod 2$ and $r\in\sqrt{-d}\mathbb{Z}$. Choose

- $t_i\in\mathbb{Z}$ such that $\left|t_i\sqrt{-d}+y_i\right| \leq \frac{\sqrt{-d}}{2}$;
- $s_i\in\mathbb{Z}$, for $i\neq 1$ such that $|s_i+w_i| \leq \frac{1}{2}$ and having chosen these t_i and s_i;
- $s_1\in\mathbb{Z}$, such that $\sum_{i=1}^{n-1}|s_i|^2 - d|t_i|^2 \equiv 0 \mod 2$ and $|s_i+w_i| \leq 1$;
- $r\in\sqrt{-d}\mathbb{Z}$ such that $|r+x-\Im\left\langle \underline{z},\zeta\right\rangle| \leq \frac{\sqrt{-d}}{2}$.

so that $\nu(\zeta,r)\circ\underline{\mathbf{v}} \in \mathrm{S}_\infty$, thus for all $\underline{\mathbf{v}}\in\mathbb{H}^n_{\mathbb{C}}$ there exists a $\nu(\zeta,r)\in\mathrm{N}(\mathfrak{O})$ such that $\nu(\zeta,r)\circ\underline{\mathbf{v}}\in\mathrm{S}_\infty$. Now suppose that $\nu(\zeta,x)\in\mathrm{N}(\mathfrak{O})$ is a Heisenberg translation with the property that $X = \mathrm{S}_\infty\cap\nu(\zeta,x)\circ\mathrm{S}_\infty \neq\emptyset$ and let $\underline{\mathbf{v}}\in X$. By assumption $\nu(\zeta,x)\circ\underline{\mathbf{v}}\in X$, therefore for $i=2\ldots n-1$

$$\underline{z}_1,\ \zeta_1+\underline{z}_1 \in \left\{ z\in\mathbb{C} \;\middle|\; |\Re z| \leq 1, |\Im z| \leq \frac{\sqrt{-d}}{4} \right\} \text{ if } i=1$$
$$\underline{z}_i,\ \zeta_i+\underline{z}_i \in \left\{ z\in\mathbb{C} \;\middle|\; |\Re z| \leq \frac{1}{2}, |\Im z| \leq \frac{\sqrt{-d}}{4} \right\} \text{ if } i=2\ldots n-1$$

Considering the real part, if $i=1$ then $|s_i+w_i| \leq 1$ implies $|s_i| \leq 1+|w_i| \leq 2$, thus $|s_i| \leq 2$; and if $i\neq 1$ then $|s_i+w_i| \leq \frac{1}{2}$ implies $|s_i| \leq \frac{1}{2}+|w_i| \leq 1$, thus $|s_i| \leq 1$. Considering the imaginary part, $\left|t_i\sqrt{-d}+y_i\right| \leq \frac{\sqrt{-d}}{2}$ implies $\left|t_i\sqrt{-d}\right| \leq \frac{\sqrt{-d}}{2}+|y_i| \leq \sqrt{-d}$, thus $|t_i| \leq 1$. Hence ζ lies in a compact set, as ζ also lies in a discrete set then there is only a finite number of ζ for which $\nu(\zeta,r)\circ\underline{\mathbf{v}}\in X$ holds. As for the previous case of $d\equiv 1 \mod 4$, $|r| \leq \sqrt{-d}+|\Im\left\langle \underline{z},\zeta\right\rangle|$. Bounding $|\Im\left\langle \underline{z},\zeta\right\rangle|$:

$$|\Im\left\langle \underline{z},\zeta\right\rangle| = \left|\sum_{i=1}^{n-1}y_is_i-x_it_i\sqrt{-d}\right| \leq \sum_{i=1}^{n-1}|y_is_i|+\left|x_it_i\sqrt{-d}\right| \leq \sum_{i=1}^{n-1}2-\frac{d}{2} = (n-1)\left(2-\frac{d}{2}\right)$$

Thus $|r| \leq \sqrt{-d}+(n-1)\left(2-\frac{d}{2}\right)$, so r lies in a compact set and since it also lies in a discrete set then there are a finite number of choices for r. Therefore there exists a finite number of $\nu\in\mathrm{N}(\mathfrak{O})$ such that

$S_\infty \cap \nu \circ S_\infty \neq \emptyset$ and as such S_∞ is a Siegel set for $N(\mathfrak{O})$. ■

4.3 Siegel Sets

This section describes how to construct a Siegel set for Γ from a Siegel container and a set of cusps. It achieves this by introducing the Phi function at a cusp which computes the maximum height a point can be raised to by the action of a cusp; this function is very closely related to the effect function at a cusp. The key result is Lemma 4.3.2 which describes the property a set of cusps Q needs to have in order to prove the existence of a Siegel set.

Lemma 4.3.1 *Suppose that $Cl(K) = 1$, let $\varepsilon > 0$, let S_∞ be a Siegel container for Γ, let $\underline{\mathbf{v}} \in S_\infty$ and suppose that there exists a cusp $\mathbf{q} \in \mathcal{C}_K$ such that $e_{\mathbf{q}}(\underline{\mathbf{v}}) \leq 1-\varepsilon$. Then there exists a $\gamma \in \Gamma$ such that $h(\gamma \circ \underline{\mathbf{v}}) \geq (1-\varepsilon)^{-1} h(\underline{\mathbf{v}})$ and $\gamma \circ \underline{\mathbf{v}} \in S_\infty$.*

PROOF By Corollary 4.1.3, there exists a $\gamma \in \Gamma$ such that $\mathbf{q} = \gamma^{-1}\mathbf{q}_\infty$, thus

$$h(\gamma \circ \underline{\mathbf{v}}) = \frac{-Q(\underline{\mathbf{v}})}{|\langle \gamma \underline{\mathbf{v}}, \mathbf{q}_\infty \rangle|^2} = \frac{-Q(\underline{\mathbf{v}})}{|\langle \underline{\mathbf{v}}, \gamma^{-1}\mathbf{q}_\infty \rangle|^2} = \frac{-Q(\underline{\mathbf{v}})}{|\langle \underline{\mathbf{v}}, \mathbf{q} \rangle|^2} = \frac{-Q(\underline{\mathbf{v}})}{e_{\mathbf{q}}(\underline{\mathbf{v}})} \geq (1-\varepsilon)^{-1} h(\underline{\mathbf{v}})$$

If $\gamma \circ \underline{\mathbf{v}} \in S_\infty$ then there is nothing to do. If not then by Corollary 4.2.4 there exists an integral parabolic automorphism $\gamma_\infty \in \Gamma_\infty$ such that $\gamma_\infty \gamma \circ \underline{\mathbf{v}} \in S_\infty$ and $h(\gamma_\infty \gamma \circ \underline{\mathbf{v}}) = h(\gamma \circ \underline{\mathbf{v}})$. Thus taking $\gamma' = \gamma_\infty \gamma$ completes the proof. ■

Lemma 4.3.2 *Suppose that $Cl(K) = 1$, let $\varepsilon > 0$, let $L > 0$, let S_∞ be a Siegel container for Γ and suppose that there exists a set of cusps $Q \subset \mathcal{C}_K$ such that for all $\underline{\mathbf{v}} \in S_\infty - S_\infty(L)$, there exists a cusps $\mathbf{q} \in Q$ such that $e_{\mathbf{q}}(\underline{\mathbf{v}}) \leq 1-\varepsilon$. Then $S_\infty(L)$ is a Siegel set for Γ.*

PROOF Define the following sequence: let $\underline{\mathbf{v}}_0 \in S_\infty - S_\infty(L)$ and put;

$$\underline{\mathbf{v}}_{i+1} = \begin{cases} \underline{\mathbf{v}}_i & \text{if } h(\underline{\mathbf{v}}_i) \geq L \\ \gamma_i \circ \underline{\mathbf{v}}_i & \text{if } h(\underline{\mathbf{v}}_i) < L \end{cases}$$

where $\gamma_i \in \Gamma$ is chosen so that $h(\gamma_i \circ \underline{\mathbf{v}}_i) \geq (1-\varepsilon)^{-1} h(\underline{\mathbf{v}}_i)$ and $\gamma_i \circ \underline{\mathbf{v}}_i \in S_\infty$; by Lemma 4.3.1, under the assumptions of this lemma such a γ_i exists. The height of $\underline{\mathbf{v}}_i$ is thus bounded below by the inequality

$$h(\underline{\mathbf{v}}_i) \geq \min\left\{L, (1-\varepsilon)^{-i} h(\underline{\mathbf{v}}_0)\right\}$$

and if $i \geq \frac{\ln(h(\underline{\mathbf{v}}_0)) - \ln(L)}{\ln(1-\varepsilon)} = \alpha$, then it follows that $(1-\varepsilon)^{-i} h(\underline{\mathbf{v}}_0) \geq L$. Hence whenever $i \geq \alpha$, then $h(\underline{\mathbf{v}}_i) \geq L$. Let $N = \lceil \alpha \rceil$ and let $\gamma = \prod_{i=0}^{N} \gamma_i$, then $\gamma \in \Gamma$ such that $\gamma \circ \underline{\mathbf{v}}_0 \in S_\infty(L)$. Therefore by Proposition 4.2.2 $S_\infty(L)$ is a Siegel set for Γ. ■

Definition 4.3.3 (Phi Function) *Let $\mathbf{q} \in \mathcal{C}_K$, let $\underline{\mathbf{v}} \in \partial \mathbb{H}^{n\times}_{\mathbb{C}}$, let*

$$\varphi'_{\mathbf{q}}(\underline{\mathbf{v}}) = 2\sqrt{\delta^{-2} - \left(x - r\delta^{-2} + \Im\left\langle \underline{z}, (\delta\beta)^{-1}\zeta \right\rangle_+\right)^2} + 2\Re\left\langle \underline{z}, (\delta\beta)^{-1}\zeta \right\rangle_+ - Q_+\left((\delta\beta)^{-1}\zeta\right) - Q_+(\underline{z})$$

and define the phi function to be

$$\varphi_{\mathbf{q}}(\underline{\mathbf{v}}) = \begin{cases} \varphi'_{\mathbf{q}}(\underline{\mathbf{v}}) & \text{if } \varphi'_{\mathbf{q}}(\underline{\mathbf{v}}) \geq 0 \\ -1 & \text{if } \varphi'_{\mathbf{q}}(\underline{\mathbf{v}}) < 0 \text{ or } \varphi'_{\mathbf{q}}(\underline{\mathbf{v}}) \notin \mathbb{R} \end{cases}$$ □

The following lemma describes the relationship between the effect and phi functions.

Lemma 4.3.4 *Let* $\underline{\mathbf{v}} \in \partial\mathbb{H}^{n\,\times}_{\mathbb{C}}$*, let* $\mathbf{q} \in \mathcal{C}_K$ *and let* $L = \varphi_{\mathbf{q}}(\underline{\mathbf{v}})$*. Then* $\mathrm{e}_{\mathbf{q}}((\underline{z},x,h)) < 1$ *for all* $h \in [0,L]$*. Conversely whenever* $\mathrm{e}_{\mathbf{q}}((\underline{z},x,h)) < 1$*, then* $h \leq L$*.*

PROOF Suppose that $L > 0$, then

$$2\sqrt{\delta^{-2} - \left(x - r\delta^{-2} + \Im\left\langle z, (\delta\beta)^{-1}\zeta\right\rangle_{+}\right)^2} + 2\Re\left\langle z, (\delta\beta)^{-1}\zeta\right\rangle_{+} - \mathrm{Q}_{+}\left((\delta\beta)^{-1}\zeta\right) - \mathrm{Q}_{+}(z) > L \geq h$$

so that on rearranging this becomes

$$\begin{aligned} \delta^{-2} &> \left(\frac{h + \mathrm{Q}_{+}\left((\delta\beta)^{-1}\zeta\right) + \mathrm{Q}_{+}(\underline{z}) - 2\Re\left\langle \underline{z}, (\delta\beta)^{-1}\zeta\right\rangle_{+}}{2}\right)^2 \\ &\quad + \left(x - r\delta^{-2} + \Im\left\langle \underline{z}, (\delta\beta)^{-1}\zeta\right\rangle_{+}\right)^2 \\ &= \delta^{-2}\mathrm{e}_{\mathbf{q}}((\underline{z}, x, h)) \end{aligned}$$

and $\mathrm{e}_{\mathbf{q}}((\underline{z},x,h)) < 1$. Conversely, if $\mathrm{e}_{\mathbf{q}}((\underline{z},x,h)) < 1$ then arguing in reverse shows that $h \leq L$. ■

Lemma 4.3.5 *Suppose that* $Cl(K) = 1$*, let* $L > 0$*, let* $\varepsilon \in \left(0, \frac{L^2}{4}\right)$*, let* $\underline{\mathbf{v}} \in \partial\mathbb{H}^{n\,\times}_{\mathbb{C}}$*, suppose that there exists a cusp* $\mathbf{q} \in \mathcal{C}_K$ *such that*

$$\varphi_{\mathbf{q}}(\underline{\mathbf{v}}) \geq \frac{L^2}{L - 2\sqrt{\varepsilon}}$$

and let $\underline{\mathbf{v}}' \in \left\{ \underline{\mathbf{v}}' \in \overline{\mathbb{H}^n_{\mathbb{C}}}^{\times} \;\middle|\; \underline{z}' = \underline{z},\ x' = x,\ h' \leq L \right\}$*. Then* $\mathrm{e}_{\mathbf{q}}(\underline{\mathbf{v}}') < 1 - \varepsilon$*.*

PROOF Let $X, Y \in [0,1]$, let $Z \in [0,2]$ and assume that $X - Y > \varepsilon X$ and $2\sqrt{X-Y} - Z \geq \frac{L^2}{L - 2\sqrt{\varepsilon}}$. Since $\varepsilon > 0$, then $2\sqrt{X-Y} - Z \geq L$, so that $\left(2\sqrt{X-Y} - Z\right)2\sqrt{\varepsilon} \geq L2\sqrt{\varepsilon X}$, thus $L\left(2\sqrt{X-Y} - Z\right) - L2\sqrt{\varepsilon X} \geq L\left(2\sqrt{X-Y} - Z\right) - \left(2\sqrt{X-Y} - Z\right)2\sqrt{\varepsilon}$ and therefore

$$\frac{L}{L - 2\sqrt{\varepsilon}} \geq \frac{2\sqrt{X-Y} - Z}{2\sqrt{X-Y} - Z - 2\sqrt{\varepsilon X}}$$

By assumption $X - Y > \varepsilon X$, so that $\sqrt{X - Y - \varepsilon X} > \sqrt{X-Y} - \sqrt{\varepsilon X}$, hence

$$\frac{L}{L - 2\sqrt{\varepsilon}} \geq \frac{2\sqrt{X-Y} - Z}{2\sqrt{X - Y - \varepsilon X} - Z}$$

and therefore $2\sqrt{X(1-\varepsilon) - Y} - Z > L$. Take

$$\begin{aligned} X &= \delta^{-2} \\ Y &= \left(x - r\delta^{-2} + \Im\left\langle \underline{z}, (\delta\beta)^{-1}\zeta\right\rangle_{+}\right)^2 \end{aligned}$$

$$Z = -2\Re\left\langle \underline{z}, (\delta\beta)^{-1}\zeta\right\rangle_{+} + \mathrm{Q}_{+}\left((\delta\beta)^{-1}\zeta\right) + \mathrm{Q}_{+}(\underline{z})$$

so that $\varphi_{\mathbf{q}}(\underline{\mathbf{v}}) = 2\sqrt{X-Y} - Z$, hence by supposition

$$2\sqrt{\delta^{-2}(1-\varepsilon) - \left(x - r\delta^{-2} + \Im\left\langle z, (\delta\beta)^{-1}\zeta\right\rangle_{+}\right)^2} + 2\Re\left\langle z, (\delta\beta)^{-1}\zeta\right\rangle_{+} - \mathrm{Q}_{+}\left((\delta\beta)^{-1}\zeta\right) - \mathrm{Q}_{+}(z) > L$$

on rearranging this becomes

$$\begin{aligned}(1-\varepsilon)\delta^{-2} &> \left(\frac{L + \mathrm{Q}_{+}\left((\delta\beta)^{-1}\zeta\right) + \mathrm{Q}_{+}(\underline{z}) - 2\Re\left\langle \underline{z}, (\delta\beta)^{-1}\zeta\right\rangle_{+}}{2}\right)^2 \\ &\quad + \left(x - r\delta^{-2} + \Im\left\langle \underline{z}, (\delta\beta)^{-1}\zeta\right\rangle_{+}\right)^2 \\ &= \delta^{-2}\mathrm{e}_{\mathbf{q}}((\underline{z}, x, L))\end{aligned}$$

implying that $\mathrm{e}_{\mathbf{q}}((\underline{z}, x, L)) < 1-\varepsilon$. The result now follows from Lemma 4.3.4. ■

This lemma can be interpreted as saying that "if for every point $\underline{\mathbf{v}} \in \mathrm{S}_{\infty} \cap \partial\mathbb{H}^{n\,\times}_{\mathbb{C}}$ it can be shown that a cusp $\mathbf{q}$ can be chosen from $\mathcal{C}_K$ such that $\varphi_{\mathbf{q}}(\underline{\mathbf{v}}) \geq \frac{L^2}{L-2\sqrt{\varepsilon}}$ then this proves that $\mathrm{S}_{\infty}(L)$ is a Siegel set for Γ." This provides the skeleton of a verifiable test for a set of cusps to show that this set of cusps generates a Siegel set.

4.4 Discretisation

Computationally it is of course not possible to calculate the Phi function at each cusp on every point on the boundary of S_{∞} since it consists of an uncountably infinite number of points, it is therefore necessary to introduce a strategy which allows only a finite number of points to be considered. This section uses the convexity of the effect function to derive such a strategy; it shows that the infimum of the Phi function on a convex polytope is equal to the infimum over the vertices of the polytope, as such by discretising the space into a finite number of convex polytopes the existence of a Siegel set can be proved by computing the Phi function on the vertices of these polytopes and hence by making a finite number of computations. Additionally an error bound on discretisation is derived which allows the bounding of overall error in the Siegel set generation algorithm found at the end of this chapter.

Definition 4.4.1 (Phi Function on a Set) *Let $\mathbf{q} \in \mathcal{C}_K$ and let $V \subset \partial\mathbb{H}^{n\,\times}_{\mathbb{C}}$, then the value of the Phi function on V at $\mathbf{q}$ is defined to be*

$$\Phi_{\mathbf{q}}(V) = \inf\{\varphi_{\mathbf{q}}(\underline{\mathbf{v}}) \mid \underline{\mathbf{v}} \in V\}$$ □

Lemma 4.4.2 *Let $V \subset \partial\mathbb{H}^{n\,\times}_{\mathbb{C}}$ be a convex polytope, let $V' = \{\underline{\mathbf{v}} \in V \mid \underline{\mathbf{v}}$ is a vertex of $V\}$ and let $\mathbf{q} \in \mathcal{C}_K$. Then $\Phi_{\mathbf{q}}(V) = \Phi_{\mathbf{q}}(V')$.*

PROOF Let $\varphi_{\mathbf{q}}(V') = L$ so that for all vertices $\underline{\mathbf{v}}$ of V, $\varphi_{\mathbf{q}}(\underline{\mathbf{v}}) \geq L$. Taking $\varepsilon = 0$ in the proof of Lemma 4.3.5 shows that for all $\underline{\mathbf{v}} \in \left\{\underline{\mathbf{v}} \in \overline{\mathbb{H}^{n}_{\mathbb{C}}}^{\times} \mid (\underline{z}, x, 0) \in V,\ h = L\right\}$, $\mathrm{e}_{\mathbf{q}}(\underline{\mathbf{v}}) \leq 1$, but then, again by using the proof of Lemma 4.3.5, $\varphi_{\mathbf{q}}(\underline{\mathbf{v}}) \geq L$ for all $\underline{\mathbf{v}} \in V$. ■

Lemma 4.4.3 *Let $Q \subset \mathcal{C}_K$, let $V \subset \partial\mathbb{H}^{n\,\times}_{\mathbb{C}}$ be a convex polytope with respect to the Euclidean metric, let $V' = \{\underline{\mathbf{v}} \mid \underline{\mathbf{v}} \text{ is a vertex of } V\}$, let $L > 0$, let $\varepsilon \in \left(0, \frac{L^2}{4}\right)$, suppose that*

$$\sup\left\{\Phi_{\mathbf{q}}(V') \;\middle|\; \mathbf{q} \in Q\right\} \geq \frac{L^2}{L - 2\sqrt{\varepsilon}}$$

and let $V(0,L) = \left\{(\underline{z}, x, h) \in \overline{\mathbb{H}^n_{\mathbb{C}}}^{\times} \mid (\underline{z}, x, 0) \in V \text{ and } h \leq L\right\}$. Then for all $\underline{\mathbf{v}} \in V(0,L)$, $\mathrm{e}_{\mathbf{q}}(\underline{\mathbf{v}}) < 1 - \varepsilon$.

PROOF Let $h \in [0,L]$ and put $V'(h) = \left\{(\underline{z}, x, h) \in \overline{\mathbb{H}^n_{\mathbb{C}}}^{\times} \;\middle|\; (\underline{z}, x, 0) \in V'\right\}$, then by Lemma 4.3.5, $\mathrm{e}_{\mathbf{q}}(\underline{\mathbf{v}}) < 1 - \varepsilon$ for all $\underline{\mathbf{v}} \in V'(L)$. Let $V(h) = \left\{(\underline{z}, x, h) \in \overline{\mathbb{H}^n_{\mathbb{C}}}^{\times} \;\middle|\; (\underline{z}, x, 0) \in V\right\}$; by Proposition 4.1.9 the effect function is a convex function and since a convex function cannot have a local maximum on any positive dimensional face of a compact convex set, $\sup\{\mathrm{e}_{\mathbf{q}}(\underline{\mathbf{v}}) \mid \underline{\mathbf{v}} \in V(h)\} = \sup\{\mathrm{e}_{\mathbf{q}}(\underline{\mathbf{v}}) \mid \underline{\mathbf{v}} \in V'(h)\}$, hence the result. ∎

Corollary 4.4.4 *Let S_∞ be a Siegel container for Γ, let $N \in \mathbb{N}$, let $V_1, \ldots, V_N \subset \mathrm{S}_\infty$ be convex polytopes such that $\mathrm{S}_\infty = \bigcup_{i=0}^{N} V_i$, let $V_i' = \{\underline{\mathbf{v}} \in V_i \mid \underline{\mathbf{v}} \text{ is a vertex of } V_i\}$, let $L > 0$, let $\varepsilon \in \left(0, \frac{L^2}{4}\right)$ and suppose that there exists a set of cusps $Q \subset \mathcal{C}_K$ such that*

$$\inf\left\{\sup\left\{\Phi_{\mathbf{q}}(V_i') \;\middle|\; \mathbf{q} \in Q\right\} \;\middle|\; i = 1, \ldots, N\right\} \geq \frac{L^2}{L - 2\sqrt{\varepsilon}}$$

Then $\mathrm{S}_\infty(L)$ is a Siegel set for Γ.

PROOF By Lemma 4.4.3, for all $\underline{\mathbf{v}} \in \mathrm{S}_\infty(L)$ there exists a cusp $\mathbf{q} \in Q$ such that $\mathrm{e}_{\mathbf{q}}(\underline{\mathbf{v}}) < 1 - \varepsilon$. Therefore by Lemma 4.3.2, $\mathrm{S}_\infty(L)$ is a Siegel set for Γ. ∎

And thus this Corollary says explicitly how to show that a set of cusps generates a Siegel set in a finite number of computations. This chapter concludes with an investigation into the bounds on the coordinates of cusps such that these cusps may be effective on a given region and uses these results to develop a strategy for discretising the search space.

Lemma 4.4.5 *Let $\mathbf{q} \in \mathcal{C}_K$, let $\underline{\mathbf{v}} \in \overline{\mathbb{H}^n_{\mathbb{C}}}^{\times}$, let $\underline{\varepsilon} \in \mathbb{C}^{n-1}$ and $\rho \in \mathbb{R}$ satisfy $\underline{z} + \underline{\varepsilon} = \frac{\zeta}{\delta\beta}$ and $x + \rho = \frac{r}{\delta^2}$ and suppose that either $|\underline{\varepsilon}_i| \geq \sqrt{\frac{2}{\delta}}$ for any $i = 1, \ldots, n-1$, or $|\rho| \geq \frac{1}{\delta} + \sqrt{\frac{2}{\delta}}\sum|\underline{z}_i|$ hold. Then $\mathrm{e}_{\mathbf{q}}(\underline{\mathbf{v}}) \geq 1$.*

PROOF By definition

$$\begin{aligned}
\delta^{-2}\mathrm{e}_{\mathbf{q}}(\underline{\mathbf{v}}) &= \left(\frac{\mathrm{Q}_+(\underline{z}+\underline{\varepsilon}) + \mathrm{Q}_+(\underline{z}) + h - 2\Re\langle \underline{z}, \underline{z}+\underline{\varepsilon}\rangle_+}{2}\right)^2 + \left(x - x - \rho + \Im\langle \underline{z}, \underline{z}+\underline{\varepsilon}\rangle_+\right)^2 \\
&= \left(\frac{\mathrm{Q}_+(\underline{\varepsilon}) + h}{2}\right)^2 + \left(\rho - \Im\langle \underline{z}, \underline{\varepsilon}\rangle_+\right)^2
\end{aligned}$$

from which it follows that if either $\mathrm{Q}_+(\underline{\varepsilon}) \geq \frac{2}{\delta}$, or $\left|\rho - \Im\langle \underline{z}, \underline{\varepsilon}\rangle_+\right| \geq \frac{1}{\delta}$, then $\mathrm{e}_{\mathbf{q}}(\underline{\mathbf{v}}) \geq 1$. Whenever $|\underline{\varepsilon}_i| \geq \sqrt{\frac{2}{\delta}}$ for any i, then $\mathrm{Q}_+(\underline{\varepsilon}) = \sum|\underline{\varepsilon}_i|^2 \geq \frac{2}{\delta}$, so without loss of generality suppose that $|\underline{\varepsilon}_i| < \sqrt{\frac{2}{\delta}}$ for all i, then $|\rho| \geq \frac{1}{\delta} + \sqrt{\frac{2}{\delta}}\sum|\underline{z}_i|$, whence

$$|\rho| \geq \frac{1}{\delta} + \sqrt{\frac{2}{\delta}}\sum|\underline{z}_i| > \frac{1}{\delta} + \sum|\underline{\varepsilon}_i||\underline{z}_i| \geq \frac{1}{\delta} + \left|\sum\overline{\underline{\varepsilon}_i}\underline{z}_i\right| = \frac{1}{\delta} + \left|\langle \underline{z}, \underline{\varepsilon}\rangle_+\right| \geq \frac{1}{\delta} + \left|\Im\langle \underline{z}, \underline{\varepsilon}\rangle_+\right|$$

therefore $|\rho| - \left|\Im\left\langle \underline{z}, \underline{\varepsilon}\right\rangle_+\right| > \frac{1}{\delta}$ and as such $\left|\rho - \Im\left\langle \underline{z}, \underline{\varepsilon}\right\rangle_+\right| > \frac{1}{\delta}$. ∎

Corollary 4.4.6 *Let* $\mathbf{q} \in \mathcal{C}_K$, *let* $\underline{\mathbf{v}} \in \overline{\mathbb{H}_{\mathbb{C}}^n}^{\times}$ *and suppose that either* $|\zeta_i| \geq \sqrt{2\delta} + \delta\left|\underline{z}_i\right|$, *or* $|r| \geq \delta + \sqrt{2\delta^3}\sum\left|\underline{z}_i\right| + \delta^2|x|$ *hold. Then* $\mathrm{e}_{\mathbf{q}}(\underline{\mathbf{v}}) \geq 1$.

PROOF Let $\underline{\varepsilon} \in \mathbb{C}^{n-1}$ satisfying $\underline{z} + \underline{\varepsilon} = \frac{\zeta}{\delta\beta}$ so that $\delta\beta(\underline{z} + \underline{\varepsilon}) = \zeta$, thus $|\zeta_i| = \left|\delta\beta(\underline{z}_i + \underline{\varepsilon}_i)\right| = \delta\left|\underline{z}_i + \underline{\varepsilon}_i\right| \leq \delta\left|\underline{z}_i\right| + \delta\left|\underline{\varepsilon}_i\right|$. Therefore if $|\zeta_i| \geq \sqrt{2\delta} + \delta\left|\underline{z}_i\right|$, then $|\underline{\varepsilon}_i| \geq \sqrt{\frac{2}{\delta}}$ and by Lemma 4.4.5 $\mathrm{e}_{\mathbf{q}}(\underline{\mathbf{v}}) \geq 1$. Let $\rho \in \mathbb{R}$ satisfying $x + \rho = \frac{r}{\delta^2}$ so that $\delta^2(x+\rho) = r$, thus $|r| \leq \delta^2|x| + \delta^2|\rho|$. Therefore if $|r| \geq \delta + \sqrt{2\delta^3}\sum\left|\underline{z}_i\right| + \delta^2|x|$, then $|\rho| \geq \frac{1}{\delta} + \sqrt{\frac{2}{\delta}}\sum\left|\underline{z}_i\right|$ and by Lemma 4.4.5 $\mathrm{e}_{\mathbf{q}}(\underline{\mathbf{v}}) \geq 1$. ∎

Lemma 4.4.7 *Let* $\mathbf{q} \in \mathcal{C}_K$, *let* $\underline{\mathbf{v}} \in \partial\mathbb{H}_{\mathbb{C}}^{n\,\times}$, *suppose that* $\varphi_{\mathbf{q}}(\underline{\mathbf{v}}) = L > 0$, *let* $\varepsilon \in \left(0, \frac{L^2}{4}\right)$, *define*

$$A = 2 + \sum\left(6\left|\underline{z}_i\right| + 4\sqrt{2}\right) \qquad B = 2\sqrt{2\left(1 + 2\sum\left(\left|\underline{z}_i\right| + \sqrt{2}\right)\right)}$$

$$C = \frac{A+B}{n-1} \qquad \sqrt{\lambda} = \frac{\sqrt{C^2 + \frac{4\varepsilon}{n-1}} - C}{2}$$

put

$$V = \left\{\underline{\mathbf{v}}' \in \partial\mathbb{H}_{\mathbb{C}}^{n\,\times} \;\middle|\; \left|\Re\underline{z}_i' - \Re\underline{z}_i\right|,\ \left|\Im\underline{z}_i' - \Im\underline{z}_i'\right|,\ \left|x' - x\right| \leq \lambda\right\}$$

Then $\Phi_{\mathbf{q}}(V) \geq L - \varepsilon$.

PROOF Let $\tilde{\zeta} = \frac{\zeta}{\delta\beta}$, let $\tilde{r} = \frac{r}{\delta^2}$, let $\underline{\lambda} = (\pm\lambda \pm \imath\lambda \cdots \pm\lambda \pm \imath\lambda) \in \mathbb{C}^{n-1}$ and let

$$V' = \left\{\underline{\mathbf{v}}' \in \partial\mathbb{H}_{\mathbb{C}}^{n\,\times} \;\middle|\; \Re\underline{z}_i' = \Re\underline{z}_i \pm \lambda,\ \Im\underline{z}_i' = \Im\underline{z}_i' \pm \lambda,\ x' = x \pm \lambda\right\}$$

so that V' is the set of vertices of V. By Lemma 4.4.2 it is sufficient to compute a lower bound on

$$\Phi_{\mathbf{q}}(V') = \inf\left\{2\sqrt{\delta^{-2} - \left(x \pm \lambda - \tilde{r} + \Im\left\langle \underline{z} + \underline{\lambda}, \tilde{\zeta}\right\rangle_+\right)^2} + 2\Re\left\langle \underline{z} + \underline{\lambda}, \tilde{\zeta}\right\rangle_+ - \mathrm{Q}_+\left(\tilde{\zeta}\right) - \mathrm{Q}_+(\underline{z} + \underline{\lambda})\right\}$$

Consider the second term in $\Phi_{\mathbf{q}}(V')$

$$\begin{aligned}
&2\Re\left\langle \underline{z} + \underline{\lambda}, \tilde{\zeta}\right\rangle_+ - \mathrm{Q}_+\left(\tilde{\zeta}\right) - \mathrm{Q}_+(\underline{z} + \underline{\lambda}) \\
\geq &2\Re\left\langle \underline{z}, \tilde{\zeta}\right\rangle_+ + 2\Re\left\langle \underline{\lambda}, \tilde{\zeta}\right\rangle_+ - \mathrm{Q}_+\left(\tilde{\zeta}\right) - \mathrm{Q}_+(\underline{z}) - 2\Re\left\langle \underline{z}, \underline{\lambda}\right\rangle_+ - \mathrm{Q}_+(\underline{\lambda}) \\
= &\underbrace{2\Re\left\langle \underline{z}, \tilde{\zeta}\right\rangle_+ - \mathrm{Q}_+\left(\tilde{\zeta}\right) - \mathrm{Q}_+(\underline{z})}_{X} + 2\Re\left\langle \underline{\lambda}, \tilde{\zeta}\right\rangle_+ - 2\Re\left\langle \underline{z}, \underline{\lambda}\right\rangle_+ - \mathrm{Q}_+(\underline{\lambda}) \\
\geq &X - 2\left|\left\langle \underline{\lambda}, \tilde{\zeta}\right\rangle_+\right| - 2\left|\left\langle \underline{z}, \underline{\lambda}\right\rangle_+\right| - \mathrm{Q}_+(\underline{\lambda}) \\
\geq &X - 2\sum|\lambda|\left|\tilde{\zeta}_i\right| - 2\sum\left|\underline{z}_i\right||\lambda| - \sum|\lambda|^2 \\
\geq &X - 2\lambda\sum\left|\tilde{\zeta}_i\right| - 2\lambda\sum\left|\underline{z}_i\right| - (n-1)\lambda^2
\end{aligned} \tag{4.6}$$

By assumption $\varphi_{\mathbf{q}}(\underline{\mathbf{v}}) > 0$ so that $\mathrm{e}_{\mathbf{q}}(\underline{\mathbf{v}}) < 1$, thus Lemma 4.4.5 applies, so $\left|\tilde{\zeta}_i\right| \leq |\underline{z}_i| + \sqrt{\frac{2}{\delta}}$ and therefore

$$\begin{aligned}
&\geq X - 2\lambda \sum \left(|\underline{z}_i| + \sqrt{\frac{2}{\delta}} \right) - 2\lambda \sum |\underline{z}_i| - (n-1)\lambda^2 \\
&\geq X - \lambda \sum \left(4|\underline{z}_i| + 2\sqrt{2} \right) - (n-1)\lambda^2
\end{aligned}$$

Now consider the first term in $\Phi_{\mathbf{q}}(V')$

$$\begin{aligned}
&2\sqrt{\delta^{-2} - \left(x \pm \lambda - \tilde{r} + \Im \left\langle \underline{z} + \underline{\lambda}, \tilde{\zeta} \right\rangle_+ \right)^2} \\
&\geq \underbrace{2\sqrt{\delta^{-2} - \left(x - \tilde{r} + \Im \left\langle \underline{z}, \tilde{\zeta} \right\rangle_+ \right)^2}}_{Y} - 2\sqrt{2\left(x - \tilde{r} + \Im \left\langle \underline{z}, \tilde{\zeta} \right\rangle_+ \right) \left| \pm\lambda + \Im \left\langle \underline{\lambda}, \tilde{\zeta} \right\rangle_+ \right|} - 2\left| \pm\lambda + \Im \left\langle \underline{\lambda}, \tilde{\zeta} \right\rangle_+ \right| \\
&\geq Y - 2\sqrt{2\delta^{-2} \left| \pm\lambda + \Im \left\langle \underline{\lambda}, \tilde{\zeta} \right\rangle_+ \right|} - 2\left| \pm\lambda + \Im \left\langle \underline{\lambda}, \tilde{\zeta} \right\rangle_+ \right| \\
&\geq Y - 2\sqrt{2\left(\pm\lambda + \left| \left\langle \underline{\lambda}, \tilde{\zeta} \right\rangle_+ \right| \right)} - 2\lambda - 2\left| \left\langle \underline{\lambda}, \tilde{\zeta} \right\rangle_+ \right| \\
&\geq Y - 2\sqrt{2\left(\pm\lambda + \sum |\underline{\lambda}_i| \left| \tilde{\zeta}_i \right| \right)} - 2\lambda - 2\sum |\underline{\lambda}_i| \left| \tilde{\zeta}_i \right| \\
&\geq Y - 2\sqrt{2\left(\lambda + \lambda \sum \left(|\underline{z}_i| + \sqrt{\frac{2}{\delta}} \right) \right)} - 2\lambda - 2\lambda \sum \left(|\underline{z}_i| + \sqrt{\frac{2}{\delta}} \right) \\
&\geq Y - 2\sqrt{2\left(\lambda + \lambda \sum \left(|\underline{z}_i| + \sqrt{2} \right) \right)} - 2\lambda - 2\lambda \sum \left(|\underline{z}_i| + \sqrt{2} \right) \qquad (4.7)
\end{aligned}$$

Combining the two inequalities (4.6) and (4.7) and noting that $L = \varphi_{\mathbf{q}}(\underline{\mathbf{v}}) = X + Y$

$$\begin{aligned}
\Phi_{\mathbf{q}}(V) \geq & L - \lambda \sum \left(4|\underline{z}_i| + 2\sqrt{2} \right) - (n-1)\lambda^2 - 2\sqrt{2\left(\lambda + \lambda \sum \left(|\underline{z}_i| + \sqrt{2} \right) \right)} - 2\lambda - 2\lambda \sum \left(|\underline{z}_i| + \sqrt{2} \right) \\
= & L - (n-1)\lambda^2 - \lambda \left(2 + \sum \left(6|\underline{z}_i| + 4\sqrt{2} \right) \right) - \sqrt{\lambda} 2\sqrt{2\left(1 + \sum \left(|\underline{z}_i| + \sqrt{2} \right) \right)}
\end{aligned}$$

Since $\delta \geq 1$, then $2 \geq \varphi_{\mathbf{q}}(\underline{\mathbf{v}})$ so that $1 \geq \lambda$, implying $\sqrt{\lambda} \geq \lambda$ and so

$$\begin{aligned}
\Phi_{\mathbf{q}}(V) &\geq L - (n-1)\lambda - \sqrt{\lambda} \left(2 + \sum \left(6|\underline{z}_i| + 4\sqrt{2} \right) \right) - \sqrt{\lambda} 2\sqrt{2\left(1 + \sum \left(|\underline{z}_i| + \sqrt{2} \right) \right)} \\
&= L - (n-1)\lambda - \sqrt{\lambda} \left(2 + \sum \left(6|\underline{z}_i| + 4\sqrt{2} \right) + 2\sqrt{2\left(1 + \sum \left(|\underline{z}_i| + \sqrt{2} \right) \right)} \right) \\
&= L - (n-1)\lambda - (A+B)\sqrt{\lambda} \\
&= L - (n-1) \left(\frac{\sqrt{C^2 + \frac{4\varepsilon}{n-1}} - C}{2} \right)^2 - (n-1)C \left(\frac{\sqrt{C^2 + \frac{4\varepsilon}{n-1}} - C}{2} \right)
\end{aligned}$$

$$= L-(n-1)\left(\frac{C^2-2C\sqrt{C^2+\frac{4\varepsilon}{n-1}}+C^2+\frac{4\varepsilon}{n-1}-2C^2+2C\sqrt{C^2+\frac{4\varepsilon}{n-1}}}{4}\right)$$
$$= L-\varepsilon$$
■

So by discretising into multidimensional rectangles where the length of each side is no greater than λ as computed in the Lemma above, then it is guaranteed that an error of no greater than ε is introduced through discretisation.

4.5 Cusp Construction

Corollary 4.4.4 explains how to compute Siegel sets under discretisation and Lemma 4.4.7 describes a strategy for discretisation and so it remains to consider how to construct a set of cusps; this section presents an algorithm for doing just this. To ease notation a few definitions are necessary;

Definition 4.5.1 *Let $X \subset \overline{\mathbb{H}^n_{\mathbb{C}}}$, let $\delta \in \mathbb{R}^{>0}$ and define*

$$\mathcal{C}_{K,\delta} = \{\mathbf{q} \in \mathcal{C}_K \mid \mathbf{q} \text{ has dilation factor } \delta\}$$
$$\mathcal{C}_K(X) = \{\mathbf{q} \in \mathcal{C}_K \mid \exists \underline{\mathbf{v}} \in X \text{ s.t. } \mathrm{e}_{\mathbf{q}}(\underline{\mathbf{v}}) < 1\}$$
$$\mathcal{C}_{K,\delta}(X) = \mathcal{C}_{K,\delta} \cap \mathcal{C}_K(X)$$
□

Let $\mu \geq 0$, let $X \subseteq \left\{\underline{\mathbf{v}} \in \partial\mathbb{H}^{n\,\times}_{\mathbb{C}} \mid |\Re z_i|,\ |\Im z_i|,\ |x| \leq \mu\right\}$, fix a dilation factor $\delta \in \mathbb{R}^{>0}$ and put $\Delta = \delta^2$ so that $\Delta \in \mathbb{N}$. Then specifically, this section derives a deterministic algorithm for generating a finite set $Q_\delta \subset \mathcal{C}_K$ such that $Q_\delta \subseteq \mathcal{C}_{K,\delta}$ and $\mathcal{C}_{K,\delta}(X) \subseteq Q_\delta$. Although it is not proved here, it is intuitively obvious that in general $\left|\mathcal{C}_{K,\delta}(X)\right| \ll |Q_\delta|$ and this inefficiency seriously impedes Siegel set generation from a practical point of view; Section 5.6 describes an improved algorithm which generates the set $\mathcal{C}_{K,\delta}(X)$ exactly.

Lemma 4.5.2 *Let $\mathbf{q} \in \mathcal{C}_K$ be a cusp of dilation factor δ. Then*

$$\beta = \begin{cases} \dfrac{a+b\sqrt{d}}{2\delta} & d \equiv 1 \mod 4 \\ \dfrac{a+b\sqrt{d}}{\delta} & d \not\equiv 1 \mod 4 \end{cases} \tag{4.8}$$

where $a, b \in \mathbb{Z}$ and

$$a^2 - db^2 = 4\Delta \quad d \equiv 1 \mod 4$$
$$a^2 - db^2 = \Delta \quad d \not\equiv 1 \mod 4$$

PROOF By Lemma 4.1.4, since $\mathbf{q}$ is a cusp, then $\delta\beta \in \mathfrak{O}$, whence β is of the form given in (4.8). By the same result $|\beta|^2 = 1$, thus

$$1 = \begin{cases} \dfrac{a^2-db^2}{4\Delta} & d \equiv 1 \mod 4 \\ \dfrac{a^2-db^2}{\Delta} & d \not\equiv 1 \mod 4 \end{cases}$$

If $d \not\equiv 1 \mod 4$ then the result is immediate. If $d \equiv 1 \mod 4$ then there is the integrality condition to satisfy; it is necessary and sufficient that $a \equiv b \mod 2$ to satisfy $\frac{a+b\sqrt{d}}{2} \in \mathfrak{O}$, however $a^2 - db^2 = 4\Delta$ and $d \equiv 1 \mod 4$ imply that $a^2 + b^2 \equiv 0 \mod 2$, and this is true if and only if $a \equiv b \mod 2$, so the integrality condition is automatically satisfied. ∎

Corollary 4.5.3 *Let $\mathbf{q} \in \mathcal{C}_K$ be a cusp of dilation factor δ. Then there is only a finite number of βs such that $\mathbf{q}$ has rotation factor β.*

PROOF The generator of the number field $d < 0$, therefore, independent of the congruence class of d, $|a|, |b| \leq 2\sqrt{\Delta}$. Since $a, b, \in \mathbb{Z}$ then the number of choices for a and b is finite. ∎

Lemma 4.5.4 *Let $\mathbf{q} \in \mathcal{C}_K$ be a cusp of dilation factor δ, rotation factor β and zeta factor ζ. Then r is a valid r factor for $\mathbf{q}$ if and only if*

$$r = r'\sqrt{-d} \tag{4.9}$$
$$2bd\,r' \equiv \mathrm{Q}_+(\zeta)\,a \mod 2\Delta \tag{4.10}$$
$$2a\,r' \equiv \mathrm{Q}_+(\zeta)\,b \mod 2\Delta \tag{4.11}$$

when $d \not\equiv 1 \mod 4$ and

$$r = \frac{r'\sqrt{-d}}{2} \tag{4.12}$$
$$bd\,r' \equiv \mathrm{Q}_+(\zeta)\,a \mod 2\Delta \tag{4.13}$$
$$a\,r' \equiv \mathrm{Q}_+(\zeta)\,b \mod 2\Delta \tag{4.14}$$
$$(a+bd)\,r' \equiv \mathrm{Q}_+(\zeta)\,(b+a) \mod 4\Delta \tag{4.15}$$

when $d \equiv 1 \mod 4$, where $r' \in \mathbb{Z}$, a and b are as in Lemma 4.5.2.

PROOF The real number r is a valid r factor for $\mathbf{q}$ if and only if $\frac{\beta}{\delta}\left(-\frac{\mathrm{Q}_+(\zeta)}{2} + \imath r\right) \in \mathfrak{O}$. Given that $\delta\beta \in \mathfrak{O}$ and $\mathfrak{O}$ is closed under complex conjugation then it follows that $\overline{\delta\beta}\frac{\beta}{\delta}\left(-\frac{\mathrm{Q}_+(\zeta)}{2} + \imath r\right) = -\frac{\mathrm{Q}_+(\zeta)}{2} + \imath r \in \mathfrak{O}$, therefore $r = r'\sqrt{-d}$ if $d \not\equiv 1 \mod 4$ and $r = \frac{r'\sqrt{-d}}{2}$ and $\mathrm{Q}_+(\zeta) \equiv r' \mod 2$ if $d \equiv 1 \mod 4$, where $r' \in \mathbb{Z}$.

Firstly taking the $d \not\equiv 1 \mod 4$ case;

$$\begin{aligned}\frac{\beta}{\delta}\left(\frac{-\mathrm{Q}_+(\zeta)}{2} + \imath r\right) &= \frac{a+b\sqrt{d}}{\Delta}\left(\frac{-\mathrm{Q}_+(\zeta) + 2r'\sqrt{d}}{2}\right) \\ &= \frac{(2bdr' - \mathrm{Q}_+(\zeta)\,a) + (2ar' - \mathrm{Q}_+(\zeta)\,b)\sqrt{d}}{2\Delta}\end{aligned} \tag{4.16}$$

Then (4.16) is integral if and only if $\frac{2bdr' - a\mathrm{Q}_+(\zeta)}{2\Delta} \in \mathbb{Z}$ and $\frac{2ar' - \mathrm{Q}_+(\zeta)b}{2\Delta} \in \mathbb{Z}$ and this is the case if and only if both (4.10) and (4.11) are satisfied.

Secondly taking the $d \equiv 1 \mod 4$ case;

$$\frac{\beta}{\delta}\left(\frac{-\mathrm{Q}_+(\zeta)}{2} + \imath r\right) = \frac{a+b\sqrt{d}}{2\Delta}\left(\frac{-\mathrm{Q}_+(\zeta) + r'\sqrt{d}}{2}\right)$$

$$= \frac{(bdr' - \mathrm{Q}_+(\zeta)\,a) + (ar' - \mathrm{Q}_+(\zeta)\,b)\sqrt{d}}{4\Delta} \tag{4.17}$$

Then (4.17) is integral if and only if $\frac{bdr' - \mathrm{Q}_+(\zeta)a}{2\Delta} \in \mathbb{Z}$, $\frac{ar' - \mathrm{Q}_+(\zeta)b}{2\Delta}$ and $bdr' - \mathrm{Q}_+(\zeta)\,a \equiv ar' - \mathrm{Q}_+(\zeta)\,b \mod 4\Delta$ and this is the case if and only if (4.13), (4.14) and (4.15) are satisfied. Note that when these conditions are satisfied, $a^2 - db^2 = 4\Delta$ immediately implies that $r' \equiv \mathrm{Q}_+(\zeta) \mod 2$. ■

This leads to the following algorithms for generating Q_δ. There are two cases depending on the congruence class of d modulo 4:

Algorithm 4.5.5 (Cusp Generation d $\not\equiv$ 1 mod 4)

Inputs: $n \in [2,3\ldots)$, $d \in \{-1,-2\}$, $\Delta \in \mathbb{N}$ and $X \subset \partial\mathbb{H}^{n\,\times}_{\mathbb{C}}$ where $X \subseteq \left\{\underline{\mathbf{v}} \in \partial\mathbb{H}^{n\,\times}_{\mathbb{C}} \mid |\Re z_i|, |\Im z_i|, |x| \leq \mu\right\}$ for some $\mu > 0$.

1. Assign $\delta \leftarrow \sqrt{\Delta}$
2. Compute $B_\delta \leftarrow \left\{ \frac{a+b\sqrt{d}}{\delta} \in \mathbb{C} \;\middle|\; a,b \in \mathbb{Z} \text{ s.t. } a^2 - db^2 = \Delta \right\}$
3. For each $\beta \in B_\delta$
   4. Compute $Z_{\delta,\beta} \leftarrow \left\{ \zeta \in \mathfrak{O}^{n-1} \;\middle|\; |\zeta_i| < \sqrt{2\delta} + \delta\mu \right\}$
   5. For each $\zeta \in Z_{\delta,\beta}$
      6. Compute

$$R_{\delta,\beta,\zeta} \leftarrow \left\{ r \in \mathbb{R} \;\middle|\; \begin{array}{l} |r| < \delta + \sqrt{2\delta^3}(n-1)\mu + \delta^2\mu,\ r = r'\sqrt{-d} \text{ where } r' \in \mathbb{Z} \text{ s.t.} \\ 2bd\,r' \equiv \mathrm{Q}_+(\zeta)\,a \mod 2\Delta \text{ and } 2a\,r' \equiv \mathrm{Q}_+(\zeta)\,b \mod 2\Delta \end{array} \right\}$$

      7. For each $r \in R_{\delta,\beta,\zeta}$
         8. Assign $\mathbf{q} \leftarrow \left(\delta\beta\ \zeta\ \frac{\beta}{\delta}\left(-\frac{\mathrm{Q}_+(\zeta)}{2} + \iota r\right)\right)^{\mathrm{t}}$
         9. Assign $Q_\delta \leftarrow Q_\delta \cup \{\mathbf{q}\}$
      10. Next
   11. Next
12. Next
13. Return Q_δ

Algorithm 4.5.6 (Cusp Generation d $\equiv$ 1 mod 4)

Inputs: $n \in [2,3\ldots)$, $d \in \{-3,-7,-11,-19,-43,-67,-163\}$, $\Delta \in \mathbb{N}$ and $X \subset \partial\mathbb{H}^{n\,\times}_{\mathbb{C}}$ where $X \subseteq \left\{\underline{\mathbf{v}} \in \partial\mathbb{H}^{n\,\times}_{\mathbb{C}} \mid |\Re z_i|, |\Im z_i|, |x| \leq \mu\right\}$ for some $\mu > 0$.

1. Assign $\delta \leftarrow \sqrt{\Delta}$
2. Compute $B_\delta = \left\{ \frac{a+b\sqrt{d}}{2\delta} \in \mathbb{C} \;\middle|\; a,b \in \mathbb{Z} \text{ s.t. } a^2 - db^2 = 4\Delta \right\}$

3. For each $\beta \in B_\delta$

   4. Compute $Z_{\delta,\beta} \leftarrow \left\{ \zeta \in \mathfrak{O}^{n-1} \;\middle|\; |\zeta_i| < \sqrt{2\delta} + \delta\mu \right\}$
   5. For each $\zeta \in Z_{\delta,\beta}$
      6. Compute

$$R_{\delta,\beta,\zeta} \leftarrow \left\{ r \in \mathbb{R} \;\middle|\; \begin{array}{l} |r| < \delta + \sqrt{2\delta^3}(n-1)\mu + \delta^2\mu,\ r = \frac{r'\sqrt{-d}}{2} \text{ where } r' \in \mathbb{Z} \text{ s.t.} \\ bd\,r' \equiv \mathrm{Q}_+(\zeta)\,a \mod 2\Delta,\ a\,r' \equiv \mathrm{Q}_+(\zeta)\,b \mod 2\Delta \text{ and} \\ (a+bd)\,r' \equiv \mathrm{Q}_+(\zeta)\,(b+a) \mod 4\Delta \end{array} \right\}$$

      7. Assign $\mathbf{q} \leftarrow \left(\delta\beta \;\; \zeta \;\; \frac{\beta}{\delta}\left(-\frac{\mathrm{Q}_+(\zeta)}{2} + \imath r\right) \right)^{\mathrm{t}}$
      8. Assign $Q_\delta \leftarrow Q_\delta \cup \{\mathbf{q}\}$
   9. Next
10. Next
11. Return Q_δ

Lemma 4.5.7 *The set $Q_\delta \subset \mathcal{C}_K$ generated by Algorithm 4.5.5 and Algorithm 4.5.6 is finite, $Q_\delta \subset \mathcal{C}_{K,\delta}$ and $Q_\delta \supseteq \mathcal{C}_{K,\delta}(X)$.*

PROOF For both algorithms, the assertion $Q_\delta \subset \mathcal{C}_{K,\delta}$ is immediate from line 1. The assertion that Q_δ is finite can be seen in the following way for both algorithms; by Corollary 4.5.3, once δ has been fixed there is only a finite number of valid β values that are available to complete a cusp and this number is $|B_\delta|$, where B_δ the set computed in line 2. In the algorithm the number of ζ values for each β is determined by $\left|Z_{\delta,\beta}\right|$, where $Z_{\delta,\beta}$ is the set computed in line 4 and since $Z_{\delta,\beta}$ is both compact and discrete, then $Z_{\delta,\beta}$ is finite for each β. The number of r values for each (β,ζ) pair is determined by the size of $R_{\delta,\beta,\zeta}$, where $R_{\delta,\beta,\zeta}$ is the set computed in line 6 and since for each pairing the set $R_{\delta,\beta,\zeta}$ is compact and discrete it is also finite. Examination of the algorithm shows that $|Q_\delta| = \sum_{\beta\in B_\delta} \sum_{\zeta\in Z_{\delta,\beta}} \left|R_{\delta,\beta,\zeta}\right|$ and since this is a finite sum of integers by the preceding argument, Q_δ is a finite set.

To prove the assertion that $Q_\delta \supseteq \mathcal{C}_{K,\delta}(X)$, the two algorithms must be treated separately. Considering Algorithm 4.5.5; let $\mathbf{q} \in \mathcal{C}_{K,\delta}(X)$ and suppose that $\mathbf{q} \notin Q_\delta$. By Lemma 4.5.2, the set B_δ consists of all possible rotation factors β allowable for a cusp of dilation factor δ, so $\beta \in B_\delta$ and as such if $\mathbf{q} \notin Q_\delta$, then either $\zeta \notin Z_{\delta,\beta}$ or $\zeta \in Z_{\delta,\beta}$ and $r \notin R_{\delta,\beta,\zeta}$. By Corollary 4.4.6, if $\zeta \notin Z_{\delta,\beta}$ and $\mathbf{q}$ is a cusp of dilation factor δ, rotation factor β and zeta factor ζ, then irrespective of the r factor of $\mathbf{q}$, $\mathrm{e}_{\mathbf{q}}(\underline{\mathbf{v}}) \geq 1$ for all $\underline{\mathbf{v}} \in X$, thus $\mathbf{q} \notin \mathcal{C}_{K,\delta}(X)$, hence it must be concluded that $\zeta \in Z_{\delta,\beta}$ and $r \notin R_{\delta,\beta,\zeta}$. However, again by Corollary 4.4.6, if $r \notin R_{\delta,\beta,\zeta}$ and $\mathbf{q}$ is a cusp of dilation factor δ, rotation factor β, zeta factor ζ, and r factor r, $\mathrm{e}_{\mathbf{q}}(\underline{\mathbf{v}}) \geq 1$ for all $\underline{\mathbf{v}} \in X$, implying that the statement: $r = r'\sqrt{-d}$ where $r' \in \mathbb{Z}$ such that $2bd\,r' \equiv \mathrm{Q}_+(\zeta)\,a \mod 2\Delta$ and $2a\,r' \equiv \mathrm{Q}_+(\zeta)\,b \mod 2\Delta$, is false. But by Lemma 4.5.4, given δ,β and ζ, $\mathbf{q}$ is a cusp with r factor r if and only if $r = r'\sqrt{-d}$ where $r' \in \mathbb{Z}$ s.t. $2bd\,r' \equiv \mathrm{Q}_+(\zeta)\,a \mod 2\Delta$ and $2a\,r' \equiv \mathrm{Q}_+(\zeta)\,b \mod 2\Delta$. Therefore $\mathbf{q} \in Q_\delta$ and this contradiction proves the result. The argument for Algorithm 4.5.6 is very similar; simply substitute in the corresponding results for $d \equiv 1 \mod 4$ from Lemma 4.5.2, Corollary 4.4.6 and Lemma 4.5.4. ∎

4.6 Siegel Set Construction

The final section in this chapter presents a general algorithm for computing Siegel sets for the action of Γ on $\mathbb{H}^n_{\mathbb{C}}$ when the imaginary quadratic field K has trivial class group. It is shown that this algorithm is guaranteed to terminate and error bounds on the output of the algorithm are derived. This algorithm is accurate and verifiable, but very slow; a much faster but less accurate and less verifiable algorithm which is more appropriate for a practical implementation is described in Section 5.10.

The following notation is defined in order to describe how to discretise the search space.

Definition 4.6.1 *Let $h \geq 0$, let $\lambda > 0$, let $X \subset \partial\mathbb{H}^{n\,\times}_{\mathbb{C}}$, let $\underline{\mathbf{v}} \in X$ and define*

$$\begin{aligned} V(\underline{\mathbf{v}},\lambda,X) &= \left\{\underline{\mathbf{v}}' \in X \;\middle|\; \left|\Re z_i' - \Re z_i\right|, \left|\Im z_i' - \Im z_i\right|, \left|x' - x\right| \leq \lambda \right\} \\ \Lambda(\lambda,X) &= \{\underline{\mathbf{v}} \in X \mid \Re z_i, \Im z_i, x \in \lambda\mathbb{Z}\} \\ \Omega(\lambda,X) &= \{V(\underline{\mathbf{v}},\lambda,X) \subset X \mid \underline{\mathbf{v}} \in \Lambda(\lambda,X)\} \end{aligned}$$

□

Algorithm 4.6.2 (Siegel Set Construction)

Inputs: $n \in \mathbb{N}^{\geq 2}$ the dimension, d a Heegner number, $\alpha \in (0,1)$ an error tolerance, a set $X \subseteq \left\{\underline{\mathbf{v}} \in \partial\mathbb{H}^{n\,\times}_{\mathbb{C}} \mid |\Re z_i|, |\Im z_i|, |x| \leq \mu\right\}$ for some $\mu > 0$.

1. Initialise: $L \leftarrow 2$, $\Delta \leftarrow 1$, $Q \leftarrow \emptyset$
2. Assign $\delta \leftarrow \sqrt{\Delta}$, $\varepsilon \leftarrow \alpha\dfrac{2}{\delta}$, $A \leftarrow 2 + \sum\left(6\mu + 4\sqrt{2}\right)$, $B \leftarrow 2\sqrt{2\left(1 + 2\sum\left(\mu + \sqrt{2}\right)\right)}$, $C \leftarrow \dfrac{A+B}{n-1}$
3. Assign $\lambda \leftarrow \left(\dfrac{\sqrt{C^2 + \frac{4\varepsilon}{n-1}} - C}{2}\right)^2$, $\Omega \leftarrow \Omega(\lambda, X)$
4. Compute Q_δ via either Algorithm 4.5.5 or Algorithm 4.5.6, depending on the congruence class of d, to X
5. Assign $Q \leftarrow Q \cup Q_\delta$
6. For each $V \in \Omega$
   7. Assign $V' \leftarrow \{\underline{\mathbf{v}} \in V \mid \underline{\mathbf{v}} \text{ is a vertex of } V\}$
   8. Assign $L' \leftarrow \sup\{\Phi_{\mathbf{q}}(V') \mid \mathbf{q} \in Q\}$
   9. If $L' < \dfrac{2}{\delta} - \varepsilon$ then assign $\Delta \leftarrow \Delta + 1$ and goto line 2
   10. $L \leftarrow \min\{L, L'\}$
11. Next
12. Return L

Proposition 4.6.3 *Let $d \in \{-1,-2,-3,-7,-11,-19,-43,-67,-163\}$, let $n \in [2,3,\dots)$, let $\alpha \in (0,1)$, S_∞ be the Siegel container computed in Lemma 4.2.6, let $X = S_\infty \cap \partial\mathbb{H}^n_{\mathbb{C}}{}^{\times}$ and let L be the output of* Algorithm 4.6.2(d,n,α,X). *Then for all $\varepsilon \in \left(0, \frac{L^2}{4}\right)$, the set $S_\infty(L-\varepsilon)$ is a Siegel set for Γ. Moreover the algorithm is guaranteed to terminate and return a value $L > 0$ and if $S_\infty(L'-\varepsilon)$ is a Siegel set for some $L' \in (0,2]$, then $\frac{L}{1-\alpha} \geq L'$.*

PROOF The set Ω consists of subsets $V_i \subset X = S_\infty \cap \{\underline{\mathbf{v}} \in S_\infty \mid h(\underline{\mathbf{v}}) = 0\}$ such that $X = \cup V_i$ and each V_i is a polytope. Putting $V_i' = \{\underline{\mathbf{v}} \in V \mid \underline{\mathbf{v}} \text{ is a vertex of } V_i\}$, the loop between lines 6 and 11 computes an L such that $L = \inf\{\sup\{\Phi_{\mathbf{q}}(V_i') \mid \mathbf{q} \in Q\} \mid i = 1,\dots,N\}$ for some set of cusps Q where N is the number of iterations in the loop. Whenever $\varepsilon \in \left(0, \frac{L^2}{4}\right)$, $\frac{L^2}{L-\sqrt{\varepsilon}} > 0$ and therefore by Corollary 4.4.4 $S_\infty(L-\varepsilon)$ is a Siegel set for Γ.

By [PR92][Theorem 4.4] Siegel sets are known to exists for all groups Γ so there exists some $L \in (0,2]$ such that $L = \inf\{\sup\{\varphi_{\mathbf{q}}(\underline{\mathbf{v}}) \mid \mathbf{q} \in \mathcal{C}_K\} \mid \underline{\mathbf{v}} \in X\}$ and as the real numbers are well ordered the set of all such L has a supremum, so let $L_{\max} \in (0,2]$ and suppose that $S_\infty(L_{\max})$ is a Siegel set and whenever $S_\infty(L)$ is a Siegel set, then $L_{\max} \geq L$. Let $\Delta = \left\lceil \left(\frac{2}{L_{\max}}\right)^2 \right\rceil$, put $\delta = \sqrt{\Delta}$ and for each convex polytope V_i let $\underline{\mathbf{v}}_i$ be the midpoint of V_i under the standard Euclidean metric. By assumption $\varphi_{\mathbf{q}}(\underline{\mathbf{v}}_i) \geq L_{\max} \geq \frac{2}{\delta}$, whence the dilation factor of $\mathbf{q}$ is less than or equal to δ, so on the Δ^{th} loop of the algorithm between lines 2 and 11, $\mathbf{q} \in Q$, $\varepsilon = \alpha\frac{2}{\delta}$,

$$\lambda = \left(\frac{\sqrt{C^2 + \frac{4\varepsilon}{n-1}} - C}{2} \right)^2$$

and $V_i = \left\{ \underline{\mathbf{v}}' \in X \;\middle|\; \left|\Re z_j' - \Re z_j\right|, \left|\Im z_j' - \Im z_j\right|, |x'-x| \leq \lambda \right\}$. Therefore by Lemma 4.4.7, $\Phi_{\mathbf{q}}(V_i) \geq L_{\max} - \alpha\frac{2}{\delta} \geq \frac{2}{\delta}(1-\alpha)$ and as such the algorithm terminates on, or before this loop. Call the output of the algorithm L; if the algorithm terminates on the Δ^{th} loop then by the preceding argument the output $L \geq L_{\max} - \alpha\frac{2}{\delta} \geq L_{\max} - \alpha L_{\max} = L_{\max}(1-\alpha)$ and so $\frac{L}{1-\alpha} \geq L_{\max}$ or; if the algorithm terminates on the $(\Delta')^{\text{th}}$ loop where $\Delta' < \Delta$, then $\Delta' \leq \left\lfloor \left(\frac{2}{L_{\max}}\right)^2 \right\rfloor$, put $\delta' = \sqrt{\Delta'}$ so that $L_{\max} \leq \frac{2}{\delta'}$ then on the $(\Delta')^{\text{th}}$ loop the output $L \geq \frac{2}{\delta'}(1-\alpha) \geq L_{\max}(1-\alpha)$. Therefore in either case $\frac{L}{1-\alpha} \geq L_{\max}$. ■

Chapter 5

Computational Improvements

The algorithms described in Chapter 4 for computing Siegel sets are written from the point of view of mathematical clarity, not computational efficiency. This chapter considers modifications to these algorithms that decrease computation time and as such make them practical for implementation.

There is an issue which is not directly connected to the algorithms that introduces a significant inefficiency in the computation;

I. The Siegel container described in Lemma 4.2.6 makes no use of automorphisms in the AM-group $\mathrm{AM}(\mathfrak{O})$. By considering the action of this group, which consists of integral rotations, the volume of the Siegel container can be reduced.

Reducing the size of the Siegel container inputted to Algorithm 4.6.2 will result in a smaller number of convex polytopes to iterate through and smaller bounds on the coordinates of cusps which are effective on the Siegel container.

There are three major inefficiencies in Algorithm 4.5.5 and Algorithm 4.5.6

II. As shall be seen in Section 5.2 there are certain cusps which either *a priori* do not contribute to the construction of Siegel sets, or have actions which are equivalent to those of other cusps; the cusp generation algorithms do not attempt to detect or remove such cusps.

III. The cusp generation algorithms do not attempt to detect and remove cusps which are not effective on the input set.

IV. The bounds on ζ and r such that a cusp of dilation factor δ could be effective on the input set which are given in Corollary 4.4.6 are very loose.

Reducing the size of the set of cusps Q generated by Algorithm 4.5.5 or Algorithm 4.5.6 will decrease the amount of work required to compute $\sup\{\Phi_{\mathbf{q}}(V') \mid \mathbf{q} \in Q\}$ in line 8 of Algorithm 4.6.2. Since this value must be computed for every polytope V, then it is clear that the size of Q is highly correlated to total

computation time.

In Algorithm 4.6.2 the majority of the computation time is spent in the loop

---

6. For each $V \in \Omega$

    8. Assign $L' \leftarrow \sup\{\Phi_{\mathbf{q}}(V') \mid \mathbf{q} \in Q\}$ (where V' is the set of vertices of V)

11. Next

---

and specifically this time is spent on line 8. So far no mention has been made of how $\sup\{\Phi_{\mathbf{q}}(V') \mid \mathbf{q} \in Q\}$ should be computed in practise, although it is clear that the naïve brute force method of computing Phi on each vertex and then taking the infimum over all vertices would be the default option. Given a set cusps Q there are two factors to consider when computing L':

V. The method by which $\Phi_{\mathbf{q}}(V')$ is computed where $\mathbf{q}$ is a cusp and V' is the set of vertices of a convex polytope V.

VI. The sequence in which the cusps $\mathbf{q} \in Q$ are chosen.

There is a major implementation impracticality in Algorithm 4.6.2;

VII. The resolution which is computed analytically based on Lemma 4.4.7, so that the error in the minimum height bound can be quantified, is in general far too large to practically perform computations on.

Decreasing the resolution will decrease the number of convex polytopes to iterate through; however it will reduce the accuracy of the output and make the error bound uncertain since Lemma 4.4.7 will no longer apply. Having said this, from the point of view of computation it is better to have a less accurate output than it is to not get an accurate output; whilst regrettable, it is true that in general computation requires some amount of compromise between the ideal and the feasible.

5.1 An Improved Siegel Container

The Siegel container calculated in Lemma 4.2.6 is a Siegel set for the Heisenberg group $\mathrm{N}(\mathfrak{O})$, it takes no account of the action of rotational automorphisms in $\mathrm{AM}(\mathfrak{O})$, this section improves on the Siegel container by considering the action of certain integral rotations.

Definition 5.1.1 *Let $n \in \mathbb{N}$. Then define*

$$\mathrm{D}_n = \{\mathrm{diag}(\sigma_1, \ldots, \sigma_n) \in \mathrm{GL}_n(\mathbb{Z}) \mid \sigma_i \in \{\pm 1\}\} \qquad \square$$

If $g = \mathrm{diag}(\sigma_1, \ldots, \sigma_n) \in \mathrm{D}_n$, then $g^* g = \mathrm{diag}(|\sigma_1|^2, \ldots, |\sigma_n|^2) = I_n$. Therefore D_n is a subgroup of $\mathrm{U}(n; \mathfrak{O})$.

Lemma 5.1.2 *Let $d \equiv 1 \mod 4$. Then*

$$\mathrm{S}_\infty = \left\{ \underline{\mathbf{v}} \in \overline{\mathbb{H}^n_{\mathbb{C}}} \;\middle|\; \left|\Re_{\underline{z}_i}\right| \leq \frac{1}{2},\ 0 \leq \Im_{\underline{z}_i} \leq \frac{\sqrt{-d}}{4},\ |x| \leq \frac{\sqrt{-d}}{2} \right\}$$

is a Siegel container for Γ.

PROOF Let $\mathrm{S}'_\infty = \left\{ \underline{\mathbf{v}} \in \overline{\mathbb{H}^n_{\mathbb{C}}} \;\middle|\; \left|\Re_{\underline{z}_i}\right| \leq \frac{1}{2},\ \left|\Im_{\underline{z}_i}\right| \leq \frac{\sqrt{-d}}{4},\ |x| \leq \frac{\sqrt{-d}}{2} \right\}$, by Lemma 4.2.6, S'_∞ is a Siegel container for Γ, therefore to prove that S_∞ is a Siegel container for Γ it is sufficient to show that for all $\underline{\mathbf{v}} \in \mathrm{S}'_\infty$ there exists a $\gamma \in \Gamma$ such that $\gamma \circ \underline{\mathbf{v}} \in \mathrm{S}_\infty$. With this aim, let $\underline{\mathbf{v}} \in \mathrm{S}'_\infty$, if $\underline{\mathbf{v}} \in \mathrm{S}_\infty$ then there is nothing to do, so assume otherwise. Let $Z = \left\{ z \in \mathbb{C} \;\middle|\; |\Re z| \leq \frac{1}{2},\ 0 \leq \Im z \leq \frac{\sqrt{-d}}{4} \right\}$, let $\sigma_i = \mathrm{sign}\left(\Im_{\underline{z}_i}\right)$ and put $u = \mathrm{diag}(\sigma_1, \ldots, \sigma_{n-1}) \in \mathrm{D}_{n-1}$ so that $u\underline{z} \in Z^{n-1}$. If $\det u = 1$ then $m(u,1) \in \mathrm{AM}(\mathfrak{O})$ and $m(u,1)\underline{\mathbf{v}} = (u\underline{z}, x, h) \in \mathrm{S}_\infty$, so take $\gamma = m(u,1)$.

Suppose conversely that $\det u = -1$. If $n \equiv 0 \mod 2$, then $\dim u \equiv 1 \mod 2$, hence $\det -u = 1$ so that $m(-u,-1) \in \mathrm{AM}(\mathfrak{O})$ and $m(-u,-1)\underline{\mathbf{v}} = (-(-u)\underline{z}, x, h) = (u\underline{z}, x, h) \in \mathrm{S}_\infty$, so take $\gamma = m(-u,-1)$ and; if $n \equiv 1 \mod 2$, then $n \geq 3$ so $u' = \begin{pmatrix} 1 & & \\ & 1 & \\ & & I_{n-3} \end{pmatrix} \in \mathrm{U}(n-1, \mathfrak{O})$ and $\det u' = -1$. The set Z^{n-1} is stable by the matrix u', i.e. $u'Z^{n-1} = Z^{n-1}$ since u' simply transposes the first two copies of Z^{n-1}, hence $u'u\underline{z} \in Z^{n-1}$ and $\det uu' = 1$ therefore $m(u'u,1) \in \mathrm{AM}(\mathfrak{O})$ and $m(u'u,1)\underline{\mathbf{v}} = (u'u\underline{z}, x, h) \in \mathrm{S}_\infty$ so take $\gamma = m(u'u,1)$. ∎

Lemma 5.1.3 *Let $d \not\equiv 1 \mod 4$ and let $n \in \mathbb{N} - \{3\}$. Then*

$$\mathrm{S}_\infty = \left\{ \underline{\mathbf{v}} \in \overline{\mathbb{H}^n_{\mathbb{C}}} \;\middle|\; \left|\Re_{\underline{z}_1}\right| \leq 1,\ \left|\Re_{\underline{z}_i}\right| \leq \frac{1}{2}\ (i \neq 1),\ 0 \leq \Im_{\underline{z}_i} \leq \frac{\sqrt{-d}}{2},\ |x| \leq \frac{\sqrt{-d}}{2} \right\}$$

is a Siegel container for Γ.

PROOF Let $\mathrm{S}'_\infty = \left\{ \underline{\mathbf{v}} \in \overline{\mathbb{H}^n_{\mathbb{C}}} \;\middle|\; \left|\Re_{\underline{z}_1}\right| \leq 1,\ \left|\Re_{\underline{z}_i}\right| \leq \frac{1}{2}\ (i \neq 1),\ \left|\Im_{\underline{z}_i}\right| \leq \frac{\sqrt{-d}}{2},\ |x| \leq \frac{\sqrt{-d}}{2} \right\}$, by Lemma 4.2.6 S'_∞ is a Siegel container for Γ, therefore to prove that S_∞ is a Siegel container for Γ it is sufficient to show that for all $\underline{\mathbf{v}} \in \mathrm{S}'_\infty$ there exists a $\gamma \in \Gamma$ such that $\gamma \circ \underline{\mathbf{v}} \in \mathrm{S}_\infty$. With this aim, let $\underline{\mathbf{v}} \in \mathrm{S}'_\infty$, if $\underline{\mathbf{v}} \in \mathrm{S}_\infty$ then there is nothing to do, so assume otherwise. Let $Z_1 = \left\{ z \in \mathbb{C} \;\middle|\; |\Re z| \leq \frac{1}{2},\ 0 \leq \Im z \leq \frac{\sqrt{-d}}{2} \right\}$, let $Z = \left\{ z \in \mathbb{C} \;\middle|\; |\Re z| \leq \frac{1}{2},\ 0 \leq \Im z \leq \frac{\sqrt{-d}}{2} \right\}$, let $\sigma_i = \mathrm{sign}\left(\Im_{\underline{z}_i}\right)$ and put $u = \mathrm{diag}(\sigma_1, \ldots, \sigma_{n-1}) \in \mathrm{D}_{n-1}$ so that $u\underline{z} \in Z_1 \times Z^{n-2}$. If $\det u = 1$ then $m(u,1) \in \mathrm{AM}(\mathfrak{O})$ and $m(u,1)\underline{\mathbf{v}} = (u\underline{z}, x, h) \in \mathrm{S}_\infty$, so take $\gamma = m(u,1)$.

Suppose conversely that $\det u = -1$. If $n \equiv 0 \mod 2$, then $\dim u \equiv 1 \mod 2$ hence $\det -u = 1$ so that $m(-u,-1) \in \mathrm{AM}(\mathfrak{O})$ and $m(-u,-1)\underline{\mathbf{v}} = (-(-u)\underline{z}, x, h) = (u\underline{z}, x, h) \in \mathrm{S}_\infty$, so take $\gamma = m(-u,-1)$. If $n \equiv 1 \mod 2$, then $n \geq 5$ so

$$u' = \begin{pmatrix} 1 & & & \\ & 1 & 1 & \\ & & & I_{n-4} \end{pmatrix} \in \mathrm{U}(n-1, \mathfrak{O})$$

and $\det u' = -1$. The set $Z_1 \times Z^{n-2}$ is stable by the matrix u', i.e. $u'(Z_1 \times Z^{n-2}) = Z_1 \times Z^{n-2}$ since u' simply transposes the second and third copies of Z, hence $u'u\underline{z} \in Z_1 \times Z^{n-2}$ and $\det uu' = 1$ therefore $m(u'u,1) \in \mathrm{AM}(\mathfrak{O})$ and $m(u'u,1)\underline{\mathbf{v}} = (u'u\underline{z}, x, h) \in \mathrm{S}_\infty$ so take $\gamma = m(u'u,1)$. ∎

For $d = -1$ or $d = -2$ and $n = 3$, the Siegel container computed in Lemma 4.2.6 must be used as input to Algorithm 4.6.2; the reason a significantly better set does not exists is the lack of symmetry between the sets which in $\underline{z}_1$ and $\underline{z}_2$ lie in these cases. However, when $d = -1$ or $d = -2$ and $n = 3$ the Siegel containers are already computationally manageable, so this is unimportant. In every other case the number of iterations in

the loop between lines 6 and 11 will be reduced by a factor of approximately 2^{n-1} since the measure of the new Siegel container is $\frac{1}{2^{n-1}}^{\text{th}}$ the size of the original Siegel container.

5.2 Non-Primitive Cusps

This section identifies a property exhibited by some cusps called primitivity; testing a cusp for primitivity is computationally fast. Let $X \subset \partial\mathbb{H}_{\mathbb{C}}^{n\times}$ and suppose Q is a set of cusps with the property that $Q \supset \prod_{\Delta=1}^{\Delta'} \mathcal{C}_{\sqrt{\Delta},K}(X)$ for some $\Delta' \in \mathbb{N}$ and suppose that $\mathbf{q} \in Q$ is a cusp with dilation factor δ and $\mathbf{q}$ is not primitive. Then either $\varphi_{\mathbf{q}}(\underline{\mathbf{v}}) \leq 0$ for all $\underline{\mathbf{v}} \in \partial\mathbb{H}_{\mathbb{C}}^{n\times}$ or there exists another cusp $\mathbf{q}' \in Q$ with dilation factor δ' with the three properties; $\mathbf{q}'$ is primitive, $\delta' < \delta$ and $\varphi_{\mathbf{q}}(\underline{\mathbf{v}}) \leq \varphi_{\mathbf{q}'}(\underline{\mathbf{v}})$ for all $\underline{\mathbf{v}} \in \partial\mathbb{H}_{\mathbb{C}}^{n\times}$. Therefore any non-primitive cusp can *a priori* be removed from Q without affecting the combined height raising properties of the cusps in Q.

Definition 5.2.1 (Primitive Cusps) *Suppose that $Cl(K) = 1$, let $\mathbf{q} \in \mathcal{C}_K$ and let $\mathcal{N}(\mathbf{q})$ be the K-norm of the ideal generated by the coordinates of $\mathbf{q}$. Then $\mathbf{q}$ is said to be a primitive cusp whenever $\mathcal{N}(\mathbf{q}) = 1$.* □

Lemma 5.2.2 *Let $\mathbf{q} \in \mathcal{C}_{K,\delta}$ and suppose that $\mathbf{q}$ is not primitive. Then there exists a primitive cusp $\mathbf{q}' \in \mathcal{C}_{K,\delta'}$ such that $\delta > \delta'$ and $\varphi_{\mathbf{q}'}(\underline{\mathbf{v}}) \geq \varphi_{\mathbf{q}}(\underline{\mathbf{v}})$ for all $\underline{\mathbf{v}} \in \partial\mathbb{H}_{\mathbb{C}}^{n\times}$.*

PROOF Since the class number of K is 1, $\mathfrak{O}$ is a principal ideal domain, thus if $\mathcal{N}(\mathbf{q}) \neq 1$, then there exists an element $q \in \mathfrak{O}$ and a vector $\mathbf{q}' \in \mathfrak{O}^{n+1}$ such that $\mathcal{N}(\mathbf{q}') = 1$ and $q\mathbf{q}' = \mathbf{q}$ where $|q|^2 = \mathcal{N}(\mathbf{q}) > 1$. Let β and β' be the rotation factors of $\mathbf{q}$ and $\mathbf{q}'$ respectively. Since $\mathbf{q} = q\mathbf{q}'$ then $\delta\beta = q\delta'\beta'$, whence $\delta' = |\delta'\beta'| = |q|^{-1}\left|q^{-1}\delta\beta\right| = |q|^{-1}\delta$ and therefore $\delta' < \delta$. Put $\tilde{\zeta} = (\delta\beta)^{-1}\zeta$, put $\tilde{r} = r\delta^{-2}$ and suppose that $\varphi_{\mathbf{q}}(\underline{\mathbf{v}}) \geq 0$, then

$$\varphi_{\mathbf{q}}(\underline{\mathbf{v}}) = 2\sqrt{\delta^{-2} - \left(x - \tilde{r} + \Im\left\langle \underline{z}, \tilde{\zeta}\right\rangle_{+}\right)^2} + 2\Re\left\langle \underline{z}, \tilde{\zeta}\right\rangle_{+} - \mathrm{Q}_{+}\left(\tilde{\zeta}\right) - \mathrm{Q}_{+}(\underline{z})$$

$$\varphi_{\mathbf{q}'}(\underline{\mathbf{v}}) = 2\sqrt{|q|^2\delta^{-2} - \left(x - \tilde{r} + \Im\left\langle \underline{z}, \tilde{\zeta}\right\rangle_{+}\right)^2} + 2\Re\left\langle \underline{z}, \tilde{\zeta}\right\rangle_{+} - \mathrm{Q}_{+}\left(\tilde{\zeta}\right) - \mathrm{Q}_{+}(\underline{z})$$

and as such $\varphi_{\mathbf{q}'}(\underline{\mathbf{v}}) \geq \varphi_{\mathbf{q}}(\underline{\mathbf{v}})$. ■

Corollary 5.2.3 *Let $X \subset \partial\mathbb{H}_{\mathbb{C}}^{n\times}$ and suppose Q is a set of cusps with the property that $Q \supset \prod_{\Delta=1}^{\Delta'} \mathcal{C}_{\sqrt{\Delta},K}(X)$ for some $\Delta' \in \mathbb{N}$ and suppose that $\mathbf{q} \in Q$ is a cusp with dilation factor δ and $\mathbf{q}$ is not primitive. Then either $\varphi_{\mathbf{q}}(\underline{\mathbf{v}}) \leq 0$ for all $\underline{\mathbf{v}} \in X$ or there exists another cusp $\mathbf{q}' \in Q$ with dilation factor δ' with the three properties; $\mathbf{q}'$ is primitive, $\delta' < \delta$ and $\varphi_{\mathbf{q}}(\underline{\mathbf{v}}) \leq \varphi_{\mathbf{q}'}(\underline{\mathbf{v}})$ for all $\underline{\mathbf{v}} \in \partial\mathbb{H}_{\mathbb{C}}^{n\times}$.*

PROOF Suppose that $\varphi_{\mathbf{q}}(\underline{\mathbf{v}}') > 0$ for some $\underline{\mathbf{v}}' \in X$, then by Lemma 5.2.2 there exists a primitive cusps $\mathbf{q}' \in \mathcal{C}_{K,\delta'}$ such that $\delta' < \delta$ and $\varphi_{\mathbf{q}}(\underline{\mathbf{v}}) \leq \varphi_{\mathbf{q}'}(\underline{\mathbf{v}})$ for all $\underline{\mathbf{v}} \in \partial\mathbb{H}_{\mathbb{C}}^{n\times}$ and therefore $\varphi_{\mathbf{q}'}(\underline{\mathbf{v}}') > 0$ whence $\mathbf{q}' \in Q$■

In order to detect non-primitive cusps it is necessary to compute the norm of the ideal generated by the coordinates of $\mathbf{q}$; this is accomplished in practise by using the theory in [Coh00, 5.2] to represent ideals and perform computations on them.

5.3 Equivalent Cusps

Another class of cusps which are *a priori* unnecessary in Siegel set construction are equivalent cusps. The notion of equivalence arises from the original projective definition of complex hyperbolic space; when constructing the ball and hyperquadric models of $\mathbb{H}^n_{\mathbb{C}}$ a unique representative of each projective point is chosen. However, there is no such uniqueness property in the definition of a cusp, thus cusps which differ only by a unit are in fact the same cusp and as such act identically on $\mathbb{H}^n_{\mathbb{C}}$. This section considers how to detect equivalent cusps and how to safely eliminate them during cusp construction; it is shown that equivalent cusps can be removed at the point at which the rotation factor of the cusps is computed.

Definition 5.3.1 (Equivalent Cusps) *Let $\mathbf{q}, \mathbf{q}' \in C_K$ and suppose that there exists an integral unit $u \in \mathfrak{O}^*$ such that $\mathbf{q} = u\mathbf{q}'$. Then $\mathbf{q}$ and $\mathbf{q}'$ are said to be equivalent.* □

Lemma 5.3.2 *Let $\mathbf{q}, \mathbf{q}' \in C_K$ be equivalent cusps. Then $\mathbf{q}$ and $\mathbf{q}'$ have the same dilation factor and $\varphi_{\mathbf{q}}(\underline{\mathbf{v}}) = \varphi_{\mathbf{q}'}(\underline{\mathbf{v}})$ for all $\underline{\mathbf{v}} \in \partial\mathbb{H}^{n\,\times}_{\mathbb{C}}$.*

PROOF Let δ, β and δ', β' be the dilation and rotation factors of $\mathbf{q}$ and $\mathbf{q}'$ respectively, then by definition $\delta\beta = u\delta'\beta'$; taking the absolute value of this equality gives $\delta = |\delta\beta| = |u\delta'\beta'| = \delta'$ Since $\mathbf{q}$ and $\mathbf{q}'$ are equivalent cusps so that there exists an integral unit $u \in \mathfrak{O}^*$ such that $\mathbf{q} = u\mathbf{q}'$. Put $\tilde{\zeta} = (\delta\beta)^{-1}\zeta$, put $\tilde{r} = r\delta^{-2}$ and suppose that $\varphi_{\mathbf{q}}(\underline{\mathbf{v}}) \geq 0$, then

$$\varphi_{\mathbf{q}}(\underline{\mathbf{v}}) = 2\sqrt{\delta^{-2} - \left(x - \tilde{r} + \Im\left\langle \underline{z}, \tilde{\zeta}\right\rangle_{+}\right)^2} + 2\Re\left\langle \underline{z}, \tilde{\zeta}\right\rangle_{+} - \mathrm{Q}_{+}\left(\tilde{\zeta}\right) - \mathrm{Q}_{+}(\underline{z})$$
$$\varphi_{\mathbf{q}'}(\underline{\mathbf{v}}) = 2\sqrt{|u|^2\,\delta^{-2} - \left(x - \tilde{r} + \Im\left\langle \underline{z}, \tilde{\zeta}\right\rangle_{+}\right)^2} + 2\Re\left\langle \underline{z}, \tilde{\zeta}\right\rangle_{+} - \mathrm{Q}_{+}\left(\tilde{\zeta}\right) - \mathrm{Q}_{+}(\underline{z})$$

and since $|u|^2 = 1$, then $\varphi_{\mathbf{q}'}(\underline{\mathbf{v}}) = \varphi_{\mathbf{q}}(\underline{\mathbf{v}})$. ■

Lemma 5.3.3 *Let $X \subset \partial\mathbb{H}^{n\,\times}_{\mathbb{C}}$, let $Q = C_{K,\delta}(X) \cap \{\mathbf{q} \mid \mathbf{q} \text{ is primitive}\}$, let $\beta \in \mathbb{C}$ be a rotation factor, let $Q_\beta = \{\mathbf{q} \in Q \mid \mathbf{q} \text{ has rotation factor } \beta\}$ and put*

$$Q_\beta^{\perp} = \bigcup_{u \in \mathfrak{O}^* - \{1\}} Q_{u\beta}$$

Then for all $\mathbf{q} \in Q_\beta^{\perp}$, there exists an equivalent cusp $\mathbf{q}' \in Q_\beta$.

PROOF Let $\mathbf{q} \in Q_\beta^{\perp}$, then the rotation factor of $\mathbf{q}$ is $u\beta$ for some $u \in \mathfrak{O}^*$. Let $\mathbf{q}' = u^{-1}\mathbf{q}$ so that $\mathbf{q}'$ is equivalent to $\mathbf{q}$. Since $\mathbf{q}$ is primitive then $\mathcal{N}(\mathbf{q}') = \mathcal{N}\left(u^{-1}\mathbf{q}\right) = 1$, so $\mathbf{q}'$ is also primitive, thus by Lemma 5.3.2 $\mathbf{q}' \in Q$. As the rotation factor of $\mathbf{q}'$ is β then $\mathbf{q}' \in Q_\beta$. ■

The preceding lemma implies equivalence is a property which can be detected at the rotation factor of cusps when certain effectiveness properties of the cusps in a set are assumed. The following algorithm applies this logic to remove equivalent cusps at the point at which the rotation factor of a cusp is calculated during cusp generation.

Algorithm 5.3.4 (Improved β values)

Inputs: d a Heegner number, $B \subset \{\beta \in \mathbb{C} \mid |\beta| = 1\}$.

1. Assign $\mathfrak{O}^* \leftarrow \{1,-1\}$, $B' \leftarrow \emptyset$.
2. If $d = -1$ then $\mathfrak{O}^* \leftarrow \mathfrak{O}^* \cup \{\imath, -\imath\}$
3. If $d = -3$ then $\mathfrak{O}^* \leftarrow \mathfrak{O}^* \cup \left\{ \frac{1+\sqrt{-3}}{2}, \frac{1-\sqrt{-3}}{2}, \frac{-1+\sqrt{-3}}{2}, \frac{-1-\sqrt{-3}}{2} \right\}$
4. For each $\beta \in B$
    5. For each $u \in \mathfrak{O}^*$
        6. If $u\beta \in B'$ goto 4
    7. Next
    8. Assign $B' \leftarrow B' \cup \{\beta\}$
9. Next
10. Return B'

Lemma 5.3.5 *Let $\delta \in \mathbb{R}^{>0}$ such that $\Delta = \delta^2 \in \mathbb{N}$ and let $B_\delta =$ Algorithm 5.4.8(d,B) where*

$$B = \begin{cases} \left\{ \frac{a+b\sqrt{d}}{\delta} \in \mathbb{C} \;\middle|\; a,b \in \mathbb{Z} \text{ s.t. } a^2 - db^2 = \Delta \right\} & \text{if } d \not\equiv 1 \mod 4 \\ \left\{ \frac{a+b\sqrt{d}}{2\delta} \in \mathbb{C} \;\middle|\; a,b \in \mathbb{Z} \text{ s.t. } a^2 - db^2 = 4\Delta \right\} & \text{if } d \equiv 1 \mod 4 \end{cases}$$

Then $u\beta \in B_\delta$, for some $u \in \mathfrak{O}^*$.

PROOF Let β' be the rotation factor of $\mathbf{q}$, if $\beta' \in B_\delta$ there is nothing to do, so assume that $\beta' \notin B_\delta$. On line of 4 Algorithm 5.3.4 every element of B is iterated over, so at some stage line 5 is reached with $\beta = \beta'$. All elements $u \in \mathfrak{O}^*$ are now iterated over. On line 6 if there exists a u such that $u\beta_{\mathbf{q}} \in B'$ then β is incremented to the next value in B and β' is not added to B', if not then line 8 is reached and β' is added to B'. By assumption $\beta' \notin B$ so there is a unit $u \in \mathfrak{O}^*$ such that $u\beta \in B'$ and $B_\delta = B'$. ∎

5.4 Improved Bounds on ζ and r

Let $\underline{\mathbf{v}} \in \partial\mathbb{H}^n_{\mathbb{C}}{}^{\times}$, let $\delta \in \mathbb{R}$, let $\mathbf{q} \in \mathcal{C}_{K,\delta}$ and fix the rotation factor of $\mathbf{q}$, then Corollary 4.4.6 gives bounds on the zeta and r factors of $\mathbf{q}$ such that whenever they are satisfied $\mathrm{e}_{\mathbf{q}}(\underline{\mathbf{v}}) \geq 1$, or equivalently $\varphi_{\mathbf{q}}(\underline{\mathbf{v}}) \leq 0$. Given a set $X \subset \partial\mathbb{H}^n_{\mathbb{C}}{}^{\times}$, a dilation factor, a dimension and a ring of integers Algorithm 4.5.5 and Algorithm 4.5.6 use these bounds to construct a set of cusps $Q_\delta \supseteq \mathcal{C}_{K,\delta}(X)$. However, these bounds are very loose, so Q_δ will in general contain a high percentage of cusps which are not effective on X; the non-effective cusps in Q_δ cause significant inefficiencies in terms of both storage and computation time. This section presents a method of improving on these bounds.

Lemma 5.4.1 *Let $\mathbf{q} \in \mathcal{C}_K(X)$, let $\underline{\mathbf{v}} \in \partial\mathbb{H}^n_{\mathbb{C}}{}^{\times}$ and suppose that*

$$\frac{1}{4} \left| \mathrm{Q}_+ (\zeta - \delta\beta_{\underline{z}}) \right|^2 + \left| \delta^2 x - r + \Im \langle \delta\beta_{\underline{z}}, \zeta \rangle_+ \right|^2 \geq \delta^2 \tag{5.1}$$

Then $\mathbf{q} \notin \mathcal{C}_{K,\delta}(X)$.

PROOF By definition it is necessary to show that if $\mathrm{e}_{\mathbf{q}}(\underline{\mathbf{v}}) \geq 1$ then (5.1) is satisfied, so consider the effect function of $\underline{\mathbf{v}}$ at $\mathbf{q}$

$$\begin{aligned}
\mathrm{e}_{\mathbf{q}}(\mathbf{v}) &= |\langle \underline{\mathbf{v}}, \mathbf{q} \rangle|^2 \\
&= \left| \begin{pmatrix} \delta\overline{\beta} & \zeta^* & \frac{\overline{\beta}}{\delta}\left(\frac{-\mathrm{Q}_+(\zeta)}{2} - \imath r\right) \end{pmatrix} H_n \begin{pmatrix} 1 \\ \underline{z} \\ \frac{-\mathrm{Q}_+(\underline{z})}{2} + \imath x \end{pmatrix} \right|^2 \\
&= \left| -\frac{\overline{\beta}}{\delta}\left(\frac{\mathrm{Q}_+(\zeta)}{2} + \imath r\right) + \langle \underline{z}, \zeta \rangle_+ + \delta\overline{\beta}\left(\frac{-\mathrm{Q}_+(\underline{z})}{2} + \imath x\right) \right|^2 \\
&= \delta^{-2} \left| \frac{-\mathrm{Q}_+(\zeta) + 2\delta\beta\langle \underline{z}, \zeta \rangle_+ - \delta^2(\mathrm{Q}_+(\underline{z}))}{2} + \imath(\delta^2 x - r) \right|^2 \\
&= \frac{1}{4\delta^2} \left| -\mathrm{Q}_+(\zeta) + 2\Re\langle \delta\beta\underline{z}, \zeta \rangle_+ - \mathrm{Q}_+(\delta\beta\underline{z}) \right|^2 + \frac{1}{\delta^2} \left| \delta^2 x - r + \Im\langle \delta\beta\underline{z}, \zeta \rangle_+ \right|^2 \\
&= \frac{1}{4\delta^2} |\mathrm{Q}_+(\zeta - \delta\beta\underline{z})|^2 + \frac{1}{\delta^2} \left| \delta^2 x - r + \Im\langle \delta\beta\underline{z}, \zeta \rangle_+ \right|^2
\end{aligned}$$

Hence if $\mathrm{e}_{\mathbf{q}}(\underline{\mathbf{v}}) \geq 1$ then (5.1) holds. ∎

Improved Bounds on ζ

Firstly the bounds on ζ are considered; the modification made to this section of the algorithm is probably the most complicated change which is made to the algorithm. The idea is that a lattice is constructed in $\mathfrak{O}^{n-1}$ which contains all valid zeta values and then this lattice is iterated through; the complication arises because the lattice changes during the iteration. The outer coordinates are assumed to be fixed and then the bounds on the inner coordinates are based on the values of the outer coordinates; each time the outer coordinates change the bounds on the inner coordinates need to be recomputed and as such the lattice changes.

Lemma 5.4.2 *Let $\mathbf{q} \in \mathcal{C}_K$, let $\underline{\mathbf{v}} \in \partial\mathbb{H}_{\mathbb{C}}^{n\times}$ and suppose that*

$$\sum \left| (\delta\beta)^{-1}\zeta_i - \underline{z}_i \right|^2 \geq 2\delta^{-1}$$

Then $\mathbf{q} \notin \mathcal{C}_K(X)$.

PROOF By Lemma 5.4.1, if $|\mathrm{Q}_+(\zeta - \delta\beta\underline{z})|^2 \geq 4\delta^2$ then $\varphi_{\mathbf{q}}(\underline{\mathbf{v}}) \leq 0$. The quadratic form $\mathrm{Q}_+(-)$ is positive definite and $\delta > 0$, so squareroots can be taken, thus this is equivalent to the inequality $2\delta \leq \mathrm{Q}_+(\zeta - \delta\beta\underline{z}) = \sum \left| \zeta_i - \delta\beta\underline{z}_i \right|^2$, dividing out by $|\delta\beta|^2$ completes the result. ∎

This Lemma implies the following Corollary which shows that the coordinates can be bounded incrementally, starting with the $(n-1)^{\text{th}}$ and ending with the first.

Corollary 5.4.3 *Let $\mathbf{q} \in \mathcal{C}_K$, let $\underline{\mathbf{v}} \in \partial\mathbb{H}_{\mathbb{C}}^{n\times}$, let $i \in \{1, \ldots n-1\}$ and suppose that*

$$\left| (\delta\beta)^{-1}\zeta_i - \underline{z}_i \right| \geq \sqrt{\max\left\{0, 2\delta^{-1} - \sum_{j=i+1}^{n-1} \left| (\delta\beta)^{-1}\zeta_j - \underline{z}_j \right|^2\right\}}$$

Then $\mathbf{q} \notin \mathcal{C}_K(X)$.

PROOF By Lemma 5.4.2, if $\left|(\delta\beta)^{-1}\zeta_i - \underline{z}_i\right|^2 \geq 2\delta^{-1} - \sum_{j\neq i}^{n-1}\left|(\delta\beta)^{-1}\zeta_j - \underline{z}_j\right|^2$ then $\varphi_{\mathbf{q}}(\underline{\mathbf{v}}) \leq 0$ and since $2\delta^{-1} - \sum_{j\neq i}^{n-1}\left|(\delta\beta)^{-1}\zeta_j - \underline{z}_j\right|^2 \geq 2\delta^{-1} - \sum_{j=i+1}^{n-1}\left|(\delta\beta)^{-1}\zeta_j - \underline{z}_j\right|^2$ the result follows. ∎

For the remainder of this chapter assume the following situation: for each $i \in \{1,\ldots n-1\}$ let $Y_i, W_i \subset \mathbb{R}$ be closed intervals, write $Z_i = W_i \times \imath Y_i \subset \mathbb{C}$ and put $Z = \prod Z_i$, let $R \in \mathbb{R}$ be a closed interval, put

$$X = Z \times R \subset \partial\mathbb{H}^{n\,\times}_{\mathbb{C}}$$

and suppose that the dilation factor δ and the rotation factor β of the cusp $\mathbf{q}$ are fixed.

Lemma 5.4.4 *Let $i \in \{1,\ldots n-1\}$, assume that the final $n-i-1$ coordinates of ζ, the zeta factor of $\mathbf{q}$, are fixed, let*

$$C_{(\zeta_{i+1},\ldots,\zeta_{n-1})} = \sqrt{\max\left\{0, 2\delta^{-1} - \sum_{j=i+1}^{n-1}\inf\left\{\left|(\delta\beta)^{-1}\zeta_j - z\right|^2 \;\middle|\; z \in Z_j\right\}\right\}}$$

$$\Lambda_{(\zeta_{i+1},\ldots,\zeta_{n-1})} = \left\{\delta\beta z \in \mathfrak{O} \;\middle|\; z \in \mathbb{C}, z' \in Z_i \text{ and } \left|z - z'\right| < C_{(\zeta_{j+1},\ldots,\zeta_{n-1})}\right\}$$

and suppose that $\zeta_i \notin \Lambda_{(\zeta_{i+1},\ldots,\zeta_{n-1})}$. Then $\mathbf{q} \notin \mathcal{C}_{K,\delta}(X)$.

PROOF Suppose $\zeta_i \notin \Lambda_{(\zeta_{i+1},\ldots,\zeta_{n-1})}$, so that by definition $\left|(\delta\beta)^{-1}\zeta_i - z\right| \geq C_{(\zeta_{i+1},\ldots,\zeta_{n-1})}$ for all $z \in Z_i$, thus by Corollary 5.4.3, $\mathbf{q} \notin \mathcal{C}_{K,\delta}(X)$. ∎

Corollary 5.4.5 *With the same set up as Lemma 5.4.4, suppose that $\mathbf{q} \in \mathcal{C}_{K,\delta}(X)$. Then for $i \in \{1,\ldots n-1\}$, $\zeta_i \in \Lambda_{(\zeta_{i+1},\ldots,\zeta_{n-1})}$.*

Corollary 5.4.6 *The $\Lambda_{(*)}$ lattices in Corollary 5.4.5 are finite.*

PROOF The sets Z_i are compact and $\mathfrak{O}$ is discrete. ∎

There are two distinct phases involved in iterating through the zeta lattices; the construction / reconstruction of the lattices and the actual iteration itself; Algorithm 5.4.7 deals with the construction / reconstruction phase and Algorithm 5.4.8 deals with the iteration phase. The outer most lattice, the $n-1$ lattice, never changes, every other lattice is recomputed every time the iterand reaches the end of that lattice, the next outer lattice is incremented and that lattice returns to the beginning.

Algorithm 5.4.7 (Zeta Lattices)

Inputs: $\delta \in \mathbb{R}$, $\beta \in \mathbb{C}$, $n \in \mathbb{N}$, an imaginary quadratic ring of integers $\mathfrak{O}$, $i \in \{1,\ldots n-2\}$, sets $Z_j \subset \mathbb{C}$ for $j = 1,\ldots,n-2$, zeta values $\zeta_k \in \mathfrak{O}$ for $k = i+1,\ldots,n-1$.

1. While $i \geq 1$

   2. Assign $C_{(\zeta_{i+1},\ldots,\zeta_{n-1})} \leftarrow \sqrt{\max\left\{0, 2\delta^{-1} - \sum_{k=i+1}^{n-1}\inf\left\{\left|(\delta\beta)^{-1}\zeta_k - z\right|^2 \;\middle|\; z \in Z_k\right\}\right\}}$
   3. Assign $\Lambda_{(\zeta_{i+1},\ldots,\zeta_{n-1})} \leftarrow \left\{\delta\beta z \in \mathfrak{O} \;\middle|\; z \in \mathbb{C}, z' \in Z_i \text{ and } \left|z - z'\right| < C_{(\zeta_{i+1},\ldots,\zeta_{n-1})}\right\}$
   4. If $\Lambda_{(\zeta_{i+1},\ldots,\zeta_{n-1})} = \emptyset$ then assign $\Lambda_{(\zeta_{i+1},\ldots,\zeta_{n-1})} \leftarrow \{0\}$

5. Assign ζ_i to the first element in $\Lambda_{(\zeta_{i+1},\ldots,\zeta_{n-1})}$
6. Assign $i \leftarrow i-1$

7. End While

8. Return $\left\{\Lambda_{(\zeta_1,\ldots,\zeta_{n-1})},\ldots,\Lambda_{(\zeta_{n-1})},\zeta_1,\ldots,\zeta_{n-1}\right\}$

In line 4 the degenerate case where $\Lambda_{(\zeta_{i+1},\ldots,\zeta_{n-1})}$ is empty is dealt with; in this case there are *a priori* no valid cusps that will be generated until ζ_{i+1} is incremented and in practise something more intelligent than adding a redundant point to $\Lambda_{(\zeta_{i+1},\ldots,\zeta_{n-1})}$ should be done. However, doing something more intelligent obfuscates the core idea behind the algorithm, which is to create a set of lattices which will generate all useful cusps. As such a naïve approach is adopted here.

Algorithm 5.4.8 (Improved ζ Values)

Inputs: d a Heegner number, $n \in \mathbb{N}-\{1\}$, $\delta \in \mathbb{R}$, $\beta \in \mathbb{C}$, sets $Z \subset \mathbb{C}^{n-1}$.

1. Initialise $Z'_{\delta,\beta} \leftarrow \emptyset$, $C \leftarrow \sqrt{2\delta^{-1}}$, $\Lambda_{()} \leftarrow \{\delta\beta z \in \mathfrak{O} \mid z \in \mathbb{C}, z' \in Z_i \text{ and } |z-z'|<C\}$, $\zeta_{n-1} \leftarrow$ the first element in $\Lambda_{()}$, $i \leftarrow n-2$
2. If $\Lambda_{()} = \emptyset$ then return $Z'_{\delta,\beta}$
3. Compute $\Lambda_{(\zeta_2,\ldots,\zeta_{n-1})},\ldots,\Lambda_{(\zeta_{i+1},\ldots,\zeta_{n-1})}$ and $\zeta_1,\ldots,\zeta_i$ using Algorithm 5.4.7 with inputs δ, β, Z_j for $j=1,\ldots,i$, L, the current value of i and $\zeta_{i+1},\ldots,\zeta_{n-1}$.
4. Assign $C_r \leftarrow 2\delta^{-1} - \sum_{k=1}^{n-1} \inf\left\{ \left| (\delta\beta)^{-1}\zeta_k - z \right|^2 \;\middle|\; z \in Z_k \right\}$
5. If $C_r \geq 0$ then assign $\zeta \leftarrow (\zeta_1,\ldots,\zeta_{n-1})$ and assign $Z'_{\delta,\beta} \leftarrow Z'_{\delta,\beta} \cup \{\zeta\}$
6. Assign $i \leftarrow 1$
7. Next $\zeta_i \in \Lambda_{(\zeta_{i+1},\ldots,\zeta_{n-1})}$
   8. If $i = 1$ then
      9. Assign $C_r \leftarrow 2\delta^{-1} - \sum_{k=1}^{n-1} \inf\left\{ \left| (\delta\beta)^{-1}\zeta_k - z \right|^2 \;\middle|\; z \in Z_k \right\}$
      10. If $C_r \geq 0$ then assign $\zeta \leftarrow (\zeta_1,\ldots,\zeta_{n-1})$ and assign $Z'_{\delta,\beta} \leftarrow Z'_{\delta,\beta} \cup \{\zeta\}$
   11. Else
      12. Assign $i \leftarrow i-1$
      13. Goto 3
14. End Next
15. If $i = n-1$ then
   16. Return $Z'_{\delta,\beta}$
17. Else

18. Assign $i \leftarrow i+1$

19. Goto 7

There are two points to make about these algorithms.

1. Computing $\inf\left\{ \left| (\delta\beta)^{-1}\zeta_i - z \right|^2 \;\middle|\; z \in Z_i \right\}$ is straightforward. The sets Z_i are of the form $Z_i = W_i \times \imath Y_i$ where $W_i, Y_i \in \mathbb{R}$ are intervals. Let $w_i \in W_i$ be the element such that $\left| (\delta\beta)^{-1}\zeta_i - w_i \right|$ is minimal and let $y_i \in Y_i$ be the element such that $\left| (\delta\beta)^{-1}\zeta_i - y_i \right|$ is minimal. Then

$$\inf\left\{ \left| (\delta\beta)^{-1}\zeta_i - z \right|^2 \;\middle|\; z \in Z_i \right\} = \left| \Re(\delta\beta)^{-1}\zeta_i - w_i \right|^2 + \left| \Im(\delta\beta)^{-1}\zeta_i - y_i \right|^2$$

   If $\Re(\delta\beta)^{-1}\zeta_i \in W_i$, then $w_i = \Re(\delta\beta)^{-1}\zeta_i$, if $\Re(\delta\beta)^{-1}\zeta_i < \inf W_i$ then $w_i = \inf W_i$ and if $\Re(\delta\beta)^{-1}\zeta_i > \sup W_i$ then $w_i = \sup W_i$. The same goes for $\Im(\delta\beta)^{-1}\zeta_i$ and y_i.

2. The $\Lambda(*)$ lattices which are constructed on line 4 of Algorithm 5.4.7 and line 1 of Algorithm 5.4.8 are not complicated from a theoretical point of view however, from the point of view of implementation they are not trivial. In the C++ implementation of the algorithm first the set

$$Z_i' = \left\{ z \in \mathbb{C} \;\middle|\; z' \in Z_i \text{ and } \left| z - z' \right| < C_{(*)} \right\}$$

   is constructed; these sets are all rectangular. Then the smallest rectangular set Z_i'' which contains $\delta\beta Z_i'$ is computed; since multiplication by a constant preserves convexity this is achieved simply by considering the action $\delta\beta$ on the vertices of Z_i'. Finally the lattice $\Lambda_{(*)}$ is constructed on the fly by iterating through all of the elements of $\mathfrak{O}$ which lie inside Z_i''; this lattice $\Lambda_{(*)}$ contains the $\Lambda_{(*)}$ in the algorithms above, but is in general bigger.

Lemma 5.4.9 *Let* $\mathbf{q} \in \mathcal{C}_{K,\delta}$ *and let* $Z_{\delta,\beta} =$ *Algorithm* 5.4.8(d,n,δ,β,Z). *Then* $\zeta \in Z_{\delta,\beta}$

PROOF Let $\mathbf{q} \in \mathcal{C}_{K,\delta}(X)$ and suppose that the rotation factor of $\mathbf{q}$ is β and the zeta factor of $\mathbf{q}$ is ζ'. By Corollary 5.4.5, $\zeta'_{n-1} \in \Lambda_{()}$ as generated on line 1 of the algorithm and by assumption $\Lambda_{()} \neq \emptyset$, thus line 3 is executed. Starting with $i = n-1$ the lattice $\Lambda_{(\zeta_{i+1},\ldots,\zeta_{n-1})}$ is computed and ζ_i is set to the first element in this lattice, whence i is decremented and this process is repeated until $i = 0$. On lines 4 and 5 the very first element in this lattice is checked for inclusion in $Z'_{\delta,\beta}$ using Lemma 5.4.2; on line 6 i is set to 1 and then between lines 7 and 14 ζ_1 is iterated through the lattice $\Lambda_{(\zeta_2,\ldots,\zeta_{n-1})}$; on each loop the element $\zeta = (\zeta_1,\ldots,\zeta_{n-1})$ is checked for inclusion in $Z'_{\delta,\beta}$ using Lemma 5.4.2. When the end of this lattice is reached; if $n = 2$ then the algorithm terminates; in this case since $\Lambda_{()} = \Lambda_{(\zeta_2,\ldots,\zeta_{n-1})}$ and $\zeta'_{n-1} \in \Lambda_{()}$ then ζ'_{n-1} is one of the ζ_1s and by Lemma 5.4.2 the element ζ'_{n-1} passes the tests on lines 9 and 10, thus $\zeta' \in Z'_{\delta,\beta}$. So assume that $n > 2$.

In this case on reaching line 17, i is set to 2 and the algorithm jumps to line 7 where ζ_2 is incremented to the next element in $\Lambda_{(\zeta_3,\ldots,\zeta_{n-1})}$. On line 11 the index i is set back to 1 and the algorithm returns to line 3 where the lattice $\Lambda_{(\zeta_2,\ldots,\zeta_{n-1})}$ is recomputed based on the new value of ζ_2 and ζ_1 is set to the first element in the new lattice $\Lambda_{(\zeta_2,\ldots,\zeta_{n-1})}$. Again on lines 4 and 5 the very first element in this lattice is checked for inclusion in $Z'_{\delta,\beta}$ using Lemma 5.4.2; on line 6 i is set to 1 and then between lines 7 and 14 ζ_1 is iterated through the new lattice $\Lambda_{(\zeta_2,\ldots,\zeta_{n-1})}$. This process is repeated until the ζ_2 reaches the end of $\Lambda_{(\zeta_3,\ldots,\zeta_{n-1})}$

whence at line 15 the algorithm either terminates or on line 18 i is set to 3, the algorithm jumps to line 7 and ζ_3 is incremented to the next value in $\Lambda_{(\zeta_4,\ldots,\zeta_{n-1})}$. Then on line 12 i is decremented to 2 and the algorithm jumps to line 3. On line 3 $\Lambda_{(\zeta_3,\ldots,\zeta_{n-1})}$ is recomputed to take account of the new value of ζ_3, ζ_2 is set to the first element in $\Lambda_{(\zeta_3,\ldots,\zeta_{n-1})}$, whence $\Lambda_{(\zeta_2,\ldots,\zeta_{n-1})}$ is recomputed to take account of the new values of ζ_3 and ζ_2; ζ_1 is now set to the first element in $\Lambda_{(\zeta_2,\ldots,\zeta_{n-1})}$ and the process begins anew on line 4.

The algorithm continues in this manner: $\Lambda_{(\zeta_{i+1},\ldots,\zeta_{n-1})}$ lattice is reached, on line 15 the algorithm either terminates or, on line 18 the index i is incremented to $i+1$, the algorithm jumps to line 7 where ζ_{i+1} is incremented to the next value in $\Lambda_{(\zeta_{i+2},\ldots,\zeta_{n-1})}$, then on line 12 the index i is decremented to $i-1$ and the algorithm jumps to line 3. On line 3 the lattice $\Lambda_{(\zeta_{i+1},\ldots,\zeta_{n-1})}$ is recomputed to take account of the new value of ζ_{i+1} and ζ_i is set to the first element in this new lattice, whence i is decremented to $i-1$ and this process is repeated until $i=0$. On lines 4 and 5 the very first element in this lattice is checked for inclusion in $Z'_{\delta,\beta}$ and then the process once again begins anew on line 4.

Thus at some stage in the algorithm ζ_{n-1} is set to ζ'_{n-1} and $\Lambda_{(\zeta_{n-1})}=\Lambda_{(\zeta'_{n-1})}$, but then by Corollary 5.4.5 $\zeta'_{n-2}\in\Lambda_{(\zeta_{n-1})}$ and as such at some stage, when $\zeta_{n-1}=\zeta'_{n-1}$, then also $\zeta_{n-2}=\zeta'_{n-2}$ and $\Lambda_{(\zeta_{n-2},\zeta_{n-1})}=\Lambda_{(\zeta'_{n-2},\zeta'_{n-1})}$. Thus inductively, at some stage in the algorithm for $i=1,\ldots n-1$, the variables $\zeta_i=\zeta'_i$ simultaneously and as such $\zeta=\zeta'$. Necessarily, since $\mathbf{q}\in\mathcal{C}_{K,\delta}(X)$ then the ζ'_i pass the checks on lines 9 and 10 and as such $\zeta'\in Z'_{\delta,\beta}$. ∎

Improved Bounds on r

The procedure for computing r changes little from before, however now the bounds are tighter; this section presents an updated algorithm for computing r more efficiently.

Lemma 5.4.10 *Let $\mathbf{q}\in\mathcal{C}_K$ and suppose that either*

$$\inf\left\{\frac{1}{4}\left|\mathrm{Q}_+\left(\zeta-\delta\beta\underline{z}\right)\right|^2\;\middle|\;\underline{z}\in Z\right\}>\delta^2$$

or

$$\inf\left\{\left|r-\delta^2x-\Im\left\langle\delta\beta\underline{z},\zeta\right\rangle_+\right|\;\middle|\;\underline{z}\in Z,\;x\in R\right\}\geq\sup\left\{\sqrt{\delta^2-\frac{1}{4}\left|\mathrm{Q}_+\left(\zeta-\delta\beta\underline{z}\right)\right|^2}\;\middle|\;\underline{z}\in Z\right\}$$

Then $\mathbf{q}\notin\mathcal{C}_{K,\delta}(X)$.

PROOF Immediate from Lemma 5.4.1. ∎

Algorithm 5.4.11 (Improved R Values)

Inputs: $n\in\mathbb{N}$, $\delta\in\mathbb{R}$, $\beta\in\mathbb{C}$, an imaginary quadratic ring of integers $\mathfrak{O}$, $\zeta\in\mathfrak{O}^{n-1}$, a set $Z\subset\mathbb{C}^{n-1}$, a set $R\in\mathbb{R}$. Note that $a=\Re\delta\beta$, $b=\Im\delta\beta$ if $d\not\equiv 1 \mod 4$ and $a=2\Re\delta\beta$, $b=2\Im\delta\beta$ if $d\equiv 1 \mod 4$.

1. Initialise $C_r\leftarrow\inf\left\{\frac{1}{4}\left|\mathrm{Q}_+\left(\zeta-\delta\beta\underline{z}\right)\right|^2\;\middle|\;\underline{z}\in Z\right\}$
2. Initialise $r_{\min}=\inf\left\{\delta^2x+\Im\left\langle\delta\beta\underline{z},\zeta\right\rangle_+\;\middle|\;x\in R\text{ and }\underline{z}\in Z\right\}$
3. Initialise $r_{\max}=\sup\left\{\delta^2x+\Im\left\langle\delta\beta\underline{z},\zeta\right\rangle_+\;\middle|\;x\in R\text{ and }\underline{z}\in Z\right\}$

4. If $d \not\equiv 1 \mod 4$ then

   5. Assign

$$R'_{\delta,\beta,\zeta} \leftarrow \left\{ r \in \mathbb{R} \;\middle|\; \begin{array}{l} \sqrt{\delta^2 - C_r} - r_{\max} < r < \sqrt{\delta^2 - C_r} - r_{\min},\ r = r'\sqrt{-d} \text{ where } r' \in \mathbb{Z} \text{ s.t.} \\ 2bd\,r' \equiv \mathrm{Q}_+(\zeta)\,a \mod 2\Delta \text{ and } 2a\,r' \equiv \mathrm{Q}_+(\zeta)\,b \mod 2\Delta \end{array} \right\}$$

6. Else

   7. Assign

$$R'_{\delta,\beta,\zeta} \leftarrow \left\{ r \in \mathbb{R} \;\middle|\; \begin{array}{l} \sqrt{\delta^2 - C_r} - r_{\max} < r < \sqrt{\delta^2 - C_r} - r_{\min},\ r = \frac{r'\sqrt{-d}}{2} \text{ where } r' \in \mathbb{Z} \text{ s.t.} \\ bd\,r' \equiv \mathrm{Q}_+(\zeta)\,a \mod 2\Delta,\ a\,r' \equiv \mathrm{Q}_+(\zeta)\,b \mod 2\Delta \text{ and} \\ (a+bd)\,r' \equiv \mathrm{Q}_+(\zeta)\,(b+a) \mod 4\Delta \end{array} \right\}$$

8. Return $R_{\delta,\beta,\zeta}$

There are two points to make about this algorithms.

1. The constant $C_r = \inf\left\{ \frac{1}{4}\,|\,\mathrm{Q}_+(\zeta - \delta\beta\underline{z})\,|^2 \;\middle|\; \underline{z} \in Z \right\}$ can be computed in the same way that the constants $C_{(*)}$ are computed in Algorithm 5.4.8.

2. The constant $r_{\min} = \inf\left\{ \delta^2 x + \Im\,\langle \delta\beta\underline{z}, \zeta\rangle_+ \;\middle|\; x \in R \text{ and } \underline{z} \in Z \right\}$

$$\begin{aligned} \inf\left\{ \delta^2 x + \Im\,\langle \delta\beta\underline{z}, \zeta\rangle_+ \;\middle|\; x \in R \text{ and } \underline{z} \in Z \right\} &= \inf\left\{ \delta^2 x + \Im\left\langle \underline{z}, \delta\overline{\beta}\overline{\zeta}\right\rangle_+ \;\middle|\; x \in R \text{ and } \underline{z} \in Z \right\} \\ &= \inf\left\{ \delta^2 x \;\middle|\; x \in R \right\} + \inf\left\{ \Im\left\langle \underline{z}, \delta\overline{\beta}\overline{\zeta}\right\rangle_+ \;\middle|\; \underline{z} \in Z \right\} \end{aligned}$$

   Since R is an interval on the real line then $\inf\left\{ \delta^2 x \;\middle|\; x \in R \right\} = \delta^2 \inf R$. Considering the second term

$$\begin{aligned} \inf\left\{ \Im\left\langle \underline{z}, \delta\overline{\beta}\overline{\zeta}\right\rangle_+ \;\middle|\; \zeta \in Z \right\} &= \delta \sum \inf\left\{ \Im\beta\overline{\zeta}_i \underline{z}_i \;\middle|\; \underline{z}_i \in Z_i \right\} \\ &= \delta \sum \inf\left\{ \Re(\beta\overline{\zeta}_i)\Im(\underline{z}_i) + \Im(\beta\overline{\zeta}_i)\Re(\underline{z}_i) \;\middle|\; \underline{z}_i \in Z_i \right\} \\ &= \delta \sum \Re(\beta\overline{\zeta}_i) \inf\left\{ \Im\underline{z}_i \;\middle|\; \underline{z}_i \in Z_i \right\} + \Im(\beta\overline{\zeta}_i) \inf\left\{ \Re\underline{z}_i \;\middle|\; \underline{z}_i \in Z_i \right\} \end{aligned}$$

   Each Z_i is the Cartesian product of two real intervals, hence $Z_i = W_i \times \imath Y_i$. Therefore

$$\inf\left\{ \Im\left\langle \underline{z}, \delta\overline{\beta}\overline{\zeta}\right\rangle_+ \;\middle|\; \zeta \in Z \right\} = \delta \sum \Re(\beta\overline{\zeta}_i) \inf W_i + \Im(\beta\overline{\zeta}_i) \inf Y_i$$

   The other constant $r_{\max}$ is computed almost identically, simply replace every occurrence of inf with sup.

Lemma 5.4.12 *Let* $\mathbf{q} \in \mathcal{C}_{K,\delta}$ *and let* $R_{\delta,\beta,\zeta} = \mathit{Algorithm}\ 5.4.11(n,\delta,\beta,\zeta,X)$. *Then* $r \in R_{\delta,\beta,\zeta}$

PROOF Put $r_{\max} = \sup\left\{ \delta^2 x - \Im\,\langle \delta\beta\underline{z}, \zeta\rangle_+ \mid \underline{z} \in Z, r \in R \right\}$ and $r_{\min} = \inf\left\{ \delta^2 x - \Im\,\langle \delta\beta\underline{z}, \zeta\rangle_+ \mid \underline{z} \in Z, r \in R \right\}$. By Lemma 5.4.10, $\sqrt{\delta^2 - C_r} - r_{\max} < r < \sqrt{\delta^2 - C_r} - r_{\min}$. Therefore, by Lemma 4.5.4, $r \in R_{\delta,\beta,\zeta}$. ∎

5.5 Non-Effective Cusps

Although removing non-primitive and equivalent cusps and improving the bounds on the zeta and r components significantly reduces the number of superfluous cusps which are generated, some percentage of the generated cusps will not be effective on the input set X. It turns out that due to the convexity of the effect function and the convexity of the input set, it is possible to say exactly which cusp are and are not effective on X, since a local minimum of a convex function on a convex set is automatically a global minimum on the set. Therefore a multidimensional minimisation algorithm can be applied to find the minimum of the effect function on the input set and thus to decide whether a cusp is effective on the input set. This operation is accurate, but also time consuming. Therefore the effectiveness of a cusp should only be explicitly computed after exhausting all other options for cusp pruning.

Lemma 5.5.1 *Let $\mathbf{q} \in \mathcal{C}_K$ and let $e_{\min}$ be a local minimum for $\mathrm{e}_{\mathbf{q}}(-)$ on X. Then $e_{\min}$ is a global minimum for $\mathrm{e}_{\mathbf{q}}(-)$ on X,*

PROOF By Proposition 4.1.9, the effect function is a convex function on $\overline{\mathbb{H}^n_{\mathbb{C}}}^{\times}$ under the standard Euclidean metric and a local minimum of a convex function on a convex set is always a global minimum. Since the set X is convex this completes the proof. ■

Corollary 5.5.2 *Let $\mathbf{q} \in \mathcal{C}_K$, let $e_{\min}$ be a local minimum for $\mathrm{e}_{\mathbf{q}}(-)$ on X and suppose that $e_{\min} \geq 1$. Then $\mathbf{q} \notin \mathcal{C}_K(X)$.*

To compute a global minimum for $\mathrm{e}_{\mathbf{q}}(-)$ on X, by Lemma 5.5.1, it is sufficient to compute a local minimum for $\mathrm{e}_{\mathbf{q}}(-)$ on X. Since the effect function is convex this minimum can be computed using the conjugate gradient multidimensional minimisation method described in [PTVF92, 10.6].

5.6 Improved Cusp Construction

The tools have now been developed to efficiently compute a tight set of effective cusps. In this section these tools are combined into a single algorithm which outputs a set of cusps Q_δ such that if $\mathbf{q} \in \mathcal{C}_{K,\delta}(X)$, then either $\mathbf{q} \in Q_\delta$, $\mathbf{q}$ is not primitive or there is an equivalent cusp to $\mathbf{q}$ in Q_δ.

Algorithm 5.6.1 (Improved Cusp Construction)

Inputs: $n \in \mathbb{N}^{\geq 2}$ the dimension, d a Heegner number, $\Delta \in \mathbb{N}$, $X = Z \times R$ a search space.

1. Assign $\delta \leftarrow \sqrt{\Delta}$
2. Compute $B_\delta \leftarrow \left\{ \frac{a+b\sqrt{d}}{\delta} \in \mathbb{C} \;\middle|\; a,b \in \mathbb{Z} \text{ s.t. } a^2 - db^2 = \Delta \right\}$
3. Assign $B'_\delta \leftarrow$ *Algorithm* 5.3.4(B_δ, d)
4. For each $\beta \in B'_\delta$
    5. Assign $Z'_{\delta,\beta} \leftarrow$ *Algorithm* 5.4.8$(n, \delta, \beta, \mathfrak{O}, Z)$
    6. For each $\zeta \in Z_{\delta,\beta}{}'$

7. Assign $R'_{\delta,\beta,\zeta} \leftarrow$ *Algorithm* 5.4.11$(n,\delta,\beta,\mathfrak{O},X)$
8. For each $r \in R'_{\delta,\beta,\zeta}$
9. Assign $\mathbf{q} \leftarrow \left(\delta\beta\ \zeta\ \frac{\beta}{\delta}\left(-\frac{Q_+(\zeta)}{2}+ir\right)\right)^{\mathrm{t}}$
10. If $\mathbf{q}$ is not primitive then Continue
11. Compute $e_{\min} \leftarrow \inf\{\mathrm{e}_{\mathbf{q}}(\underline{\mathbf{v}}) \,|\underline{\mathbf{v}} \in X\}$
12. If $e_{\min} \geq 1$ then Continue
13. Assign $Q_\delta \leftarrow Q_\delta \cup \{\mathbf{q}\}$
14. Next
15. Next
16. Next
17. Return Q_δ

Proposition 5.6.2 *Let $\Delta \in \mathbb{N}$, put $\delta = \sqrt{\Delta}$, let $Q_\delta =$ Algorithm* 5.6.1(n,d,Δ,X). *Then $Q_\delta \subset \mathcal{C}_{K,\delta}(X)$ and if $\mathbf{q} \in \mathcal{C}_{K,\delta}(X)$, then either $\mathbf{q} \in Q_\delta$, $\mathbf{q}$ is not primitive or there is an equivalent cusp to $\mathbf{q}$ in Q_δ.*

PROOF All non-primitive cusps are removed on Line 10 and all non-effective cusps are removed on Line 12, so $Q_\delta \subseteq \mathcal{C}_{K,\delta}(X) \cap \{\mathbf{q} \mid \mathbf{q} \text{ is primitive}\}$. Let $\mathbf{q} \in \mathcal{C}_{K,\delta}(X) \cap \{\mathbf{q} \mid \mathbf{q} \text{ is primitive}\}$, suppose that Line 3 is removed from Algorithm 5.6.1 so that

$$B_\delta = \begin{cases} \left\{ \frac{a+b\sqrt{d}}{\delta} \in \mathbb{C} \;\middle|\; a,b \in \mathbb{Z} \text{ s.t. } a^2 - db^2 = \Delta \right\} & \text{if } d \not\equiv 1 \mod 4 \\ \left\{ \frac{a+b\sqrt{d}}{2\delta} \in \mathbb{C} \;\middle|\; a,b \in \mathbb{Z} \text{ s.t. } a^2 - db^2 = 4\Delta \right\} & \text{if } d \equiv 1 \mod 4 \end{cases}$$

and call the output of this modified algorithm Q'_δ. In this case, by Lemma 4.5.2, $\beta \in B_\delta$, by Lemma 5.4.9, $\zeta \in Z_{\delta,\beta}$ and by Lemma 5.4.12, $r \in R_{\delta,\beta,\zeta}$. As $\mathbf{q}$ is primitive, then it is not removed from Q'_δ on Line 10 and as $\mathbf{q}$ is effective on X it is not removed on line 12. Therefore $\mathbf{q} \in Q'_\delta$, thus $Q'_\delta = \mathcal{C}_{K,\delta}(X) \cap \{\mathbf{q} \mid \mathbf{q} \text{ is primitive}\}$.

Suppose now that Line 3 is no longer removed and call the output of the original unmodified algorithm Q_δ. Let $\mathbf{q} \in \mathcal{C}_{K,\delta}(X) \cap \{\mathbf{q} \mid \mathbf{q} \text{ is primitive}\}$. If $\beta \in B_\delta$, then by the argument for the modified algorithm above $\mathbf{q} \in Q_\delta$, so assume $\beta \notin B_\delta$. By Lemma 5.3.5, there exists a unit $u \in \mathfrak{O}^*$ such that $u\beta \in B_\delta$. Put $\beta' = u\beta$ and let $Q_{\delta,\beta'} = \{\mathbf{q} \in Q_\delta \mid \mathbf{q} \text{ has rotation factor } \beta'\}$; since $Q_\delta \subset Q'_\delta$, then $Q_{\delta,\beta'} \subset Q'_\delta$. In the notation of Lemma 5.3.3 $\mathbf{q} \in Q^{\perp}_{\delta,\beta'}$ and by this Lemma, since $Q'_\delta = \mathcal{C}_{K,\delta}(X) \cap \{\mathbf{q} \mid \mathbf{q} \text{ is primitive}\}$, there is an equivalent cusp to $\mathbf{q}$ in $Q_{\delta,\beta'}$. Again by the proceeding argument $Q_{\delta,\beta'} \subset Q_\delta$, so either $\mathbf{q} \in Q_\delta$, $\mathbf{q}$ is not primitive or there is an equivalent cusp to $\mathbf{q}$ in Q_δ. ∎

The minimisation routine used on Line 11 of Algorithm 5.6.1 to compute $\inf\{\mathrm{e}_{\mathbf{q}}(\underline{\mathbf{v}}) \mid \underline{\mathbf{v}} \in X\}$ is an expensive computational procedure, as can be seen by examining the implementation described in [PTVF92, 10.6]; it involves performing a large number of linear minimisations which are in themselves are time expensive. By comparison, removing non-primitive cusps, removing equivalent cusps and tightening the bounds on the zeta and r factors of cusps are all computationally cheap. Therefore practically, since these cheap operation reduces the size of Q_δ quite substantially and since removing equivalent cusps and tightening the bounds on the zeta and r factors all speed up construction time, it is much faster to remove all

non-effective cusps after implementing these optimisations than it is to remove the non-effective cusps from the much larger unoptimised set generated by Algorithm 4.5.5 or Algorithm 4.5.6. However, the cusp sets output from both procedures will perform identically with respect to Siegel set construction.

5.7 Computing the Resolution

The current situation is that $X \in \partial\mathbb{H}^{n\,\times}_{\mathbb{C}}$ is subdivided into N multidimensional rectangles; let $\varepsilon > 0$ and let $\underline{\mathbf{v}} \in \{\underline{\mathbf{v}} \in X \mid \Re z_i, \Im z_i, x \in \varepsilon\mathbb{Z}\}$ then each rectangle V is of the form

$$V = \left\{\underline{\mathbf{v}}' \in X \;\middle|\; \left|\Re z_i' - \Re z_i\right| \leq \varepsilon, \left|\Im z_i' - \Im z_i\right| \leq \varepsilon, \left|x' - x\right| \leq \varepsilon\right\} \tag{5.2}$$

and all of these rectangles V are identical, except for those rectangles where one of the coordinates of $\underline{\mathbf{v}}$ is closer than ε to the boundary of X, in this case V shall be smaller than the standard rectangle. Theoretically this is fine, however practically it is neither easy to implement, nor is it particularly efficient from the point of view of computation due to the overlap between adjacent rectangles. This section considers a more practical approach to the problem of discretisation.

Suppose instead that we begin with a resolution N. The real dimension of $Z \times R$ is $2n-1$; the complex part Z decomposes as $\prod_{i=1}^{n-1} Z_i$ where $Z_i = W_i \times \imath Y_i$ and both W_i and Y_i are intervals on the real line. For $i \in \{1, \ldots, n-1\}$ define $I_{2i-1} = W_i$, $I_{2i} = Y_i$ and define $I_{2n-1} = R$, then as a real vector space $Z \times R = \prod_{i=1}^{2n-1} I_i$. Let $l_i = |I_i|$ and put $m = \prod_{i=1}^{2n-1} l_i$ so that m is the Euclidean measure of $Z \times R$. Let $N_i = \left\lceil \left(\frac{N}{m}\right)^{\frac{1}{2n-1}} l_i \right\rceil$, let $\varepsilon_i = \frac{l_i}{2N_i}$ and define

$$\begin{aligned}
V(\underline{\mathbf{v}}, \{\varepsilon_i\}, X) &= \left\{\underline{\mathbf{v}}' \in X \;\middle|\; \left|\Re z_i' - \Re z_i\right| \leq \varepsilon_{2i-1}, \left|\Im z_i' - \Im z_i\right| \leq \varepsilon_{2i}, \left|x' - x\right| \leq \varepsilon_{2n-1}\right\} \\
\Lambda(\{\varepsilon_i\}, X) &= \left\{\underline{\mathbf{v}} \in X \;\middle|\; \begin{array}{l} \Re z_i - \inf I_{2i-1} \in \varepsilon_{2i-1}\mathbb{Z}^{\text{odd}}, \Im z_i - \inf I_{2i} \in \varepsilon_{2i}\mathbb{Z}^{\text{odd}}, \\ x - \inf I_{2n-1} \in \varepsilon_{2n-1}\mathbb{Z}^{\text{odd}} \end{array}\right\} \\
\Omega(\{\varepsilon_i\}, X) &= \{V(\underline{\mathbf{v}}, \{\varepsilon_i\}, X) \subset X \mid \underline{\mathbf{v}} \in \Lambda(\{\varepsilon_i\}, X)\}
\end{aligned}$$

so that $X = \bigcup_{V \in \Omega(\{\varepsilon_i\}, X)} V$ and the new resolution of the discretisation is $N' = |\Omega(\{\varepsilon_i\}, X)| = \prod_{i=1}^{2n-1} N_i$.

Lemma 5.7.1 *With the set up as described above: $N' \geq N$ and*

$$\frac{l_i}{\left(\frac{N}{m}\right)^{\frac{1}{2n-1}} l_i + 1} \leq 2\varepsilon_i \leq \left(\frac{m}{N}\right)^{\frac{1}{2n-1}}$$

PROOF The formula for the new resolution is $N' = \prod_{i=1}^{2n-1} N_i$ so

$$N' = \prod_{i=1}^{2n-1} N_i = \prod_{i=1}^{2n-1} \left\lceil \left(\frac{N}{m}\right)^{\frac{1}{2n-1}} l_i \right\rceil \geq \prod_{i=1}^{2n-1} \left(\frac{N}{m}\right)^{\frac{1}{2n-1}} l_i = \frac{N}{m} \prod_{i=1}^{2n-1} l_i = \frac{N}{m} m = N$$

To bound ε_i observe that $\left(\frac{N}{m}\right)^{\frac{1}{2n-1}} l_i \leq N_i \leq \left(\frac{N}{m}\right)^{\frac{1}{2n-1}} l_i + 1$. ∎

From a computational point of view the smaller the resolution, the better in terms of speed of computation. However conversely, the smaller the resolution, the greater the amount of error introduced through discretisation. Given this the resolution is chosen based on the following heuristic: Let δ be the current maximum dilation factor in the Siegel set computation algorithm, let $\underline{\mathbf{v}}' \in \Lambda(\{\varepsilon_i\}, X)$, let $V = V(\underline{\mathbf{v}}', \{\varepsilon_i\}, X)$, let $\mathbf{q} \in \mathcal{C}_K$ and put $\tilde{\mathbf{q}} = (\delta\beta)^{-1}\mathbf{q} \in \partial\mathbb{H}^n_{\mathbb{C}}$ so that

$$\sup\{\mathrm{e}_{\mathbf{q}}(\underline{\mathbf{v}}) \mid \underline{\mathbf{v}} \in V\} = \sup\left\{|\langle \underline{\mathbf{v}}, \mathbf{q}\rangle|^2 \mid \underline{\mathbf{v}} \in V\right\} = \sup\left\{|\langle \underline{\mathbf{v}}, \delta\beta\tilde{\mathbf{q}}\rangle|^2 \mid \underline{\mathbf{v}} \in V\right\} = \delta \sup\left\{|\langle \underline{\mathbf{v}}, \tilde{\mathbf{q}}\rangle|^2 \mid \underline{\mathbf{v}} \in V\right\}$$

Thus by Lemma 4.3.4, $\Phi_{\mathbf{q}}(V) > 0$ if and only if $\sup\left\{|\langle \underline{\mathbf{v}}, \tilde{\mathbf{q}}\rangle|^2 \mid \underline{\mathbf{v}} \in V\right\} < \delta^{-2}$. The point $\underline{\mathbf{v}}'$ is the midpoint of V under the standard Euclidean metric and in general there will not exist a β such that $\mathbf{q}' = \delta\beta\underline{\mathbf{v}}' \in \mathcal{C}_K$, however if such a β existed and $\Phi_{\mathbf{q}'}(V) \leq 0$ then, given the convexity of the effect function, the chance of their existing another cusp $\mathbf{q}'' \in \mathcal{C}_{K,\delta}$ with the property that $\Phi_{\mathbf{q}''}(V) > 0$ are low. So computing

$$e = \sup\left\{\sup\left\{|\langle \underline{\mathbf{v}}, \underline{\mathbf{v}}'\rangle|^2 \;\middle|\; \underline{\mathbf{v}} \in V(\underline{\mathbf{v}}', \{\varepsilon_i\}, X)\right\} \;\middle|\; \underline{\mathbf{v}}' \in \Lambda(\{\varepsilon_i\}, X)\right\}$$

provides a good indication of how well cusps of maximal dilation factor can be expected to perform under the current discretisation over the whole of X; the smaller the value of e the better the discretisation can be expected to perform.

Lemma 5.7.2 *Let* $e = \sup\left\{\sup\left\{|\langle \underline{\mathbf{v}}, \underline{\mathbf{v}}'\rangle|^2 \;\middle|\; \underline{\mathbf{v}} \in V(\underline{\mathbf{v}}', \{\varepsilon_i\}, X)\right\} \;\middle|\; \underline{\mathbf{v}}' \in \Lambda(\{\varepsilon_i\}, X)\right\}$. *Then*

$$e = \frac{\left(\sum_{i=1}^{n-1} \varepsilon_{2i-1}^2 + \varepsilon_{2i}^2\right)^2}{4} + \left(\left(\sum_{i=1}^{n-1} \varepsilon_{2i} \max\{\inf|W_i|, \sup|W_i|\} + \varepsilon_{2i-1} \max\{\inf|Y_i|, \sup|Y_i|\}\right) + \varepsilon_{2n-1}\right)^2$$

PROOF Let $\underline{\mathbf{v}}$ be a vertex of V and let $\underline{\mathbf{v}}'$ be the midpoint of V, then

$$\begin{aligned}
|\langle \underline{\mathbf{v}}, \underline{\mathbf{v}}'\rangle|^2 &= \frac{\mathrm{Q}_+(\underline{z} - \underline{z}')^2}{4} + \left(\Im\langle \underline{z}, \underline{z}'\rangle_+ + x - x'\right)^2 \\
&= \frac{\left(\sum_{i=1}^{n-1} \varepsilon_{2i-1}^2 + \varepsilon_{2i}^2\right)^2}{4} + \left(\Im\langle \underline{z}, \underline{z}'\rangle_+ \pm \varepsilon_{2n-1}\right)^2 \\
&= \frac{\left(\sum_{i=1}^{n-1} \varepsilon_{2i-1}^2 + \varepsilon_{2i}^2\right)^2}{4} + \left(\left(\sum_{i=1}^{n-1} \pm\varepsilon_{2i}\Re\underline{z}_i \pm \varepsilon_{2i-1}\Im\underline{z}_i\right) \pm \varepsilon_{2n-1}\right)^2
\end{aligned}$$

From the proof of Lemma 4.4.3, $\sup\left\{|\langle \underline{\mathbf{v}}, \underline{\mathbf{v}}'\rangle|^2 \mid \underline{\mathbf{v}} \in V\right\} = \sup\left\{|\langle \underline{\mathbf{v}}, \underline{\mathbf{v}}'\rangle|^2 \mid \underline{\mathbf{v}} \text{ is a vertex of } V\right\}$ since the effect function is convex and V is a convex set, from which the result follows. ■

Note that since both $\max\{\inf|W_i|, \sup|W_i|\}$ and $\max\{\inf|Y_i|, \sup|Y_i|\}$ are known, then computing e in Lemma 5.7.2 is a simple operation.

Lemma 5.7.3 *Let* $\alpha \in (0,1)$, *let* $z = \sum_{i=1}^{n-1} \max\{\inf|W_i|, \sup|W_i|\} + \max\{\inf|Y_i|, \sup|Y_i|\}$, *put*

$$c_0 = \frac{2(\alpha - 1)}{\delta} \qquad c_1 = m^{\frac{2}{2n-1}}(z+1)^2 \qquad c_2 = \frac{m^{\frac{4}{2n-1}}(n-1)^2}{4} \qquad N = \left(\frac{c_1 - \sqrt{c_1^2 - 4c_0c_2}}{2c_2}\right)^{\frac{2}{1-2n}}$$

and discretise X with resolution N. Then $e \leq \frac{2(1-\alpha)}{\delta}$.

PROOF By Lemma 5.7.1, $\varepsilon_i \leq \frac{1}{2}\left(\frac{m}{N}\right)^{\frac{1}{2n-1}}$ so by Lemma 5.7.2, e is bounded above by

$$e \leq \frac{(n-1)^2}{4}\left(\frac{m}{N}\right)^{\frac{4}{2n-1}} + (z+1)^2\left(\frac{m}{N}\right)^{\frac{2}{2n-1}}$$

Therefore under this discretisation, the inequality $e \leq \frac{2(1-\alpha)}{\delta}$ is satisfied. ■

So setting the resolution using Lemma 5.7.3 ensures that $e \leq \frac{2(1-\alpha)}{\delta}$ and provides user control over how well the cusps of maximum dilation factor will perform with respect to the discretisation; all cusps of smaller dilation factor will perform better.

5.8 Computing Phi on *V*

The process of computing a Siegel set has two phases; constructing cusps and computing Phi. The construction of cusps has been discussed above, but as yet nothing has been said about computing Phi on the vertices of a convex polytope; specifically on the vertices of a multidimensional rectangle. The naïve approach is simply to compute Phi over every vertex and then take the minimum over all vertices; this is fine in theory, but in practise, because the value of Phi of adjacent vertices is related, this is quite inefficient. This section presents a better method of computing Phi which makes use of the geometric properties of the polytopes V which are iterated over.

Let $\mathbf{q} \in \mathcal{C}_K$, let $\underline{\mathbf{v}}' \in \partial\mathbb{H}^n_{\mathbb{C}}$, let $V = V(\underline{\mathbf{v}}', \{\varepsilon_i\}, X)$ and let $\underline{\mathbf{v}}$ be the vertex of V where each coordinate, when considered as an element of a real vector space, is minimal coordinate-wise over all vertices. Write $\tilde{\zeta} = (\delta\beta)^{-1}\zeta$ and $\tilde{r} = r\delta^{-2}$, then

$$\varphi_{\mathbf{q}}(\underline{\mathbf{v}}) = 2\sqrt{\delta^{-2} - \left(x - \tilde{r} + \Im\left\langle \underline{z}, \tilde{\zeta}\right\rangle_+\right)^2} + 2\Re\left\langle \underline{z}, \tilde{\zeta}\right\rangle_+ - \mathrm{Q}_+\left(\tilde{\zeta}\right) - \mathrm{Q}_+(\underline{z})$$

Identify the set $\partial\mathbb{H}^{n\times}_{\mathbb{C}}$ with $\mathbb{R}^{2n-1}$, let $\mu_i \in \{0,1\}$ for $i = \{1,\ldots,2n-1\}$ and define $\underline{\mathbf{v}}_{(\mu_1,\ldots,\mu_{2n-1})} = \underline{\mathbf{v}} + (\mu_1 2\varepsilon_1, \ldots, \mu_{2n-1}2\varepsilon_{2n-1})$, so the set of all $\underline{\mathbf{v}}_{(\mu_1,\ldots,\mu_{2n-1})}$ comprises the set of vertices of V. Whence

$$\begin{aligned}\varphi_{\mathbf{q}}\left(\underline{\mathbf{v}}_{(\mu_1,\ldots,\mu_{2n-1})}\right) =& 2\sqrt{\delta^{-2} - \left(x + 2\mu_{2n-1}\varepsilon_{2n-1} - \tilde{r} + \Im\left\langle \underline{z}, \tilde{\zeta}\right\rangle_+ + 2\sum_{i=1}^{n-1}(\mu_{2i-1}\varepsilon_{2i-1}\Im\zeta_i - \mu_{2i}\varepsilon_{2i}\Re\zeta_i)\right)^2} \\ &+ 2\Re\left\langle \underline{z}, \tilde{\zeta}\right\rangle_+ + 4\sum_{i=1}^{n-1}(\mu_{2i-1}\varepsilon_{2i-1}\Re\zeta_i + \mu_{2i}\varepsilon_{2i}\Im\zeta_i) - \mathrm{Q}_+\left(\tilde{\zeta}\right) \\ &- \mathrm{Q}_+(\underline{z}) - 4\sum_{i=1}^{2n-1}(\mu_i|\varepsilon_i|^2) - 4\sum_{i=1}^{n-1}(\mu_{2i-1}\varepsilon_{2i-1}\Re\underline{z}_i + \mu_{2i}\varepsilon_{2i}\Im\underline{z}_i)\end{aligned}$$

Assume that for some $(\mu_1,\ldots,\mu_{2n-1})$ the formula $\varphi_{\mathbf{q}}\left(\underline{\mathbf{v}}_{(\mu_1,\ldots,\mu_{2n-1})}\right)$ has been computed and the values

$$c_1 = x + 2\mu_{2n-1}\varepsilon_{2n-1} - \tilde{r} + \Im\left\langle \underline{z}, \tilde{\zeta}\right\rangle_+ + 2\sum_{i=1}^{n-1}(\mu_{2i-1}\varepsilon_{2i-1}\Im\zeta_i - \mu_{2i}\varepsilon_{2i}\Re\zeta_i)$$

$$c_2 = 2\Re\left\langle \underline{z}, \tilde{\zeta}\right\rangle_+ + 4\sum_{i=1}^{n-1}(\mu_{2i-1}\varepsilon_{2i-1}\Re\zeta_i + \mu_{2i}\varepsilon_{2i}\Im\zeta_i) - \mathrm{Q}_+\left(\tilde{\zeta}\right)$$
$$- \mathrm{Q}_+(\underline{z}) - 4\sum_{i=1}^{2n-1}(\mu_i|\varepsilon_i|^2) - 4\sum_{i=1}^{n-1}(\mu_{2i-1}\varepsilon_{2i-1}\Re\underline{z}_i + \mu_{2i}\varepsilon_{2i}\Im\underline{z}_i)$$

have been stored and suppose $j \in \{1,\ldots,2n-1\}$ such that $\mu_j = 0$. Then setting $\mu_j = 1$

$$\varphi_{\mathbf{q}}\left(\underline{\mathbf{v}}_{(\mu_1,\ldots,\mu_{2n-1})}\right) = 2\sqrt{\delta^{-2} - (c_1 + 2\varepsilon_{2n-1})^2} + c_2 \qquad \text{if } j = 2n-1$$

$$\varphi_{\mathbf{q}}\left(\underline{\mathbf{v}}_{(\mu_1,\ldots,\mu_{2n-1})}\right) = 2\sqrt{\delta^{-2} - \left(c_1 + 2\varepsilon_j\Im\zeta_{\left\lceil\frac{j+1}{2}\right\rceil}\right)^2} + c_2 + 4\varepsilon_j\Re\zeta_{\left\lceil\frac{j+1}{2}\right\rceil} \qquad \text{if } j \equiv 1 \mod 2$$
$$- 4\varepsilon_j\Re\underline{z}_{\left\lceil\frac{j+1}{2}\right\rceil} - 4\varepsilon_j^2$$

$$\varphi_{\mathbf{q}}\left(\underline{\mathbf{v}}_{(\mu_1,\ldots,\mu_{2n-1})}\right) = 2\sqrt{\delta^{-2} - \left(c_1 - 2\varepsilon_j\Re\zeta_{\left\lceil\frac{j+1}{2}\right\rceil}\right)^2} + c_2 + 4\varepsilon_j\Im\zeta_{\left\lceil\frac{j+1}{2}\right\rceil} \qquad \text{if } j \equiv 0 \mod 2$$
$$- 4\varepsilon_j\Im\underline{z}_{\left\lceil\frac{j+1}{2}\right\rceil} - 4\varepsilon_j^2$$

Therefore having computed c_1, c_2 and $\varphi_{\mathbf{q}}(\underline{\mathbf{v}})$ for some vertex $\underline{\mathbf{v}}$ of V, then each adjacent vertex may be computed with at most 5 floating point multiplications, 5 additions and 1 square root operation irrespective of the dimension of the space; this is under the assumption that $4\varepsilon_i$, $4\varepsilon_i$, $-4\varepsilon_i$ and $-4\varepsilon_i^2$ have been pre-computed for all $i \in \{1,\ldots,2n-1\}$; since the values of ε_i are fixed for all sets V then this is a perfectly reasonable assumption.

So to compute the value of $\Phi_{\mathbf{q}}(V')$ on line 8 of Algorithm 4.6.2, it is not necessary to construct all of the vertices of V, only one vertex $\underline{\mathbf{v}}$ needs to be constructed and then the value of $\Phi_{\mathbf{q}}(V')$ can be interpolated from $\varphi_{\mathbf{q}}(\underline{\mathbf{v}})$; this is beneficial not only because it makes the computation of $\varphi_{\mathbf{q}}(-)$ for all but one of the vertices a constant time operation, but it also means that only one, rather than all, of the vertices of V needs to be iterated through X; this creates a significant time efficiency.

Algorithm 5.8.1 (Computing Phi on a Set)

Inputs: a dimension $n \in \mathbb{N}$, an index $i \in \{0,\ldots,2n-1\}$, a set of positive real numbers $\{\varepsilon_i,\ldots,\varepsilon_{2n-1}\}$, a cusp $\mathbf{q} \in \mathcal{C}_K$, constants c_1 and c_2

1. If $i = 0$ do nothing
2. Else if $i = 2n-1$ then $c_1 \leftarrow c_1 + 2\varepsilon_{2n-1}$
3. Else if $i = 1 \mod 2$ then $c_1 \leftarrow c_1 + 2\varepsilon_j\Im\zeta_{\left\lceil\frac{j+1}{2}\right\rceil}$, $c_2 \leftarrow c_2 + 4\varepsilon_j\Re\zeta_{\left\lceil\frac{j+1}{2}\right\rceil} - 4\varepsilon_j\Re\underline{z}_{\left\lceil\frac{j+1}{2}\right\rceil} - 4\varepsilon_j^2$
4. Else $c_1 \leftarrow c_1 + 2\varepsilon_j\Re\zeta_{\left\lceil\frac{j+1}{2}\right\rceil}$, $c_2 \leftarrow c_2 + 4\varepsilon_j\Im\zeta_{\left\lceil\frac{j+1}{2}\right\rceil} - 4\varepsilon_j\Im\underline{z}_{\left\lceil\frac{j+1}{2}\right\rceil} - 4\varepsilon_j^2$
5. Assign $L \leftarrow 2\sqrt{\delta^{-2} - c_1^2} + c_2$
6. If $L \notin [0,\infty)$ then assign $L \leftarrow -1$ and return L
7. For each $j \in \{i+1,\ldots,2n-1\}$

8. Recursively Assign $L \leftarrow \min\left\{L, \text{Algorithm 5.8.1}\left(n, j, \left\{\varepsilon_j, \ldots, \varepsilon_{2n-1}\right\}, \mathbf{q}, c_1, c_2\right)\right\}$

9. Next

10. Return L

Lemma 5.8.2 *Let $\mathbf{q} \in \mathcal{C}_K$, let $\underline{\mathbf{v}}$ be the minimal vertex of a rectangular set V, let V' be the set of vertices of V, let $c_1 = x - r\delta^{-2} + \Im\left\langle \underline{z}, (\delta\beta)^{-1}\zeta\right\rangle_+$ and $c_2 = 2\Re\left\langle \underline{z}, (\delta\beta)^{-1}\zeta\right\rangle_+ - \mathrm{Q}_+\left((\delta\beta)^{-1}\zeta\right) - \mathrm{Q}_+(\underline{z})$. Then $\Phi_{\mathbf{q}}(V) =$ Algorithm 5.8.1 $(n, 0, \{\varepsilon_1, \ldots, \varepsilon_{2n-1}\}, \mathbf{q}, c_1, c_2)$.*

PROOF On the first recursive loop with $i = 0$ the variable L is set to $L = \varphi_{\mathbf{q}}(\underline{\mathbf{v}})$ on lines 5 and 6 and the values of c_1 and c_2 have been precomputed at the time of input. On the second recursive loop, for each $i_1 \in \{1, \ldots, 2n-1\}$, the variable L is set to $L = \varphi_{\mathbf{q}}\left(\underline{\mathbf{v}}_{(0,\ldots,\mu_{i_1},\ldots,0)}\right)$ where $\mu_{i_1} = 1$ and the corresponding constants c_1 and c_2 are computed according to the value of i_1 as described above. On the third recursive loop, for each pair (i_1, i_2) where $i_1, i_2 \in \{1, \ldots, 2n-1\}$ and $i_1 \neq i_2$, the variable L is set to $L = \varphi_{\mathbf{q}}\left(\underline{\mathbf{v}}_{(0,\ldots,\mu_{i_1},\ldots,\mu_{i_2},\ldots,0)}\right)$ where $\mu_{i_1} = \mu_{i_2} = 1$ and the corresponding constants c_1 and c_2 are computed according to the values of i_1 and i_2. In general on the m^{th} recursive loop for each m-tuple $(i_1, \ldots, i_m)$ where $i_1, \ldots, i_m \in \{1, \ldots, 2n-1\}$ and pairwise $i_j \neq i_k$ for all $j \neq k$, the variable L is set to $L = \varphi_{\mathbf{q}}\left(\underline{\mathbf{v}}_{(0,\ldots,\mu_{i_1},\ldots,\mu_{i_m},\ldots,0)}\right)$ where $\mu_{i_1} = \ldots = \mu_{i_m} = 1$ and the corresponding constants c_1 and c_2 are computed according to the values of $i_1, \ldots, i_m$. Thus over all recursive loops, the value of $L = \varphi_{\mathbf{q}}\left(\underline{\mathbf{v}}_{(\mu_1,\ldots,\mu_{2n-1})}\right)$ is computed for all tuples $(\mu_1, \ldots, \mu_{2n-1})$ and the output value of the algorithm is the minimum over all of these values of L, therefore $\Phi_{\mathbf{q}}(V) =$ Algorithm 5.8.1 $(n, 0, \{\varepsilon_1, \ldots, \varepsilon_{2n-1}\}, \mathbf{q}, c_1, c_2)$. ∎

5.9 Choosing Cusps from Q

Just as it is not very efficient to naïvely compute Phi over all vertices by computing Phi at each vertex, it is also not very efficient to naïvely iterate through every cusp in Q to find the most effective cusp for a given polytope V. Starting with the observation that it is not necessary to find the best possible cusp for V, but it is just necessary to find a cusp which is sufficiently good (i.e. one which raises V above the current minimum height), this section considers how the set Q can be sorted in order to improve the chances that a sufficiently effective cusp is chosen from Q quickly.

Let $S \subset \overline{\mathbb{H}^n_{\mathbb{C}}}$ and with respect to S define the binary relation $\leq_S$ on $\mathcal{C}_K$ in the following way; let $\mathbf{q}, \mathbf{q}' \in \mathcal{C}_K$, let $e_{(\mathbf{q},S)} = \inf\{\mathrm{e}_{\mathbf{q}}(\underline{\mathbf{v}}) \mid \underline{\mathbf{v}} \in S\}$ and let $e_{(\mathbf{q}',S)} = \inf\left\{\mathrm{e}_{\mathbf{q}'}(\underline{\mathbf{v}}) \mid \underline{\mathbf{v}} \in S\right\}$, then $\mathbf{q} \leq_S \mathbf{q}'$ if $e_{(\mathbf{q},S)} \leq e_{(\mathbf{q}',S)}$. The relation $\leq_S$ is a total preorder (reflexive and transitive) since $\mathbb{R}$ is totally ordered, but $\leq_S$ is not antisymmetric as is clear from taking $S = \overline{\mathbb{H}^n_{\mathbb{C}}}$ in which case for any two cusps $e_{(\mathbf{q},S)} = e_{(\mathbf{q}',S)} = 0$.

Let $V \subset S$, let $\mathbf{q}, \mathbf{q}' \in \mathcal{C}_K$ and suppose that $\mathbf{q} \leq_S \mathbf{q}'$; this does not imply that $\Phi_{\mathbf{q}'}(V) \leq \Phi_{\mathbf{q}}(V)$, but given the convexity of the effect function and the fact that the phi function varies inversely to the effect function, if no further information about $\mathbf{q}$ and $\mathbf{q}'$ in relation to V is known then assuming $\Phi_{\mathbf{q}'}(V) \leq \Phi_{\mathbf{q}}(V)$ is a logical heuristic. Observe that on line 8 of Algorithm 4.6.2 it is not in general necessary to compute $L' = \sup\{\Phi_{\mathbf{q}}(V') \mid \mathbf{q} \in Q\}$, since on line 10, the new lower height bound is taken as $L = \min\{L, L'\}$, therefore it is sufficient to find some $\mathbf{q} \in Q$ such that $L \leq \Phi_{\mathbf{q}}(V')$; although of course if no such $\mathbf{q}$ exists then it is necessary to compute $L' = \sup\{\Phi_{\mathbf{q}}(V') \mid \mathbf{q} \in Q\}$. Therefore, ordering the cusps in Q by $\leq_X$ is a justifiable heuristic which should (and in practise does) improve the speed of computation; in C++ using

a `std::set` as the model for Q, inserting cusps into Q and simultaneously ordering Q on the fly is a logarithmic time operation in the size of Q, as such it is computationally negligible in comparison to the cost of iterating through the elements $\mathbf{q} \in Q$ and computing $\Phi_{\mathbf{q}}(V)$, which is at least linear in the size of Q.

Rather than ordering the cusps in Q based solely on the relation $\leq_X$, the set X can be partitioned and Q can be ordered on each partition as is done in the following algorithm;

Algorithm 5.9.1 (Cusp Partitioning and Ordering)

Inputs: Sets $X_i \subseteq X$ for $i = 1, \ldots, s$ such that $X = \bigcup_{i=1}^{s} X_i$ and a preordered set of cusps $Q_i \subset \mathcal{C}_K(X_i)$ for $i = 1, \ldots, s$, a cusp $\mathbf{q} \in \mathcal{C}_K$

1. For each $i \in \{1, \ldots, s\}$

    2. Compute $e_{(\mathbf{q},i)} = \inf\{\mathrm{e}_{\mathbf{q}}(\underline{\mathbf{v}}) \mid \underline{\mathbf{v}} \in X_i\}$ (using the minimisation algorithm described in [PTVF92, 10.6] from Section 5.5)

    3. If $e_{(\mathbf{q},i)} < 1$ then insert $\mathbf{q}$ into Q_i with respect to the preorder $\leq_{X_i}$

4. Next

5. Return $\{Q_i, \ldots, Q_s\}$

Lemma 5.9.2 *Construct the sets Q_i for $i \in \{1, \ldots, m\}$ by passing all cusps in Q through Algorithm 5.9.1, let $V \subset X$, let $j \in \{1, \ldots, m\}$ such that $V \cap X_j$ and suppose that $\mathbf{q} \in Q \cap \mathcal{C}_K(V)$. Then $\mathbf{q} \in Q_j$.*

PROOF By Lemma 4.3.4, $\mathrm{e}_{\mathbf{q}}(\underline{\mathbf{v}}) < 1$ if and only if $\varphi_{\mathbf{q}}(\underline{\mathbf{v}}) > 0$, so from lines 2 and 3 of Algorithm 5.9.1 it follows that $Q_j = \left\{\mathbf{q} \in Q \;\middle|\; 0 < \sup\left\{\varphi_{\mathbf{q}}(\underline{\mathbf{v}}) \mid \underline{\mathbf{v}} \in X_j\right\}\right\}$. By assumption, $\Phi_{\mathbf{q}}(V) > 0$ so there exists a $\underline{\mathbf{v}} \in V \cap X_j$ such that $\varphi_{\mathbf{q}}(\underline{\mathbf{v}}) > 0$ and since $\underline{\mathbf{v}} \in X_i$, then $\varphi_{\mathbf{q}}(\underline{\mathbf{v}}) \leq \sup\left\{\varphi_{\mathbf{q}}(\underline{\mathbf{v}}) \mid \underline{\mathbf{v}} \in X_j\right\}$, hence $\mathbf{q} \in Q_i$. ∎

In the C++ implementation of the algorithm the sets X_i are constructed by choosing $s' \in \mathbb{N} \cup \{0\}$ and putting $s = 2^{s'}$, then the $2n-1$ real intervals of X are bisected s' times in total via a binary tree structure to create a partition of X into s sets. Recall that $X = \prod_{i=1}^{2n-1} I_i$ where the $I_i \subset \mathbb{R}$ are intervals. At the root of the tree, zeroth level, there is $1 = 2^0$ space and this space is $X_1^0 = X$. At the first level there are $2 = 2^1$ spaces, these spaces are formed by bisecting the first interval of X_1^0 into two, call the first one X_1^1, call the second X_2^1, then $X_1^1 = \left[\inf I_1, \inf I_1 + \frac{|I_1|}{2}\right] \times \prod_{i=2} I_i$ and $X_2^1 = \left[\sup I_1 - \frac{|I_1|}{2}, \sup I_1\right] \times \prod_{i=2} I_i$. On the second level there $4 = 2^2$ spaces; $X_1^2, \ldots, X_4^2$. The spaces X_1^2 and X_2^2 are formed by bisecting the second interval I_2 of X_1^1, the subspace X_1^2 taking the first half of the interval and X_2^2 taking the second half and copying all other intervals of X_1^1 identically, the spaces X_3^2 and X_4^2 are formed identically from X_2^1. In general on level $l \leq s'$ there are 2^l spaces and the $(l \mod 2n-1)^{\text{th}}$ interval is bisected; space X_{2i}^l takes the lower half of the $(l \mod 2n-1)^{\text{th}}$ interval of X_i^{l-1} and copies all of the other intervals identically, space X_{2i+1}^l takes the upper half of the $(l \mod 2n-1)^{\text{th}}$ interval of X_i^{l-1} and copies all of the other intervals identically.

This tree structure allows cusps to be sorted and cusp sets to be retrieved efficiently. To sort a cusp $\mathbf{q} \in \mathcal{C}_K$ compute $e_1^0 = \inf\left\{\mathrm{e}_{\mathbf{q}}(\underline{\mathbf{v}}) \mid \underline{\mathbf{v}} \in X_1^0\right\}$, if $e_1^0 \geq 1$ then the cusp can be rejected because it plays no part in Siegel set construction, otherwise compute $e_1^1 = \inf\left\{\mathrm{e}_{\mathbf{q}}(\underline{\mathbf{v}}) \mid \underline{\mathbf{v}} \in X_1^1\right\}$ and $e_2^1 = \inf\left\{\mathrm{e}_{\mathbf{q}}(\underline{\mathbf{v}}) \mid \underline{\mathbf{v}} \in X_2^1\right\}$. Since $e_1^0 < 1$, then either $e_1^1 < 1$, or $e_2^1 < 1$ or both; if $e_i^1 < 1$ then compute $e_{2i}^2 = \inf\left\{\mathrm{e}_{\mathbf{q}}(\underline{\mathbf{v}}) \mid \underline{\mathbf{v}} \in X_{2i}^2\right\}$ and

$e^2_{2i+1} = \inf\left\{\mathrm{e}_{\mathbf{q}}(\underline{\mathbf{v}}) \mid \underline{\mathbf{v}} \in X^2_{2i+1}\right\}$. In general on level l if $e^l_i < 1$ then compute $e^{l+1}_{2i} = \inf\left\{\mathrm{e}_{\mathbf{q}}(\underline{\mathbf{v}}) \mid \underline{\mathbf{v}} \in X^{l+1}_{2i}\right\}$ and $e^{l+1}_{2i+1} = \inf\left\{\mathrm{e}_{\mathbf{q}}(\underline{\mathbf{v}}) \mid \underline{\mathbf{v}} \in X^{l+1}_{2i+1}\right\}$; hence on level $l = s'$ a list of at most $2^{s'}$ indices i are computed such that $e^{s'}_i < 1$, if this is the case then add $\mathbf{q}$ to Q_i.

Given a rectangle V, to retrieve a set of cusps Q_i such that if $\mathbf{q} \in \mathcal{C}_K$ and $\Phi_{\mathbf{q}}(V) > 0$ then $\mathbf{q} \in Q_i$, by Lemma 5.9.2 it is sufficient to pick any point in $\underline{\mathbf{v}} \in V$ and then find a set X_i such that $\underline{\mathbf{v}} \in X_i$. Therefore a vertex $\underline{\mathbf{v}}$ of V can be chosen and then this can be passed through the tree in the following way; since $V \subset X$ then $\underline{\mathbf{v}} \in X^0_1$, so begin by checking $\underline{\mathbf{v}}$ for inclusion in X^1_1. If $\underline{\mathbf{v}} \in X^1_1$ then pass down to the second level and consider inclusion in X^2_1. If not then $\underline{\mathbf{v}} \in X^1_2$ so pass down to the second level and consider inclusion in X^2_3. In general on level l there will be exactly two candidate sets that $\underline{\mathbf{v}}$ could lie in, these being X^l_i and X^l_{i+1}; if $\underline{\mathbf{v}} \in X^l_i$ then passing down to level $l+1$, either $\underline{\mathbf{v}} \in X^{l+1}_{2i}$ or $\underline{\mathbf{v}} \in X^{l+1}_{2i+1}$; otherwise passing down to level $l+1$, either $\underline{\mathbf{v}} \in X^{l+1}_{2i+2}$ or $\underline{\mathbf{v}} \in X^{l+1}_{2i+3}$. As such only one inclusion check needs to be performed on each level, thus finding a valid set Q_i given a rectangle V is a linear time operation based on the number of levels in the tree and logarithmic in the number of partitions of X.

5.10 Improved Siegel Set Construction

The final section in this chapter describes an improved algorithm for Siegel set construction based on the tools developed in this chapter. Compared with Algorithm 4.6.2 it is much faster and it is still guaranteed to terminate. However, the error bound on the maximum attainable height is sacrificed for speed; this could be easily rectified by using the resolution computation technique from the old algorithm.

Algorithm 5.10.1 (Improved Siegel Set Construction)

Inputs: $n \in \mathbb{N}^{\geq 2}$ the dimension, d a Heegner number, $\alpha \in (0,1)$ an error tolerance, $X = \prod_{i=1}^{2n-1} I_i$ where the I_i are closed intervals on the real line, $X_i \subseteq X$ for $i \in \{1,\ldots,s\}$ such that $X = \cup_{i=1}^{s} X_i$.

1. Initialise: $L \leftarrow 2$, $\Delta \leftarrow 1$, $l_i \leftarrow |I_i|$ for $i \in \{1,\ldots,2n-1\}$, $m \leftarrow \prod_{i=1}^{2n-1} l_i$, $c_2 \leftarrow \frac{m^{\frac{4}{2n-1}}(n-1)^2}{4}$, $z \leftarrow \sum \max\{\inf|W_i|, \sup|W_i|\} + \max\{\inf|Y_i|, \sup|Y_i|\}$, $c_1 \leftarrow m^{\frac{2}{2n-1}}(z+1)^2$, $Q_i \leftarrow \emptyset$ for $i \in \{1,\ldots,s\}$
2. Assign $\delta \leftarrow \sqrt{\Delta}$, $c_0 \leftarrow \frac{2(\alpha-1)}{\delta}$, $N \leftarrow \left(\frac{c_1 - \sqrt{c_1^2 - 4c_0c_2}}{2c_2}\right)^{\frac{2}{1-2n}}$, $N_i \leftarrow \left\lceil \left(\frac{N}{m}\right)^{\frac{1}{2n-1}} l_i \right\rceil$, $\varepsilon_i \leftarrow \frac{l_i}{2N_i}$, for $i \in \{1,\ldots,2n-1\}$, $\Omega \leftarrow \Omega(\{\varepsilon_1,\ldots,\varepsilon_{2n-1}\}, X)$
3. Compute $Q_\delta \leftarrow$ Algorithm 5.6.1(n, d, Δ, X)
4. For each $\mathbf{q} \in Q_\delta$ assign $\{Q_1,\ldots,Q_s\} \leftarrow$ Algorithm 5.9.1$(\{X_1,\ldots,X_s\}, \{Q_1,\ldots,Q_s\}, \mathbf{q})$.
5. For each $V \in \Omega$
    6. Assign $\underline{\mathbf{v}} \leftarrow$ the minimal vertex of V, $i \leftarrow$ the index such that $\underline{\mathbf{v}} \in X_i$, $L_V \leftarrow -1$.
    7. For each $\mathbf{q} \in Q_i$
        8. Assign $p_1 \leftarrow x - r\delta^{-2} + \Im\left\langle \underline{z}, (\delta\beta)^{-1}\zeta\right\rangle_+$, $p_2 \leftarrow 2\Re\left\langle \underline{z}, (\delta\beta)^{-1}\zeta\right\rangle_+ - \mathrm{Q}_+\left((\delta\beta)^{-1}\zeta\right) - \mathrm{Q}_+(\underline{z})$
        9. Compute $L'_V \leftarrow$ Algorithm 5.8.1$(n, 0, \{\varepsilon_1,\ldots,\varepsilon_{2n-1}\}, \mathbf{q}, p_1, p_2)$
        10. $L_V \leftarrow \max\{L_V, L'_V\}$

11. If $L_V \geq L$ then Break
12. Next
13. If $L_V < \frac{2(1-\alpha)}{\delta}$ then assign $\Delta \leftarrow \Delta + 1$ and goto line 2
14. $L \leftarrow \min\{L, L_V\}$

15. Next

16. Return L

Proposition 5.10.2 *Let $d \in \{-1,-2,-3,-7,-11,-19,-43,-67,-163\}$, let $n \in \mathbb{N}^{\geq 2}$, let $\alpha \in (0,1)$, let S_∞ be the Siegel container computed in Lemma 5.1.2 or Lemma 5.1.3 depending upon the congruence class of d, let $X = \mathrm{S}_\infty \cap \partial\mathbb{H}^{n\,\times}_{\mathbb{C}}$, choose a partition of sets $X_i \subseteq X$ for $i \in \{1,\ldots,s\}$ such that $X = \cup_{i=1}^{s} X_i$ and let $L =$ Algorithm 4.6.2$(d,n,\alpha,X,\{X_1,\ldots,X_s\})$. Then for all $\varepsilon \in \left(0, \frac{L^2}{4}\right)$, the set $\mathrm{S}_\infty(L-\varepsilon)$ is a Siegel set for Γ. Moreover the algorithm is guaranteed to terminate.*

PROOF Since S_∞ is a Siegel container for Γ, then to show that $\mathrm{S}_\infty(L-\varepsilon)$ is a Siegel set for Γ, it is sufficient to show that the algorithm proves that for all $\underline{\mathbf{v}} \in X$, there exists a $\mathbf{q} \in \mathcal{C}_K$ such that $\varphi_{\mathbf{q}}(\mathbf{q}) \geq L$. So let $\underline{\mathbf{v}} \in X$, then by the definition of Ω, $\underline{\mathbf{v}} \in V$ for some $V \in \Omega$ and by Lemma 5.8.2, if $\mathbf{q} \in Q_i$ is the current cusp in the loop between lines 7 and 12, then $\Phi_{\mathbf{q}}(V) =$ Algorithm 5.8.1$(n,0,\{\varepsilon_1,\ldots,\varepsilon_{2n-1}\},\mathbf{q},p_1,p_2)$. Now as the algorithm has terminated with output L then every $V \in \Omega$ must have been iterated through between lines 5 and 15 and for each of these rectangles V line 14 must have been reached; if this were not the case then for some particular V the condition on line 13 would not have been satisfied and the flow of the algorithm would have jumped back to line 2. Therefore for every $V \in \Omega$ there exists a cusp $\mathbf{q}$ in some Q_i such that $\Phi_{\mathbf{q}}(V) \geq L$, thus for the same cusp $\varphi_{\mathbf{q}}(\underline{\mathbf{v}}) \geq L$ and so $\mathrm{S}_\infty(L-\varepsilon)$ is a Siegel set for Γ.

By [PR92][Proposition 4.11], for all Γ there exists an L such that $\mathrm{S}_\infty(L)$ is a Siegel set for Γ. So there is a set of cusps $Q \subset \mathcal{C}_K(\mathrm{S}_\infty(L))$ such that if $\mathbf{q} \notin Q$, then $\mathrm{e}_{\mathbf{q}}(\underline{\mathbf{v}}) \leq 0$ for all $\underline{\mathbf{v}} \in \mathrm{S}_\infty(L)$ and necessarily, $\mathbf{q} \in \mathcal{C}_{K\delta}$ where $\delta \leq \frac{2}{L}$. Let $\mathbf{q} \in Q$, then by Proposition 5.6.2 and Lemma 5.9.2 either $\mathbf{q} \in Q_i$ for some Q_i, or there exists a cusp $\mathbf{q}' \in Q_i$ such that $\varphi_{\mathbf{q}'}(\underline{\mathbf{v}}) \geq \varphi_{\mathbf{q}}(\underline{\mathbf{v}})$ for all $\underline{\mathbf{v}} \in X$, thus if Ω were continuous, i.e. $\Omega \equiv X$, then the algorithm would terminate on or before the Δ^{th} loop where $\Delta \geq \frac{4}{L^2}$. In practise the set Ω is not continuous, but on the Δ^{th} loop the resolution is set to

$$N = \left(\frac{c_1 - \sqrt{c_1^2 - 4\frac{2(\alpha-1)}{\delta} c_2}}{2c_2} \right)^{\frac{2}{1-2n}}$$

so by Lemma 5.7.1, $\varepsilon_i \leq \frac{1}{2}\left(\frac{m}{N}\right)^{\frac{2}{1-2n}}$ and therefore $\lim_{\delta\to\infty} \varepsilon_i = 0$. Thus by the continuity of the effect function and given that ε_i is monotone decreasing function of δ, then for all $V \in \Omega$, $\lim_{\delta\to\infty} \Phi_{\mathbf{q}}(V) = \varphi_{\mathbf{q}}(\underline{\mathbf{v}}') \geq L$ since $V \to \underline{\mathbf{v}}'$ where $\underline{\mathbf{v}}'$ is the midpoint of V. As such there must exist some finite δ for which $\Phi_{\mathbf{q}}(V) > 0$ for all $V \in \Omega$ and therefore the algorithm terminates. ∎

Bibliography

[Coh00] Henri Cohen. *Advanced topics in computational number theory*, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[FL03] Gábor Francsics and Peter D. Lax. A fundamental domain for the Picard modular group. *ESI preprint*, 2003.

[FL05] Gábor Francsics and Peter D. Lax. A semi-explicit fundamental domain for a Picard modular group in complex hyperbolic space. In *Geometric analysis of PDE and several complex variables*, volume 368 of *Contemp. Math.*, pages 211–226. Amer. Math. Soc., Providence, RI, 2005.

[FP06] Elisha Falbel and John Parker. The geometry of the Eisenstein-Picard modular group. *Duke Math. J.*, 131(2):249–289, 2006.

[Gol99] William M. Goldman. *Complex hyperbolic geometry*. Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York, 1999. Oxford Science Publications.

[PR92] Vladimir Platonov and Andreĭ Rapinchuk. *Algebraic groups and number theory*. Boston Academic Press, 1992.

[PTVF92] William H. Press, Saul A. Teukolsky, William T. Vetterling, and Brian P. Flannery. *Numerical recipes in C*. Cambridge University Press, Cambridge, second edition, 1992. The art of scientific computing.

[Yas05] Dan Yasaki. *On the existence of spines for $\mathbb{Q}$-rank 1 groups*. PhD thesis, Duke University, 2005.

[Zin79] Thomas Zink. Über die Anzahl der Spitzen einiger arithmetischer Untergruppen unitärer Gruppen. *Math. Nachr.*, 89:315–320, 1979.