F. S. Kalker

Reduction of binary forms over discrete complex principal ideal domains

Bachelor thesis

March 23, 2023

Thesis supervisor: Dr. T.C. Streng

Leiden University
Mathematical Institute

Contents

1 Introduction

A *binary form* is a homogeneous polynomial in two variables, for example

$$\begin{aligned}F(X,Z) = {} & (-345117947278637540 - 5573462011296016 87i)X^6 \\ & + (139680088221948568187 - 1928517650300333522 66i)X^5Z \\ & + (35030008596671180091651 + 8472805989353978220340i)X^4Z^2 \\ & + (44110094143931728796908 3 + 2875545097232627721377912i)X^3Z^3 \\ & + (-11317862181637361544257 3605 + 6811008492736756717295 2422i)X^2Z^4 \\ & + (-25666120500722404158582 18695 - 1909095637617069339428 945974i)XZ^5 \\ & + (79854202645916692233020 54474 - 3127241565296649273377 6691049i)Z^6,\end{aligned}$$

and

$$G(X,Z) = X^6 + X^5Z + X^4Z^2 + X^3Z^3 + X^2Z^4 + XZ^5 + Z^6 \in \mathbb{Z}[i][X,Z].$$

These binary forms are *equivalent*, because there exists an invertible change of coordinates transforming one into the other:

$$G(X,Z) = F\left(\begin{pmatrix} 703+588i & -16769+52890i \\ 79+43i & -592+5413i \end{pmatrix} \cdot \begin{pmatrix} X \\ Z \end{pmatrix}\right).$$

This reduction of a binary form with big coefficients to a binary form with small coefficients has applications to the study of hyperelliptic curves and cryptography.

Gaston Julia layed the foundation of the reduction of binary forms in his thesis in 1917 [6] using earlier work of Charles Hermite [4]. Julia formulated a method for reducing square-free binary forms with integer coefficients of degrees 3 and 4. Cremona gave a reformulation of these methods in 2003, which were computationally more practical [2]. Stoll and Cremona generalised this to complex binary forms of degree $n \geq 3$, with some restrictions on the the multiplicities of their zeros [10]. In a follow-up paper, Hutz and Stoll were able to give explicit bounds on the size of the coefficients of a binary form after it is reduced, and used this to construct an algorithm to find the binary form in the $\mathrm{SL}_2(\mathbb{Z})$ orbit with the lowest possible coefficients [5].

In this Bachelor thesis we will cover the methods of Stoll and Cremona. We will extend these methods to all discrete principal ideal domains that are subrings of $\mathbb{C}$. In addition, we will also cover the algorithm for optimal reduction of real binary forms over $\mathrm{SL}_2(\mathbb{Z})$ from Hutz and Stoll, and generalise this to binary forms with coefficients in discrete norm-Euclidean subrings of $\mathbb{C}$.

Basic knowledge about linear algebra, group theory, ring theory and topology is required to read this thesis.

2 Binary forms and the special linear group

In the following section we let R be a subring of $\mathbb{C}$ and n a positive integer.

Definition 2.1. A *binary form* $F = F(X, Z)$ over R is a homogeneous polynomial in two variables over R. We will denote the set of all binary forms of degree n by $R[X, Z]_n$.

There exists a right action of $\mathrm{SL}_2(R)$ on $R[X, Z]_n$, given by the following formula:

$$F(X, Z) \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = F(aX + bZ, cX + dZ). \tag{2.2}$$

One can simply view this as a composition of $F(X, Z)$ with a linear map in $\mathrm{SL}_2(R)$, It is then clear that this defines a right action on $R[X, Z]_n$.

The primary goal of this thesis will be to determine a matrix $\gamma \in \mathrm{SL}_2(R)$ such that the coefficients of $F \cdot \gamma$ are small, in the following sense:

Definition 2.3. Let $F = a_0X^n + a_1X^{n-1}Z + \cdots + a_nZ^n \in \mathbb{C}[X, Z]_n$ be a binary form of degree n. We define

- the *size* of F to be $\|F\| = \sum_{j=0}^{n} |a_j|^2$,
- the *height* of F to be $H(F) = \max_{0 \leq j \leq n} |a_j|$.

Given a binary form F over R, we want to find $\gamma \in \mathrm{SL}_2(R)$ such that $\|F\|$ is small relative to the other binary forms in its orbit under the action of $SL_2(R)$. Because of the inequalities $n \cdot H(F)^2 \geq \|F\| \geq H(F)^2$, the size $\|F\|$ being small implies that the height $H(F)$ will also be small. When trying to find a binary form in the $\mathrm{SL}_2(R)$ orbit of F with the lowest size or height, this distinction will be relevant, and we will describe a way to find both for square-free binary forms over some suitable subrings of $\mathbb{C}$.

2.1 The zeros of binary forms

Let $F = F(X, Z)$ with coefficients in $\mathbb{C}$. We call a pair of complex numbers (α, β) a zero of F if $F(\alpha, \beta) = 0$. If n is the degree of F and $\lambda \in \mathbb{C}^*$ is a scalar, then $F(\lambda X, \lambda Z) = \lambda^n F(X, Z)$. Consequently, if (α, β) is a zero of F, then $(\lambda\alpha, \lambda\beta)$ is also a zero of F. This gives motivation for the following definition:

Definition 2.4. Let the equivalence relation $\sim$ on $\mathbb{C}^2 \setminus \{(0, 0)\}$ be given by $(z_1, z_2) \sim (z_1', z_2')$ if and only if there exists $\lambda \in \mathbb{C}^*$ such that $(z_1, z_2) = (z_1', z_2')\lambda$. We define the *complex projective line* $\mathbb{P}^1(\mathbb{C})$ to be $(\mathbb{C}^2 \setminus \{(0, 0)\})/\sim$. The equivalence class of (z_1, z_2) in $\mathbb{P}^1(\mathbb{C})$ will be denoted by $(z_1 : z_2)$.

One can interpret $\mathbb{P}^1(\mathbb{C})$ to be the set of complex lines through the origin in $\mathbb{C}^2$. If (α, β) is a zero of F, then so is the entire equivalence class $(\alpha : \beta)$. We will therefore view the zeros of a binary form F as points in $\mathbb{P}^1(\mathbb{C})$. If $(\alpha : \beta)$ is a zero of F, then $\beta X - \alpha Z$ is an irreducible factor of F. Using the fundamental theorem of algebra we also find that any binary form of degree $n \geq 1$ has at least one zero. Therefore if F is non-zero, then we can always find a decomposition F into linear factors. When none of these factors repeat up to scaling with a constant $\lambda \in \mathbb{C}^*$, we call F *square-free*. We will denote the set of all square-free binary forms over R of degree n by $R[X, Z]_n'$. When whe act on a square-free binary form $F \in R[X, Z]_n'$ with a matrix $\gamma \in \mathrm{SL}_2(R)$, the binary form $F \cdot \gamma$ will also be square-free.

There exists a natural embedding of $\mathbb{C}$ into $\mathbb{P}^1(\mathbb{C})$, called the *affine coordinate patch* φ, given by

$$\varphi : \mathbb{C} \to \mathbb{P}^1(\mathbb{C}),\ z \mapsto (z : 1). \tag{2.5}$$

The image of φ is the entirety of $\mathbb{P}^1(\mathbb{C})$ apart from the point $(1 : 0)$. We will call this point *infinity*. Because of this, the set $\mathbb{P}^1(\mathbb{C})$ is also occasionaly written as $\mathbb{C} \cup \{\infty\}$.

2.2 The action of $\mathrm{SL}_2(\mathbb{C})$ on $\mathbb{P}^1(\mathbb{C})$

As $\{(0,0)\}$ is its own $\mathrm{SL}_2(\mathbb{C})$-orbit, we can restrict the action of $\mathrm{SL}_2(\mathbb{C})$ on $\mathbb{C}^2$ to the complement of $\{(0,0)\}$, namely $\mathbb{C}^2 \setminus \{(0,0)\}$. Then two elements of the same equivalence class are always mapped to the same equivalence class. Therefore the action of $\mathrm{SL}_2(\mathbb{C})$ on $\mathbb{C}^2 \setminus \{(0,0)\}$ induces an action of $\mathrm{SL}_2(\mathbb{C})$ on $\mathbb{P}^1(\mathbb{C})$, given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} (z_1 : z_2) = (az_1 + bz_2 : cz_1 + dz_2). \tag{2.6}$$

Suppose that F is a binary form, and that $(\alpha : \beta)$ is a zero of F. Then for $\gamma \in \mathrm{SL}_2(\mathbb{C})$, the point $\gamma^{-1} \cdot (\alpha : \beta)$ is a zero of $F \cdot \gamma$.

3 The hyperbolic upper half-plane and upper half-space

We will relate the action of $\mathrm{SL}_2(\mathbb{C})$ on complex binary forms to the action of $\mathrm{SL}_2(\mathbb{C})$ on another set, the *upper half-space*. For real binary forms, we will consider a subset of this upper half-space, namely the *upper half-plane*, which invariant under the action of $\mathrm{SL}_2(\mathbb{R})$.

3.1 The upper half-plane

As we have seen in the previous section, there is an action of $\mathrm{SL}_2(\mathbb{C})$ on $\mathbb{P}^1(\mathbb{C})$. We define the upper half-plane to be a subset of $\mathbb{P}^1(\mathbb{C})$, as follows:

Definition 3.1. We define the *upper half-plane* to be $\mathcal{H} = \{(z:1) \in \mathbb{P}^1(\mathbb{C}) \mid \mathrm{Im}(z) > 0\}$

As $\mathrm{SL}_2(\mathbb{R})$ is a subgroup of $\mathrm{SL}_2(\mathbb{C})$, we also have an action of $\mathrm{SL}_2(\mathbb{R})$ on $\mathbb{P}^1(\mathbb{C})$ induced by restriction. The action of $\mathrm{SL}_2(\mathbb{R})$ on the subset $\mathcal{H}$ of $\mathbb{P}^1(\mathbb{C})$ is given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} (z:1) = (az+b : cz+d) = \left(\frac{az+b}{cz+d} : 1\right). \tag{3.2}$$

The following calculation shows that this still lies in $\mathcal{H}$:

$$\mathrm{Im}\left(\frac{az+b}{cz+d}\right) = \frac{(ad-bc)\cdot \mathrm{Im}(z)}{|cz+d|^2} = \frac{\mathrm{Im}(z)}{|cz+d|^2} > 0. \tag{3.3}$$

Therefore, the subset $\mathcal{H}$ of $\mathbb{P}^1(\mathbb{C})$ is invariant under the action of $\mathrm{SL}_2(\mathbb{R})$. Thus we have a well-defined action of $\mathrm{SL}_2(\mathbb{R})$ on $\mathcal{H}$. As $\mathcal{H}$ lies entirely within the image of the affine coordinate patch φ, we can also look at the inverse image of $\mathcal{H}$ under φ. We can write $\mathcal{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$, and the action of $\mathrm{SL}_2(\mathbb{R})$ on $\mathcal{H}$ is given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az+b}{cz+d}. \tag{3.4}$$

3.2 Correspondence with positive definite quadratic forms

We will see that there exists a correspondence between the upper half-space and *positive definite quadratic forms*, where quadratic forms are real binary forms of degree 2. A general formula for a quadratic form is $Q(X,Z) = aX^2 + 2bXZ + cZ^2$ for $a, b, c \in \mathbb{R}$. We call a quadratic form *positive definitie* if $Q(x,z) > 0$ for all $x, z \in \mathbb{R}$ not both equal to zero.

Definition 3.5. Let $Q(X,Z) = aX^2 + 2bXZ + cZ^2 \in \mathbb{R}[X,Z]_2$ be a quadratic form. We define the *discriminant* $\mathrm{disc}(Q)$ as

$$\mathrm{disc}(Q) = 4b^2 - 4ac. \tag{3.6}$$

A quadratic form Q always has two zeros in $\mathbb{P}^1(\mathbb{C})$ when counted with multiplicity. When $\mathrm{disc}(Q)$ is negative, one of its zeros will lie in $\mathcal{H}$, and the other zero will be its complex conjugate.

Lemma 3.7. *A quadratic form $Q(X,Z) = aX^2 + 2bXZ + cZ^2 \in \mathbb{R}[X,Z]_2$ is positive definite if and only if $a > 0$ and $\mathrm{disc}(Q) < 0$.*

Proof. Suppose $a > 0$ and $\mathrm{disc}(Q) < 0$. Then Q has two zeros: $(\alpha : 1)$ and $(\overline{\alpha} : 1)$, where $\alpha = -b/a + \sqrt{\mathrm{disc}(Q)}/2a$. Therefore Q can be written as $a(X - \alpha Z)(X - \overline{\alpha} Z) = a|X - \alpha Z|^2$, which is positive definite.

Conversely, if $a \leq 0$, then $Q(1,0) \leq 0$. Secondly if $\mathrm{disc}(Q) \geq 0$ and $a > 0$ both hold, then we have $Q(-b, a) = -\frac{a}{4}\mathrm{disc}(Q) \leq 0$. So Q is not positive definite if $a \leq 0$ or $\mathrm{disc}(Q) \geq 0$ □

Now let $Q(X, Z)$ be a positive definite quadratic form. Then $Q(X, Z)$ has the zero $(\alpha : 1) \in \mathcal{H}$, with α as in the proof of Lemma 3.7. Furthermore, for all $\lambda > 0$, the quadratic form $\lambda Q(X, Z)$ is still positive definite, and it has the same zero in the upper half-space. So the following map, called the *zero map*, is well-defined:

$$\begin{aligned} \xi : \{\text{positive definite quadratic forms}\}/\mathbb{R}^*_{>0} &\to \mathcal{H}, \\ aX^2 + 2bXZ + cZ^2 &\mapsto \frac{-2b + \sqrt{\operatorname{disc}(Q)}}{2a}. \end{aligned} \tag{3.8}$$

We have a right action of $\mathrm{SL}_2(\mathbb{R})$ on quadratic forms given by function composition. If $\gamma \in \mathrm{SL}_2(\mathbb{R})$ is a matrix, then $(Q \cdot \gamma)(x, z) = Q(\gamma \cdot (x, z)^\top)$, so $Q \cdot \gamma$ is still positive definite. Secondly, we have $\lambda \cdot (Q \cdot \gamma) = (\lambda \cdot Q) \cdot \gamma$ for $\lambda > 0$, and therefore there is an action of $\mathrm{SL}_2(\mathbb{R})$ on the set of positive definite quadratic forms up to scaling by a positive constant.

Lemma 3.9. *The zero map ξ is a one-to-one correspondence which respects the action of $\mathrm{SL}_2(\mathbb{R})$. More concretely, if $\gamma \in \mathrm{SL}_2(\mathbb{R})$ and Q is a positive definite quadratic form, then $\xi(Q \cdot \gamma) = \gamma^{-1} \cdot \xi(Q)$.*

Proof. We will first show that ξ is injective. Suppose two positive definite quadratic forms Q, Q' have the same zero α in the upper half-plane. Then we can write $Q = a|X - \alpha Z|^2$ and $Q' = a'|X - \alpha Z|^2$ for some $a, a' > 0$. Therefore Q and Q' differ by a positive constant, and are equal in the quotient. To show surjectivity, let $\alpha \in \mathcal{H}$. Then $(\alpha : 1)$ is a zero of the positive definite quadratic form $|X - \alpha Z|^2 = X^2 - 2\operatorname{Re}(\alpha) + |\alpha|^2 Z^2$.

We have left to show that ξ respects the action of $\mathrm{SL}_2(\mathbb{R})$. This follows from the fact that $\gamma^{-1}\xi(Q)$ is a zero of the $Q \cdot \gamma$, and every positive definite quadratic form has a unique zero in the upper half-plane. □

Because the zero map respects the action of $\mathrm{SL}_2(\mathbb{R})$, we call ξ *covariant*.

3.3 The upper half-space as a subset of the projective quaternion line

For complex binary forms, we will relate the action of $\mathrm{SL}_2(\mathbb{C})$, to an action of $\mathrm{SL}_2(\mathbb{C})$ on a three-dimensional analogy to the upper half-plane, the *upper half-space*. Lars Ahlfors describes a way to view the upper half-space as a subset of the set of quaternions, in the same way that the upper half-plane can be viewed as a subset of the complex numbers [1]. The action of $\mathrm{SL}_2(\mathbb{C})$ on the upper half-space can then be written in an elegant manner. First, we will define the *quaternions*.

Definition 3.10. The set of *quaternions* $\mathbb{H}$ is defined to be a real four-dimensional vector space with basis $1, i, j, k$, along with an $\mathbb{R}$-bilinear multiplication given by

$$\begin{aligned} i^2 = j^2 = k^2 &= -1, \\ ij = -ji &= k, \\ jk = -kj &= i, \\ ki = -ik &= j, \end{aligned} \tag{3.11}$$

along with $a \cdot 1 = 1 \cdot a = a$ for all $a \in \mathbb{H}$.

The multiplication on $\mathbb{H}$ is associative, but not commutative. This makes $\mathbb{H}$ a four-dimensional $\mathbb{R}$-algebra. We define the *conjugate* of an element $\omega = a + bi + cj + dk \in \mathbb{H}$ as $\overline{\omega} = a - bi - cj - dk$.

For any two elements $\omega_1, \omega_2 \in \mathbb{H}$ we then have $\overline{\omega_1 \cdot \omega_2} = \overline{\omega}_2 \cdot \overline{\omega}_1$. Using this we can also define a *norm* map $|\cdot| : \mathbb{H} \to \mathbb{R}_{\geq 0}$ such that

$$|\omega|^2 = \omega \cdot \overline{\omega} = a^2 + b^2 + c^2 + d^2. \tag{3.12}$$

Using this, we see that $\mathbb{H}$ is a division ring, as $\omega \cdot \overline{\omega}/|\omega|^2 = 1$ for ω non-zero. To generalise the real part and imaginary part functions on $\mathbb{C}$, we define the following four projections:

$$\begin{aligned} \mathrm{Re}(a + bi + cj + dk) &= a, \\ \pi_i(a + bi + cj + dk) &= b, \\ \pi_j(a + bi + cj + dk) &= c, \\ \pi_k(a + bi + cj + dk) &= d. \end{aligned} \tag{3.13}$$

We can view the set of complex numbers $\mathbb{C}$ as the subspace of $\mathbb{H}$ generated by 1 and i, such that the group $\mathrm{SL}_2(\mathbb{C})$ has a natural action on $\mathbb{H}^2$. As $\{(0,0)\}$ is its own orbit, the group $\mathrm{SL}_2(\mathbb{C})$ also acts on the subset $\mathbb{H}^2 \setminus \{(0,0)\}$. Similarly to how we defined the upper half-plane to be a subset of the complex projective line $\mathbb{P}^1(\mathbb{C})$, we will also define the upper half-space to be a subset of the quaternion projective line.

Definition 3.14. Define the equivalence relation $\sim$ on $\mathbb{H}^2 \setminus \{(0,0)\}$ as $(\tau_1, \tau_2) \sim (\tau_1', \tau_2')$ if and only if there exists $\lambda \in \mathbb{H}^*$ such that $(\tau_1, \tau_2) = (\tau_1', \tau_2') \cdot \lambda$. Then the *projective quaternion line* $\mathbb{P}^1(\mathbb{H})$ is defined to be $(\mathbb{H}^2 \setminus \{(0,0)\})/\sim$. Equivalence classes in $\mathbb{P}^1(\mathbb{H})$ are denoted by $(\tau_1 : \tau_2)$.

By associativity of matrix multiplication, the action of $\mathrm{SL}_2(\mathbb{C})$ on $\mathbb{H}^2 \setminus \{(0,0)\}$ respects this equivalence relation. Therefore this action induces an action of $\mathrm{SL}_2(\mathbb{C})$ on $\mathbb{P}^1(\mathbb{H})$, given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} (\tau_1 : \tau_2) = (a\tau_1 + b\tau_2 : c\tau_1 + d\tau_2). \tag{3.15}$$

Similar to the way $\mathbb{C}$ is embedded into $\mathbb{P}^1(\mathbb{C})$, there is a natural embedding of $\mathbb{H}$ into $\mathbb{P}^1(\mathbb{H})$. We again call this embedding the *affine coordinate patch*, defined as

$$\varphi : \mathbb{H} \to \mathbb{P}^1(\mathbb{H}),\ \omega \mapsto (\omega : 1). \tag{3.16}$$

Definition 3.17. We define the *upper half-space* $\mathcal{H}_3$ as the subset

$$\{(a + bi + cj : 1) \mid a, b, c, \in \mathbb{R},\ c > 0\} \subset \mathbb{P}^1(\mathbb{H}). \tag{3.18}$$

The action of $\mathrm{SL}_2(\mathbb{C})$ on the upper half-space can be written as

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} (\omega : 1) = (a\omega + b : c\omega + d) = \left((a\omega + b)(c\omega + d)^{-1} : 1\right). \tag{3.19}$$

Using the following equations we find that $\mathcal{H}_3$ is invariant under the action of $\mathrm{SL}_2(\mathbb{C})$:

$$\pi_j((a\omega + b)(c\omega + d)^{-1}) = \frac{\mathrm{Re}(ad - bc)\pi_j(\omega)}{|c\omega + d|^2} = \frac{\pi_j(\omega)}{|c\omega + d|^2} > 0, \tag{3.20}$$

$$\pi_k((a\omega + b)(c\omega + d)^{-1}) = \frac{\mathrm{Im}(ad - bc)\pi_j(\omega)}{|c\omega + d|^2} = 0, \tag{3.21}$$

where a, b, c, d are complex numbers with $ad - bc = 1$. As $\mathcal{H}_3$ is contained in the image of the affine coordinate patch φ, we will often identify $\mathcal{H}_3$ with its inverse image under φ. The action of $\mathrm{SL}_2(\mathbb{C})$ on $\mathcal{H}_3$ can then be written as

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \omega = (a\omega + b)(c\omega + d)^{-1}. \tag{3.22}$$

We can view the upper half-plane $\mathcal{H}$ as a subset of the upper half-space $\mathcal{H}_3$, using the map $a + bi \mapsto a + bj$. Then $\mathcal{H}$ can be identified with the subset of $\mathcal{H}_3$ consisting of all elements $\tau + uj$ with $\mathrm{Im}(\tau) = 0$.

3.4 Correspondence to positive definite Hermitian forms

In the previous section we have seen that there exists a correspondence between the upper half-plane and the set of positive definite quadratic forms up to scaling with a positive constant. We can extend this correspondence to the upper half-space by extending positive definite quadratic forms to their complex analogy: *positive definite Hermitian forms*. A *Hermitian form* can be represented as $Q(X, Z) = a|X|^2 + bX\overline{Z} + \overline{bX}Z + c|Z|^2$, with $a, c \in \mathbb{R}$ and $b \in \mathbb{C}$ [10].

Definition 3.23. Let $Q(X, Z) = a|X|^2 + bX\overline{Z} + \overline{bX}Z + c|Z|^2$ be a Hermitian form. We define the *discriminant* $\mathrm{disc}(Q)$ of Q to be $4|b|^2 - 4ac$.

A Hermitian form is called *positive definite* if $Q(x, z) > 0$ for all $x, z \in \mathbb{C}$ not both equal to zero.

Lemma 3.24. *A Hermitian form $Q(X, Z) = a|X|^2 + bX\overline{Z} + \overline{bX}Z + c|Z|^2$ for $a, c \in \mathbb{R}$ and $b \in \mathbb{C}$ is positive definite if and only if $a > 0$ and $\mathrm{disc}(Q) < 0$.*

Proof. Suppose $a > 0$ and $\mathrm{disc}(Q) < 0$. We can write $Q(X, Z) = a|X + \overline{b}/aZ|^2 - \mathrm{disc}(Q)/a|Z|^2$, which is clearly positive definite.

Now suppose $a \leq 0$. Then we have $Q(1, 0) = a \leq 0$. Otherwise if $a > 0$ and $\mathrm{disc}(Q) \geq 0$, then we have $Q(-\overline{b}, a) = -a(|b|^2 - ac) \leq 0$. So if either $a \leq 0$ or $\mathrm{disc}(Q) \geq 0$ holds, the Hermitian form Q is not positive definite. □

We will define a correspondence between the upper half-space and the set of positive definite Hermitian forms, up to scaling with a positive constant. First define

$$\begin{aligned} \psi : \mathbb{P}^1(\mathbb{H}) &\to \{\text{maps } \mathbb{C}^2 \to \mathbb{R}_{\geq 0}\}/\mathbb{R}^*_{>0}, \\ (\alpha : \beta) &\mapsto \left[(X, Z) \mapsto |X\beta - Z\alpha|^2\right]. \end{aligned} \tag{3.25}$$

If we multiply $\alpha, \beta \in \mathbb{H}$ by some scalar $\lambda \in \mathbb{H}^*$ on the right, then $\psi(\alpha\lambda : \beta\lambda) = \psi(\alpha : \beta) \cdot |\lambda|^2$. It follows that this map is well-defined. When we restrict ψ to the upper half-plane, we can write $\psi(\omega : 1) = |X - Z\omega|^2 = |X - Z\tau|^2 + u^2|Z|^2$ with $\omega = \tau + uj$, where we used that X and Z only take values in $\mathbb{C}$. This is a positive definite Hermitian form.

Proposition 3.26. *The map $\psi|_{\mathcal{H}_3} : \mathcal{H}_3 \to \{\text{positive definite Hermitian forms}\}/\mathbb{R}^*_{>0}$ is a bijection, with inverse given by*

$$a|X|^2 + bX\overline{Z} + \overline{bX}Z + c|Z|^2 \mapsto \left(\frac{-2\overline{b} + j\sqrt{-\mathrm{disc}(Q)}}{2a} : 1\right). \tag{3.27}$$

This proposition follows from quick calculation which we leave to the reader. We call the inverse of $\psi|_{\mathcal{H}_3}$ the *zero map*, denoted by ξ, and for all positive definite Hermitian forms Q we call $\xi(Q)$ the point in the upper half-space *corresponding* to Q.

There is a right action of $\mathrm{SL}_2(\mathbb{C})$ on the set of maps $\mathbb{C}^2 \to \mathbb{R}_{\geq 0}$ up to scaling with a positive constant given by function composition, and also a left action of $\mathrm{SL}_2(\mathbb{C})$ on $\mathbb{P}^1(\mathbb{H})$. If $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{C})$ is a matrix, then we have

$$\psi(\alpha : \beta) \cdot \gamma = |(aX + bZ)\beta - (cX + dZ)\alpha|^2 = |X(-c\alpha + a\beta) - Z(d\alpha - b\beta)|^2 = \psi(\gamma^{-1} \cdot (\alpha : \beta)).$$

If we now restrict ψ to $\mathcal{H}_3$, we find that ξ is *covariant*, that is, $\xi(Q \cdot \gamma) = \gamma^{-1}\xi(Q)$ for any positive definite Hermitian form Q.

We can embed the set of positive definite quadratic forms up to scaling with a positive constant into the set of positive definite Hermitian forms up to scaling with a positive constant, with the map $aX^2 + 2bXZ + cZ^2 \mapsto a|X|^2 + bX\overline{Z} + b\overline{X}Z + c|Z|^2$. With this embedding, the zero map on quadratic forms agrees with the zero map on Hermitian forms.

3.5 Hyperbolic Geometry

The upper half-plane is often endowed with a hyperbolic geometry. This geometry can also be extended to the upper half-space, which we will use to justify reduction algorithms. Hutz and Stoll used this hyperbolic metric to give an explicit upper and lower bounds on the size of a binary form [5]. We will also define a generalised notion of distance to the *ideal boundary* of the upper half-space. This generalised distance was first given by Stoll and Cremona in order to obtain geometric intuition for the reduction of complex binary forms [10].

In order to define the metric on $\mathcal{H}_3$, we need to consider *paths* in $\mathcal{H}_3$, defined as continuously differentiable maps from $[0, 1]$ to $\mathcal{H}_3$.

Definition 3.28. Let $\gamma : [0, 1] \to \mathcal{H}_3$ be a path. Then the length $L(\gamma)$ of γ is defined as the integral

$$L(\gamma) = \int_0^1 \frac{|\gamma'(t)|}{\pi_j(\gamma(t))} \mathrm{d}t. \tag{3.29}$$

We define for any $\omega_1, \omega_2 \in \mathcal{H}$

$$d(\omega_1, \omega_2) = \inf\{L(\gamma) : \gamma \text{ is a path from } \omega_1 \text{ to } \omega_2\}. \tag{3.30}$$

All of the maps induced by the action of $\mathrm{SL}_2(\mathbb{C})$ are isometries using this metric. As we can view the upper half-plane as a subset of the upper half-space, the upper half-plane inherits a metric. This metric is the same as the usual hyperbolic metric on the upper half-plane, defined analogously. The group $\mathrm{SL}_2(\mathbb{R})$ acts on the upper half-plane using isometries in this metric [1].

We will now give a generalised notion of distance of points in the upper half-space, to points in the *ideal boundary*. We will use this generalised distance to obtain some geometric intuition of one of the maps from the set of binary forms to the upper half-space, which we will define in the following section. This generalised notion of distance will not be necessary for our reduction algorithms, so it can be skipped by the reader.

Recall that we can write $\mathcal{H}_3 = \{(\omega : 1) \mid \omega \in \mathbb{H}, \pi_j(\omega) > 0, \pi_k(\omega) = 0\}$. We will define the ideal boundary $\partial\mathcal{H}_3$ of $\mathcal{H}_3$ as $\{(\tau : 1) \mid \tau \in \mathbb{C}\} \cup \{(0 : 1)\} \subset \mathbb{P}^1(\mathbb{H})$. We can identify this with the set $\mathbb{P}^1(\mathbb{C})$. The zeros of a binary form can now be viewed as elements of the ideal boundary $\partial\mathcal{H}_3$.

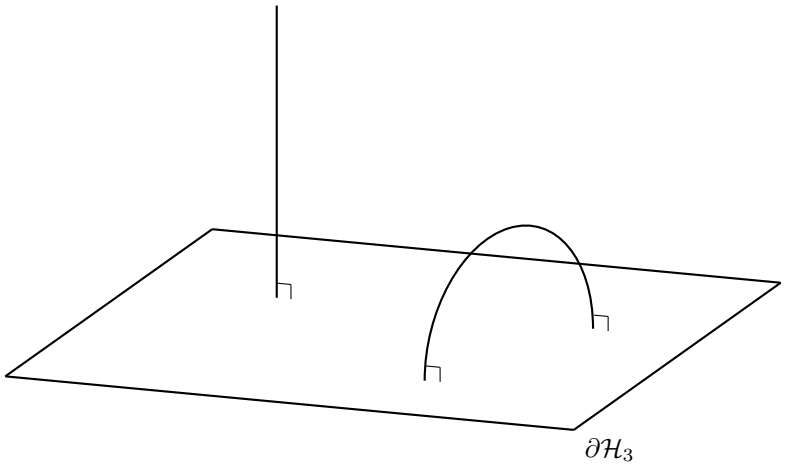


Figure 1: Geodesics in $\mathcal{H}_3$

Definition 3.31. Let $\omega = \tau + uj \in \mathcal{H}_3$ and $z \in \mathbb{C} \subset \partial\mathcal{H}_3$. Then we define the *generalised distance* d_∂ between these points as

$$d_\partial(\omega, z) = \log\left(\frac{|\omega - z|^2}{u}\right) = \log\left(\frac{|\tau - z|^2 + u^2}{u}\right). \tag{3.32}$$

For $z = \infty$, we define the generalised distance as

$$d_\partial(\omega, \infty) = \log\left(\frac{1}{u}\right). \tag{3.33}$$

Note that these generalised distances can be negative.

We define *geodesics* to be locally length-minimizing curves. The geodesics of the upper half-space using this metric, are either vertical lines or vertical half-circles, as shown in Firgur 1 Every geodesic intersects the ideal boundary $\partial\mathcal{H}_3 = \mathbb{P}^1(\mathbb{C})$ exactly twice. Using these geodesics we can express the distance between two points ω_1, ω_2 using the generalised distance.

Lemma 3.34. *Let $\omega_1, \omega_2 \in \mathcal{H}_3$, and let z be one of the two points where the geodesic connecting ω_1 and ω_2 intersects the ideal boundary $\partial H_3 = \mathbb{P}^1(\mathbb{C})$. Then the following equality holds:*

$$d(\omega_1, \omega_2) = |d_\partial(\omega_1, z) - d_\partial(\omega_2, z)|. \tag{3.35}$$

We will not be proving this here. This was first noted by Stoll and Cremona [10]. Elezi and Shaska proved this using an alternative definition of the hyperbolic geometry on the upper half-space [3]. Lars Ahlfors shows that these definitions agree [1].

The action of $\mathrm{SL}_2(\mathbb{C})$ does not preserve distances between points in $\mathcal{H}_3$ and points on the edge. The distance changes by an additive constant, depending on the matrix $\gamma \in \mathrm{SL}_2(\mathbb{C})$ and the point on the edge, but not on the point in $\mathcal{H}_3$ [10]. This constant cancels in equation 3.35.

4 Covariant maps to the upper half-plane

For the reduction of binary forms, we will restrict ourselves to square-free binary forms of degree $n \geq 3$. We will need this restriction to define two maps from the set of complex square-free binary forms to the upper half-space, as Stoll and Cremona give in their paper in 2003 [10]. These maps will have the important property that they are *covariant* with respect to the action of $\mathrm{SL}_2(\mathbb{C})$ on both the set of binary forms and the upper half-space. Using this property we can relate the action of $\mathrm{SL}_2(\mathbb{C})$ on the set of binary forms to the action of $\mathrm{SL}_2(\mathbb{C})$ on the upper half-space. In a later paper, Hutz and Stoll give explicit bounds on the size of a binary form in terms of the distance between the point $j \in \mathcal{H}_3$ and the image of F under one of these covariant maps [5].

4.1 The covariant z

Gaston Julia dealt with the reduction of binary forms with integer coefficients of degrees 3 and 4 in his thesis in 1917 [6]. Stoll and Cremona generalised his work to complex binary forms of degree $n \geq 3$, with some restrictions on the multiplicities on the zeros. Let $F \in \mathbb{C}[X,Z]'_n$ be a square-free binary form. Stoll and Cremona often assumed F has no zeros at infinity. We will generalise their methods here so this assumption is not necessary. Write $F = \prod_{j=1}^{n}(\beta_j X - \alpha_j Z)$. We then assign the following class Hermitian forms up to sclaing to F:

$$Q(F)(X,Z) = \sum_{j=1}^{n} t_j |\beta_j X - \alpha_j Z|^2, \tag{4.1}$$

where the t_j are positive real numbers chosen in such a way as to minimize

$$\theta(t_1,\ldots,t_n) = \frac{|\operatorname{disc}(Q(F))|^{n/2}}{n^n t_1 t_2 \cdots t_n}. \tag{4.2}$$

Note that $\theta(t_1,\ldots,t_n)$ is invariant under simultaneous scaling of all of the t_i with a positive scalar. We will show later that the $t = (t_1,\ldots,t_n)$ is uniquely determined up to scaling, and that $Q(F)$ is independent of the choice of factorisation of F.

Definition 4.3. Let F be a square-free binary form of degree $n \geq 3$. Then $z(F)$ is defined as the point in the upper half-plane corresponding to $Q(F)$.

We can assume without loss of generality that $t_1 t_2 \cdots t_n = 1$ holds, as $\theta(t_1,\ldots,t_n)$ is invariant under scaling of t. Finding $Q(F)$ then comes down to minimizing $|\operatorname{disc}(Q(F))|$ under this constraint.

Using $|\beta_j X - \alpha_j Z|^2 = |\beta|^2|X|^2 + \beta\overline{\alpha}X\overline{Z} + \overline{\beta}\alpha\overline{X}Z + |\alpha|^2|Z|^2$ we obtain the following equation:

$$Q = \sum_{j=1}^{n} t_j|\beta_j|^2|X|^2 + \sum_{j=1}^{n} t_j\beta_j\overline{\alpha_j}X\overline{Z} + \sum_{j=1}^{n} t_j\overline{\beta_j}\alpha_j\overline{X}Z + \sum_{j=1}^{n} t_j|\alpha|^2|Z|^2. \tag{4.4}$$

We now find for $\operatorname{disc}(Q)$:

$$\begin{aligned} \tfrac{1}{4}|\operatorname{disc}(Q)| &= \left(\sum_{j=1}^{n} t_j|\beta_j|^2\right)\left(\sum_{j=1}^{n} t_j|\alpha_j|^2\right) - \left|\sum_{j=1}^{n} t_j\beta_j\overline{\alpha}_j\right|^2 \\ &= \sum_{j=1}^{n}\sum_{k=1}^{n} t_j t_k(|\beta_j|^2|\alpha_k|^2 - \overline{\beta}_j\beta_k\alpha_j\overline{\alpha}_k) \\ &= \sum_{j<k} t_j t_k|\beta_j\alpha_k - \beta_k\alpha_j|^2. \end{aligned} \tag{4.5}$$

We introduce the variables $u_1, \ldots, u_n$ such that $t_j = \exp u_j$ for all $1 \leq j \leq n$, i.e. $u_j = \log(t_j)$. This is possible because the t_j are all positive. The constraint $t_1 t_2 \cdots t_n = 1$ is then equivalent to $\sum_j u_j = 0$. Minimizing the discriminant is now reduced to minimizing the function

$$D(u) = \sum_{j<k} |\beta_j \alpha_k - \beta_k \alpha_j|^2 \exp(u_j + u_k), \tag{4.6}$$

on the subspace given by $\sum_j u_j = 0$.

Lemma 4.7 (Lemma 4.2 in [10])**.** *If F is a square-free binary form of degree $n \geq 3$, then D is strictly convex from below on $\mathbb{R}^n$. Furthermore, D attains a unique minimum on the subspace V_0 of $\mathbb{R}^n$ given by $\sum_j u_j = 0$*

Proof. This is a slight generalisation of Lemma 4.2 from Stoll and Cremona, as they assume F has no zero at infinity. However, the proof is the analogous. See [10]. □

Let $(u_1, \ldots, u_n)$ be the unique minimum of $D|_{V_0}$. Then for the Hermitian form $Q(F)$ we find $Q(F) = \sum_{j=1}^n \exp(u_j)|\beta_j X - \alpha_j Z|^2$. Now $z(F)$ is the point in $\mathcal{H}_3$ corresponding to $Q(F)$. We define the quantity $\theta(F)$ to be the minimal value of $\theta(t_1, \ldots, t_n)$.

Lemma 4.8. *The Hermitian form $Q(F)$ is well-defined up to scaling, and the map $F \mapsto Q(F)$ is covariant. Consequently, $z(F)$ is also well-defined and covariant. Furthermore, the map $F \mapsto \theta(F)$ is invariant under the action of* $\mathrm{SL}_2(\mathbb{C})$.

Proof. First we will prove that $Q(F)$ is well-defined up to scaling. Given two factorisations $\prod_{j=1}^n (\beta_j X - \alpha_j Z) = \prod_{j=1}^n (\beta'_j X - \alpha'_j Z)$ of F into linear factos, there exist constants $c_j \in \mathbb{C}$ wich $c_1 c_2 \cdots c_n = 1$ and a permutation $\sigma \in S_n$ such that $(\beta_j, \alpha_j) = c_j(\beta_{\sigma(j)}, \alpha_{\sigma(j)})$. As reordering has no effect on the Hermitian form $Q(F)$, we can assume that σ is the identity map. The constants c_j correspond to multiplying t_j with a factor of $|c_j|^2$ in (4.1). This is simply a reparametrisation of the t_j which leaves $t_1 t_2 \ldots t_n$ invariant, so this will have no effect on the quadratic form $Q(F)$. Secondly by Lemma 4.7, the vector t is uniquely determined up to scaling by a positive constant. Therefore $Q(F)$ is well-defined up to scaling. As a result the corresponding point $z(F)$ is also well-defined.

To prove covariance, let $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{C}$. Then we have

$$\beta_1 \alpha_2 - \beta_2 \alpha_1 = \begin{pmatrix} \alpha_1 & \beta_1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix}. \tag{4.9}$$

Now let $\gamma \in \mathrm{SL}_2(\mathbb{C})$ and define $\alpha'_1, \alpha'_2, \beta'_1, \beta'_2$ such that $(\alpha'_j, \beta'_j)^\top = \gamma(\alpha, \beta)^\top$. We find

$$\beta'_1 \alpha'_2 - \beta'_2 \alpha'_1 = \begin{pmatrix} \alpha_1 & \beta_1 \end{pmatrix} \gamma^\top \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \gamma \begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix} = \begin{pmatrix} \alpha_1 & \beta_1 \end{pmatrix} \begin{pmatrix} 0 & -\det\gamma \\ \det\gamma & 0 \end{pmatrix} \begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix}. \tag{4.10}$$

Hence, $\beta'_1 \alpha'_2 - \beta'_2 \alpha'_1 = \beta_1 \alpha_2 - \beta_2 \alpha_1$. Let F be a complex square-free binary form of degree $n \geq 3$. Using this equality we find that the function $D(u)$ is invariant under the action of $\mathrm{SL}_2(\mathbb{C})$ on F. Therefore, the same t_j minimize θ in (4.2) for both F and $F \cdot \gamma$. This implies that θ is an invariant, and $Q(F \cdot \gamma) = Q(F) \cdot \gamma$. Now $z(F \cdot \gamma) = \gamma^{-1} z(F)$ follows from the covariance of the zero map. □

If F is complex binary form, then the zeros of its conjugate $\overline{F}$ are equal to the conjugates of the zeros of F. Therefore the map D is invariant under conjugation of F, so the same t_i minimize $\theta(t_1, \ldots, t_n)$. Using this we find $Q(\overline{F})(X, Z) = Q(F)(\overline{X}, \overline{Z})$. Therefore the corresponding point $z(\overline{F})$ in the upper half-space is equal to $z(F)$ with its i-part multiplied by -1. If F is real, then $F = \overline{F}$. As a consequence the i-part of $z(F)$ is equal to 0, and $z(F)$ is an element of the embedding of the upper half-space into the upper half-plane.

According to Lemma 4.7, computing $z(F)$ numerically comes down to finding the minimum of a convex function. For this thesis I have implemented this into the program SageMath. There are numerous algorithms to find this minimum, for example Newton iteration, gradient descent or the Broyden-Fletcher-Goldfarb-Shanno algorithm, the latter of which is used in this implementation. The SageMath code can be found in Appendix B.

Hutz and Stoll computed upper and lower bounds on $\|F\|$, depending on the hyperbolic distance between the covariant point $z(F)$ and $j \in \mathcal{H}_3$, and the value $\theta(F)$. The main theorem from their paper is as follows:

Theorem 4.11 (Theorem 4.7 from Hutz and Stoll [5])**.** *Let $F \in \mathbb{C}[X, Z]_n$ be a square-free binary form of degree $n \geq 3$ and let $\delta = \cosh d(z(F), j)$. There exists a constant $\varepsilon(F) \in \mathbb{R}_{>0}$ such that the following inequalities hold:*

$$\varepsilon(F)\delta^{n-2} \leq \frac{\|F\|}{\theta(F)} \leq 2^{-n} \binom{2n}{n} \delta^n. \tag{4.12}$$

This $\varepsilon(F)$ differs by a factor of 2^{n-1} from the definition used by Hutz and Stoll. In their paper they give an explicit expression for $\varepsilon(F)$. Let $F \in \mathbb{C}[X, Z]'_n$ be a square-free binary form of degree $n \geq 3$. Because $\mathrm{SL}_2(\mathbb{C})$ acts transitively on the upper half-space, there exists a matrix $\gamma_0 \in \mathrm{SL}_2(\mathbb{C})$ such that $z(F_0) = j$, where $F_0 = F \cdot \gamma_0$. The zeros α_k of F_0 are elements of $\mathbb{P}^1(\mathbb{C})$. We can view the set $\mathbb{P}^1(\mathbb{C})$ as a sphere in $\mathbb{R}^3$ using the inverse of the *stereographic projection*. The inverse images under the stereographic projection of the zeros α_k are given by

$$\phi_k = \begin{cases} \left(\frac{2 \operatorname{Re} \alpha_k}{|\alpha_k|^2+1}, \frac{2 \operatorname{Im} \alpha_k}{|\alpha_k|^2+1}, \frac{|\alpha_k|^2-1}{|\alpha_k|^2+1} \right), & \text{if } \alpha_k \in \mathbb{C}, \\ (0, 0, 1), & \text{if } \alpha_k = \infty. \end{cases} \tag{4.13}$$

Then $\varepsilon(F_0)$ is defined as follows:

$$\varepsilon(F_0) = 2^{-n} \left(1 - \max_{k \neq k'} \sqrt{\frac{\langle \phi_k, \phi_{k'} \rangle + 1}{2}} \right)^{n-1}. \tag{4.14}$$

Now we define $\varepsilon(F)$ to be equal to $\varepsilon(F_0)$. This definition does not depend on the choice of γ_0 [5]. As a result the map $F \mapsto \varepsilon(F)$ is invariant under the action of $\mathrm{SL}_2(\mathbb{C})$ on $\mathbb{C}[X, Z]'_n$. Because F is square-free, all of the ϕ_k are different. Hence $\langle \phi_k, \phi_{k'} \rangle$ is strictly smaller than 1 for $k \neq k'$. This implies that $\varepsilon(F) > 0$ for all square-free binary forms F.

As cosh is strictly increasing on $\mathbb{R}_{\geq 0}$, both the upper and lower bound on the size $\|F\|$ of a binary form $F \in \mathbb{C}[X, Z]'_n$ are minimal when $d(z(F), j)$ is minimal. Since $\mathrm{SL}_2(\mathbb{C})$ acts transitively on $\mathcal{H}_3$, we can immediately define a reduction algorithm over $\mathrm{SL}_2(\mathbb{C})$. If we determine $\gamma \in \mathrm{SL}_2(\mathbb{C})$ such that $\gamma^{-1} z(F) = j$, then $F \cdot \gamma$ will have the lowest possible upper and lower bound on $\|F \cdot \gamma\|$. However, this is of course no guarantee that $\|F \cdot \gamma\|$ is minimal. Similarly, to reduce real binary forms, which have their covariant point in the upper half-plane, over $\mathrm{SL}_2(\mathbb{R})$, we can determine $\gamma \in \mathrm{SL}_2(\mathbb{R})$ such that $z(F \cdot \gamma) = i$.

For reduction of F over $\mathrm{SL}_2(R)$, with R a discrete complex principal ideal domain, the strategy will be the same. We will determine $\gamma \in \mathrm{SL}_2(R)$ such that $d(z(F \cdot \gamma), j)$ is minimal, and then $\|F \cdot \gamma\|$ will have the lowest possible upper and lower bound.

Corollary 4.15. *Let $F \in \mathbb{C}[X, Z]_n$ be a square-free binary form of degree $n \geq 3$, and let $\gamma \in \mathrm{SL}_2(\mathbb{C})$. If the inequality*

$$\cosh d(\gamma^{-1} z(F), j) > \left(\frac{\|F\|}{\varepsilon(F)\theta(F)} \right)^{1/(n-2)} \tag{4.16}$$

holds, then $\|F \cdot \gamma\| > \|F\|$.

Proof. Define $\delta = \cosh d(\gamma^{-1} z(F), j)$. Then (4.16) is equivalent to $\varepsilon(F)\theta(F)\delta^{n-2} > \|F\|$. The implication $\|F \cdot \gamma\| > \|F\|$ now immediately follows from the lower bound given in Theorem 4.11 applied to the binary form $F \cdot \gamma$, and the invariance of θ and ε under $\mathrm{SL}_2(\mathbb{C})$. □

For discrete *norm-Euclidean* subrings $R \subset \mathbb{C}$, we will be able to use this explicit condition to determine the binary form with minimal size in the orbit of F. Let c be the right hand side in equation (4.16). If we iterate over all matrices $\gamma \in \mathrm{SL}_2(R)$ with $d(z(F \cdot \gamma), j) < c$ and check for which matrix the size $\|F \cdot \gamma\|$ is minimal, then we have found the binary form with minimal size in the entire $\mathrm{SL}_2(R)$-orbit of F. We will see later that there are indeed finitely many $\gamma \in \mathrm{SL}_2(R)$ for which $d(z(F \cdot \gamma)) < c$ holds.

To find the the binary form in the orbit of F with minimal height, we can use the inequalities $n \cdot H(F)^2 \geq \|F\| \geq H(F)^2$. If $\|F \cdot \gamma\| \geq n \cdot H(F)^2$, then $H(F \cdot \gamma) \geq H(F)$. Thus we need to replace $\|F\|$ with $n \cdot H(F)^2$ in the right-hand side of equation (4.16), to obtain the inequality

$$\cosh d(\gamma^{-1} z(F), j) > \left(\frac{n \cdot H(F)^2}{\varepsilon(F)\theta(F)} \right)^{1/(n-2)}. \tag{4.17}$$

If this inequality holds for a square-free binary form F and $\gamma \in \mathrm{SL}_2(\mathbb{C})$, then $H(F \cdot \gamma) > H(F)$.

Stoll and Cremona also give a reformulation of the covariant map z. Hutz and Stoll use this alternative definition of the covariant z to prove Theorem 4.11. This reformlation also allows for a geometric interpretation using the generalised notion of distance.

Let $n \geq 3$ be an integer. Then we define the map $R : \mathbb{C}[X, Z]'_n \times \mathcal{H}_3 \to \mathbb{R}_{\geq 0}$ as follows. For square-free binary form F we first write $F = \prod_{j=1}^{n} (\beta_j X - \alpha_j Z)$. We define $R(F, \tau + uj)$ as

$$R(F, \tau + uj) = \prod_{j=1}^{n} \frac{|\alpha_j - \beta_j \tau|^2 + |\beta_j|^2 u^2}{u}. \tag{4.18}$$

For a binary form F, the covariant point $z(F)$ is the unique minimizer of $R(F, -)$. Moreover, the quantity $R(F, z(F))$ is equal to $\theta(F)$ [10, Proposition 5.1].

For the geometric interpretation we will consider $\log R(F, \omega)$. As the logarithm function is strictly increasing, the value $R(F, \omega)$ is minimal in ω if and only if $\log R(F, \omega)$ is minimal. We have

$$\log R(F, \omega) = \sum_{j=1}^{n} \log \left(\frac{|\alpha_j - \beta_j \tau|^2 + |\beta_j|^2 u^2}{u} \right). \tag{4.19}$$

Stoll and Cremona then note the following:

Proposition 4.20 (Proposition 5.3 from Stoll and Cremona [10]). *The representative point $z(F)$ is the unique point in the upper half-space such that the sum of its distances from all the roots of F is minimal.*

Proof. The point $z(F)$ is equal to the unique minimizer ω of $R(F,\omega)$ shown in equation 4.19. For all zeros $(\alpha_j : \beta_j)$ of F, the term

$$\log\left(\frac{|\alpha_j - \beta_j\tau|^2 + |\beta_j|^2u^2}{u}\right)$$

is equal to $d_\partial(\tau+uj, (\alpha_j : \beta_j))$ up to some constant. This constant is equal to $2\log|\alpha_j|$ if $\beta_j = 0$, and and $2\log|\beta_j|$ else. Hence $\log R(F,\omega)$ is equal to the sum of the hyperbolic distances of ω to the zeros of F, seen as points in the ideal boundary $\partial\mathcal{H}_3 = \mathbb{P}^1(\mathbb{C})$, up to some constant only dependent on F. Therefore they have the same unique minimizer $z(F)$. □

4.2 The covariant z_0

For real square-free binary forms of degrees $n = 3$ and $n = 4$, Julia gave an explicit solution of the optimization problem of minimizing $\theta(t_1, \ldots, t_n)$. Stoll and Cremona generalised this solution to all complex square-free binary forms of degree $n \geq 3$, giving a second map to the upper half-space.

Definition 4.21. Let $F \in \mathbb{C}[X,Z]_n$ be a square-free binary form of degree $n \geq 3$ and write $F = \prod_{j=1}^n(\beta_jX - \alpha_jZ)$ for $\alpha_j, \beta_j \in \mathbb{C}$. We define the Hermitian form $Q_0(F)$ as

$$Q_0(F) = \sum_{j=1}^n \left(\prod_{\substack{k=1\\k\neq j}}^n |\alpha_j\beta_k - \alpha_k\beta_j|\right)^{\frac{-2}{n-2}} |\beta_jX - \alpha_jZ|^2, \tag{4.22}$$

and $z_0(F)$ as the point in the upper half-space corresponding to $Q_0(F)$.

Again this is a slight generalisation of the definition given by Stoll and Cremona, as they assumed the binary form F had no zero at infinity. For $n = 3, 4$, this map agrees with the covariant z. This is not necessarily the case if $n > 4$.

Lemma 4.23. *The maps Q_0 and z_0 are well-defined and covariant.*

Proof. Let F be a square-free binary form, and let $(\alpha_j : \beta_j)$ for $1 \leq n \leq j$ be it's zeros. Because F is square-free, we have $(\alpha_j : \beta_j) \neq (\alpha_k : \beta_k)$ for $j \neq k$, which implies $\alpha_j\beta_k - \beta_j\alpha_k \neq 0$. Thus, we do not divide by zero in any of the terms of $Q_0(F)$.

To show Q_0 is well-defined, we have left to show that $Q_0(F)$ is independent of the different ways of factorising F into linear terms. When we scale α_i, β_i with a factor $\lambda \in \mathbb{C}^*$, we scale the i-th term in (4.22) with a factor of $(|\lambda|^{n-1})^{-2/(n-2)} \cdot |\lambda|^2 = |\lambda|^{(2-2n)/(n-2)+2} = |\lambda|^{-2/(n-2)}$ and all other terms also with a factor of $|\lambda|^{-2/(n-2)}$. Now suppose we have two different factorisations $F = \prod_{j=1}^n(\beta_jX - \alpha_jZ)$ and $F = \prod_{j=1}^n(\beta'_jX - \alpha'_jZ)$ of F. Then there exist constants $c_1, \ldots, c_n \in \mathbb{C}$ with $c_1c_2\cdots c_n = 1$ and a permutation $\sigma \in S_n$ such that $(\alpha_j, \beta_j) = c_j(\alpha'_{\sigma(j)}, \beta'_{\sigma(j)})$. If we calculate $Q_0(F)$ using the other factorisation, it differs by a factor of $\prod_{j=1}^n |c_j|^{-2/(n-2)} = 1$. So $Q_0(F)$ is well-defined, and so is $z_0(F)$ Using equation (4.10) we find that the coefficients of $Q_0(F)$ and $Q_0(F\cdot\gamma)$ are the same. Hence $Q_0(F)\cdot\gamma = Q_0(F\cdot\gamma)$. The covariance of the zero map now gives $z(F\cdot\gamma) = \gamma^{-1}z(F)$. □

If F is a complex square-free binary form of degree $n \geq 3$, then the coefficients of $Q(\overline{F})$ are equal to the coefficients of $Q(F)$. Using this we find $Q(\overline{F})(X, Z) = Q(F)(\overline{X}, \overline{Z})$. Thus the corresponding point $z_0(\overline{F})$ is equal to $z_0(F)$ with its i-part multiplied by -1, and if F is real then $z(F)$ will lie in the embedding of the upper half-plane into the upper half-space.

For the numerical computation of $z_0(F)$, we need to numerically approximate the zeros of F. After this we can directly compute $z_0(F)$. For this thesis I have also implemented the numerical computation of $z_0(F)$ into SageMath. See the appendix for this implementation.

It is much faster to compute $z_0(F)$ than it is to compute $z(F)$, which makes this second map useful when reducing binary forms of degree $n = 3$ or $n = 4$. Also for binary forms of higher degrees, the point $z_0(F)$ is a good approximation of $z(F)$. Therefore it can be faster to use the map $z_0(F)$ in the first steps of the reduction.

5 Reduction over $\mathbb{Z}$

The covariant maps z and z_0 both map real binary forms to the embedding of the upper half-plane into the upper half-space. We will use this fact to reduce real binary forms over $\mathrm{SL}_2(\mathbb{Z})$. Theorem 4.11 tells us that we want to minimize the hyperbolic distance of the covariant point $z(F)$ of a binary form to the point j. In the embedding $\mathcal{H} \hookrightarrow \mathcal{H}_3$, the point $j \in \mathcal{H}_3$ corresponds to $i \in \mathcal{H}$. Therefore, we want to minimize the distance to i.

Consider the region $\mathcal{F}_\mathbb{Z}$ given by

$$\mathcal{F}_\mathbb{Z} = \{z \in \mathcal{H} : |\operatorname{Re}(z)| \leq \tfrac{1}{2}, |z| \geq 1\}. \tag{5.1}$$

We will show that $\mathcal{F}_\mathbb{Z}$ is a *fundamental domain* for the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathcal{H}$.

Definition 5.2. Let X be a topological space and G a group that acts on X. A subset $\mathcal{F} \subset X$ is called a *fundamental domain* if:

- for all $x \in X$, there exists $g \in G$ such that $gx \in \mathcal{F}$,
- if x is an element of the interior $\mathcal{F}^\circ$, then x is the unique point in its orbit contained in $\mathcal{F}$.

To show that $\mathcal{F}_\mathbb{Z}$ is a fundamental domain, we will first need the following lemma.

Lemma 5.3. *Let $z \in \mathcal{H}$. Then the set $\{\operatorname{Im}(\gamma z) : \operatorname{Im}(\gamma z) \geq \operatorname{Im}(z), \gamma \in \mathrm{SL}_2(\mathbb{Z})\}$ is finite.*

Proof. Let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and suppose $\operatorname{Im}(\gamma z) \geq \operatorname{Im}(z)$. Using equation 3.3 we find that $\operatorname{Im}(\gamma z) \geq \operatorname{Im}(z)$ holds if and only if $|cz + d|^2 \leq 1$. There are only finitely many pairs c, d for which this is the case, which proves the statement. □

Proposition 5.4. *The set $\mathcal{F}_\mathbb{Z}$ consists of all points in $\mathcal{H}$ that have maximal imaginary part for their $\mathrm{SL}_2(\mathbb{Z})$-orbit and have real part between $-\frac{1}{2}$ and $\frac{1}{2}$. Furthermore, it is a fundamental domain for the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathcal{H}$.*

Proof. Let $z \in \mathcal{F}_\mathbb{Z}$ and $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. The inequality $\operatorname{Im}(\gamma z) > \operatorname{Im}(z)$ is equivalent to $|cz + d| < 1$. We will show that there do not exist pairs $c, d \in \mathbb{Z}$ with $(c, d) \neq (0, 0)$ for which this strict inequality holds. As $|\operatorname{Re}(z)| \leq \frac{1}{2}$ and $|z|^2 = |\operatorname{Re}(z)|^2 + |\operatorname{Im}(z)|^2 \geq 1$, we find $\operatorname{Im}(z) \geq \frac{\sqrt{3}}{2}$. Therefore if $|cz + d| < 1$, then the only possible values for c are $-1, 0, 1$. If $c = 0$ then d is also equal to zero which is against our assumption. If $c = \pm 1$ we find $|cz + d| = |z \pm d| \geq 1$, as the real part of z cannot be reduced under translation with an integer. Therefore $\mathcal{F}_\mathbb{Z}$ does indeed consist of points with maximal imaginary part.

Now suppose a point $z \in \mathcal{H}$ has maximal imaginary part with respect to its orbit and $|\operatorname{Re}(z)| \leq \frac{1}{2}$. Then in particular we have $\operatorname{Im}(z) \geq \operatorname{Im}(\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) z) = \operatorname{Im}(z)/|z|^2$. It follows that $|z| \geq 1$, and that z is an of $\mathcal{F}_\mathbb{Z}$.

To show that $\mathcal{F}_\mathbb{Z}$ is a fundamental domain, let $z \in \mathcal{H}$. according to Lemma 5.3, the set $\{\operatorname{Im}(\gamma z) : \operatorname{Im}(\gamma z) \geq \operatorname{Im}(z), \gamma \in \mathrm{SL}_2(\mathbb{Z})\}$ is finite. As a result there exists a matrix γ such that γz has maximal imaginary part. Let n be equal to $\operatorname{Re}(\gamma z)$ rounded to a nearest integer. Then $|\operatorname{Re}(\gamma z - n)| \leq \frac{1}{2}$ and the point $\left(\begin{smallmatrix} 1 & -n \\ 0 & 1 \end{smallmatrix}\right) \gamma z$ will also have maximal imaginary part in its orbit. Hence $\left(\begin{smallmatrix} 1 & -n \\ 0 & 1 \end{smallmatrix}\right) \gamma z \in \mathcal{F}_\mathbb{Z}$. To show uniqueness let z be an element of the interior $\mathcal{F}_\mathbb{Z}^\circ$ and suppose $\gamma z \in \mathcal{F}_\mathbb{Z}$ for some matrix $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. As $\mathcal{F}_\mathbb{Z}$ consists of points with maximal imaginary part, we find $\operatorname{Im}(z) = \operatorname{Im}(\gamma z) = \operatorname{Im}(z)/|cz + d|^2$, which gives $|cz + d|^2 = 1$. As $z \in \mathcal{F}_\mathbb{Z}^\circ$, there is a strict inequality $|z| > 1$, and because $|\operatorname{Re}(z)| \leq \frac{1}{2}$, we also have $|z + n| > 1$ for all $n \in \mathbb{Z}$.

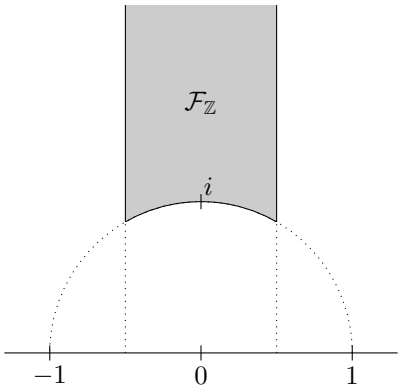


Figure 2: Fundamental domain $\mathcal{F}_{\mathbb{Z}}$ for the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathcal{H}$

Therefore $c = 0$, and we find $\gamma = \left(\begin{smallmatrix} \pm 1 & b \\ 0 & \pm 1 \end{smallmatrix}\right)$. However, if b is non-zero, then $|\operatorname{Re}(z+b)| > \frac{1}{2}$. This gives $\gamma = \pm I_2$. As I_2 and $-I_2$ both act trivially on $\mathcal{H}$ we find $\gamma z = z$. □

The proof of lemma 5.4 tells us that for all $z \in \mathcal{H}$, there exists $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma z \in \mathcal{H}$. However, it does not tell us how to find γ. To do that, we have the following algorithm.

Algorithm 5.5 Given $z \in \mathcal{H}$, find $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma z \in \mathcal{F}_{\mathbb{Z}}$.

1: Let $\gamma = I_2$
2: **while** $z \notin \mathcal{F}$ **do**
3: Determine $n \in \mathbb{Z}$ such that $|\operatorname{Re}(z+n)| \leq \frac{1}{2}$
4: Replace $\gamma \leftarrow \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \cdot \gamma$
5: Replace $z \leftarrow z + n$
6: **if** $|z| < 1$ **then**
7: Replace $\gamma \leftarrow \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \gamma$
8: Replace $z \leftarrow -z^{-1}$
9: **end if**
10: **end while**

Proof. By Lemma 5.3 there exists only finitely many possible imaginary values of points in the orbit of z that are larger than $\operatorname{Im}(z)$. In line 8 of the algorithm, the imaginary part of z strictly increases, because $\operatorname{Im}(\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) z) = \operatorname{Im}(z)/|z|^2 > \operatorname{Im}(z)$. Therefore the `if` statement in line 6 can only be passed finitely many times, and if $|z| \geq 1$ holds in this step, then z lies in $\mathcal{F}_{\mathbb{Z}}$. □

This algorithm will be very useful in the reduction of binary forms over $\mathbb{Z}$.

Corollary 5.6. *The group* $\mathrm{SL}_2(\mathbb{Z})$ *is generated by the matrices*

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ and } T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Proof. Let $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ be a matrix. We can use Algorithm 5.5 to determine $\gamma' \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma' \cdot \gamma \cdot (2i) \in \mathcal{F}_{\mathbb{Z}}$. The matrix γ' is then the product of matrices of the form $T^n = \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$

and S. Hence $\gamma' \in \langle S, T\rangle$. Since $2i$ lies in the interior of $\mathcal{F}_\mathbb{Z}$, the matrix $\gamma' \cdot \gamma$ is an alement of the stabilizer of $2i$, which is equal to $\{\pm I\}$. This implies that $\gamma' \cdot \gamma = \pm I_2$. Using $S^2 = -I_2$ and $\gamma = -\gamma'^{-1}$ we find $\gamma \in \langle S, T\rangle$. □

Proposition 5.7. *For all $z \in \mathcal{F}_\mathbb{Z}$, the distance $d(z, i)$ is minimal in the orbit of z.*

Proof. Let $z \in \mathcal{H}_3$ and write $z = a + bi$. Then $\cosh d(z, i) = \frac{|a|^2+b^2+1}{2b}$ [5]. If $|a + n| < |a|$, then $d(z + n, i) < d(z, i)$. as cosh is strictly increasing on $\mathbb{R}_{\geq 0}$. Secondly $d(z, i) = d(Sz, i)$ for $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ because S is an isometry of $\mathcal{H}$ which fixes i. Therefore in every step in Algorithm 5.5 the distance to i does not increase. Now if z lies in the interior $\mathcal{F}_\mathbb{Z}^\circ$, and $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, then we can use Algorithm 5.5 to find γ' such that $\gamma'\gamma z \in \mathcal{F}_\mathbb{Z}$. By the previous argument, $d(\gamma'\gamma z, i) \leq d(\gamma z, i)$, and because $\mathcal{F}_\mathbb{Z}$ is a fundamental domain we know $z = \gamma'\gamma z$.

The interior $\mathcal{F}_\mathbb{Z}^\circ$ is dense in $\mathcal{F}_\mathbb{Z}$, so if z lies in the edge $\partial\mathcal{F}_\mathbb{Z}$, there exists a sequence $\{z_n\}_{n\geq 1} \subset \mathcal{F}_\mathbb{Z}^\circ$ converging to z. For all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, we have $d(z_n, i) \leq d(\gamma z_n, i)$. By continuity of γ and the metric d, we have

$$d(z, i) = \lim_{n\to\infty} d(z_n, i) \leq \lim_{n\to\infty} d(\gamma z_n, i) = d(\gamma z, i).$$ □

So given a real square-free binary form F, Algorithm 5.5 gives us a way to determine $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $d(\gamma^{-1}z(F), i)$ is minimal. We then expect $\|F \cdot \gamma\|$ to be small, because the upper and lower bound obtained from Theorem 4.11 are minimal. We can also use the lower bound on $\|F\|$ to find $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ for which $\|F \cdot \gamma\|$ is optimal. We do this by first determining an upper bound $c > 0$ such that if $d(z(F \cdot \gamma), i) > i$, then $\|F \cdot \gamma\| > \|F\|$, where F is binary form with $z(F) \in \mathcal{F}_\mathbb{Z}$. We can then iterate over all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ with $d(z(F \cdot \gamma), i) \leq c$ and check which one has the smallest size. First however we want to know wheter there are finitly many γ with $d(z(F \cdot \gamma), i) \leq c$.

Lemma 5.8. *Let $M > 0$ and let $z \in \mathcal{F}_\mathbb{Z}$. Then there exist only finitely many $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $d(\gamma z, i) \leq M$.*

Proof. The distance $d(\gamma z, i)$ is given by $\cosh^{-1}\left(\frac{|z|^2+1}{2\,\mathrm{Im}(\gamma z)}\right)$ [5]. Suppose $d(\gamma\omega, j) \leq M$. Then, as cosh is strictly increasing and bijective on $\mathbb{R}_{\geq 0}$ to $\mathbb{R}_{\geq 1}$, we obtain a lower bound for $\mathrm{Im}(z)$. Let m be this lower bound. Write $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Then $\mathrm{Im}(z) \geq m$ is equivalent to $|c\omega + d|^2 \leq \mathrm{Im}(z)/m$. By the proof of Lemma 5.3 there are only finitely many $c, d \in R$ for which this is the case. In particular there are finitely many coprime pairs c, d for which this holds.

For each coprime pair $c, d \in \mathrm{SL}_2(R)$ we will show that there exist only finitely many $a, b \in R$ such that $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(R)$ and $d(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) z, i) \leq M$. As $c, d \in R$ are coprime, there exists at least one pair a, b such that $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(R)$. Now let $a', b' \in R$ be two different elements such that $\gamma' = \left(\begin{smallmatrix} a' & b' \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(R)$. Then we have

$$\gamma\gamma'^{-1} = \begin{pmatrix} ad - bc & a'b - ab' \\ 0 & a'd - b'c \end{pmatrix} = \begin{pmatrix} 1 & a'b - ab' \\ 0 & 1 \end{pmatrix}.$$

So, γ and γ' differ by a translation and $\gamma' z = \gamma z + n$. Only finitely many $n \in \mathbb{Z}$ have the property that $\frac{(x+n)^2+y^2+1}{2y} < \cosh(M)$, which implies that there are finitely many pairs $a, b \in R$ with $d(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) z, i) \leq M$. Combining this with the fact that the pair c, d can take on finitely many values, we find that there are only finitely many $\gamma \in \mathrm{SL}_2(R)$ such that $d(\gamma\omega, j) \leq M$. □

Proposition 5.9. *Let $F \in \mathbb{R}[X,Z]'_n$ be a square-free binary form of degree $n \geq 3$. Then there exists $\gamma_{\min} \in \mathrm{SL}_2(\mathbb{Z})$ such that $\|F \cdot \gamma_{\min}\| \leq \|F \cdot \gamma\|$ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.*

Proof. By Corollary 4.15 there exists a constant $c > 0$ such that if $d(\gamma^{-1}z(F), i) > c$, then $\|F \cdot \gamma\| > \|F\|$. By Lemma 5.8 there exist only finitely many γ such that $d(\gamma^{-1}z(F), i) \leq c$. Of these matrices, the matrix $\gamma_{\min}$ that minimizes $\|F \cdot \gamma_{\min}\|$ satisfies the statement. □

We can use the following algorithm to determine this matrix $\gamma_{\min}$:

Algorithm 5.10 Given a real square-free binary form $F \in \mathbb{R}[X,Z]'_n$ of degree $n \geq 3$ with $z(F) \in \mathcal{F}_{\mathbb{Z}}$, find a matrix $\gamma_{\min} \in \mathrm{SL}_2(\mathbb{Z})$ such that $\|F \cdot \gamma_{\min}\|$ is minimal.

Let $\gamma_{\min} = I_2$
Let $m = \|F\|$
Calculate $\varepsilon(F)$ and $\theta(F)$
Let $c = \cosh^{-1}\left(\left(\frac{m}{\varepsilon(F)\theta(F)}\right)^{1/(n-2)}\right)$
Define the list $L = [(I_2, \texttt{start})]$
for $(\gamma, \texttt{previous action}) \in L$ in ascending order of $d(\gamma z(F), j)$ **do**
    if $\|F \cdot \gamma^{-1}\| < m$ **then**
        Update $m \leftarrow \|F \cdot \gamma^{-1}\|$
        Update $\gamma_{\min} \leftarrow \gamma^{-1}$
        Let $c = \cosh^{-1}\left(\left(\frac{m}{\varepsilon(F)\theta(F)}\right)^{1/(n-2)}\right)$
        Throw out all elements γ' of L for which $d(\gamma' \cdot z(F), i) > c$
    end if
    if ‘`previous action`’ is ‘`inversion`’ or ‘`start`’ **then**
        for all $n \in \mathbb{Z} \setminus \{0\}$ such that $d(\gamma \cdot z(F) + n, i) < c$ **do**
            Let $T_n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$
            Add $(T_n \cdot \gamma, \texttt{translation})$ to L
        end for
    end if
    if ‘`previous action`’ is ‘`translation`’ or ‘`start`’ **then**
        Let $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$
        if $|S\gamma \cdot 2j| < 1$ and $|\operatorname{Re}(S\gamma \cdot 2j)| \leq \frac{1}{2}$ **then**
            Add $(S \cdot \gamma, \texttt{inversion})$ to L
        end if
    end if
end for

Proof. Let $F \in \mathbb{R}[X,Z]'_n$ be a square-free binary form of degree $n \geq 3$ with $z(F) \in \mathcal{F}_{\mathbb{Z}}$. Proposition 5.9 states that there exists a matrix $\gamma_{\min} \in \mathrm{SL}_2(\mathbb{Z})$ such that $\|F \cdot \gamma_{\min}\|$ is minimal. Let c' be the upper bound for $d(z(F \cdot \gamma), i)$ obtained from Corollary 4.15 when applied to $\|F \cdot \gamma_{\min}\|$. For any matrix γ considered in the `for` loop in this algorithm, we add all matrices γ' such that $d(\gamma' \cdot z(F), j) < c'$ and such that they are reduced to γ in one step (translation or inversion) of Algorithm 5.5 applied to the point $\gamma' \cdot 2j$. If γ is matrix such that $d(\gamma \cdot z(F), j) < c'$ then we can use Algorithm 5.5 to find γ' such that $\gamma'\gamma \cdot 2j \in \mathcal{F}_{\mathbb{Z}}$. If $\gamma'\gamma = I_2$, then we find inductively that γ

is added to the list L at some point in this algorithm. Therefore we check all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ with $d(\gamma \cdot z(F), j) < c'$ up to sign, including $\pm\gamma_{\min}^{-1}$.

The imaginary part of $S\gamma \cdot 2j$ is smaller than the imaginary part of $\gamma \cdot 2j$ if $|S\gamma \cdot 2j| < 1$. Therefore this algorithm cannot add the same matrix to L twice. Let c be the original upper bound defined in line 4. Then we never add a matrix γ such that $d(\gamma \cdot z(F), j) \geq c$ to the list L. There are only finitely many such γ, which implies that this algorithm will terminate at some point. □

In line 21 of this algorithm, we look at the points $S\gamma \cdot 2j$ instead of $S\gamma \cdot z(F)$. We do this so that we can carry out exact calculations in the implementation of this algorithm. This ensures that the algorithm cannot loop due to numerical error.

We can use the upper bound from equation 4.17 to find a matrix $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that the height $H(F \cdot \gamma)$ is minimal, with an analogous algorithm. If we replace

$$\cosh^{-1}\left(\left(\frac{m}{\varepsilon(F)\theta(F)}\right)^{1/(n-2)}\right) \tag{5.11}$$

on lines 4 and 10 with

$$\cosh^{-1}\left(\left(\frac{n \cdot m^2}{\varepsilon(F)\theta(F)}\right)^{1/(n-2)}\right), \tag{5.12}$$

and consider the height instead of the size in lines 2, 7, 8, then we will find the matrix γ such that $H(F \cdot \gamma)$ is minimal.

6 Reduction over complex discrete norm-Euclidean rings

In this section we will generalise the reduction of real binary forms over $\mathbb{Z}$, to complex binary forms over some suitable subrings of $\mathbb{C}$. Our reduction algorithm will again rely on determining a matrix $\gamma \in \mathrm{SL}_2(R)$ such that $d(z(F \cdot \gamma), j)$ is minimal, where R is a suitable subring of $\mathbb{C}$, and F is a square-free binary form. The upper and lower bounds on $\|F \cdot \gamma\|$ given by Theorem 4.11 are then also minimal. To make sure this γ exists, we constrain ourselves to discrete subrings of $\mathbb{C}$. Hence, we will first need some knowledge about discrete rings. Later in this section we will give an algorithm for determining this γ if R is a discrete *norm-Euclidean* ring. We will also define an algorithm for computing γ such that either $\|F\|$ or $H(F)$ is minimal.

6.1 Discrete subrings of $\mathbb{C}$

Let $R \subset \mathbb{C}$ be subring of $\mathbb{C}$. We call R *discrete* if it is discrete as a subset of $\mathbb{C}$ using the usual topology. We will give a complete characterisation of all complex discrete subrings in Proposition 6.8. Leading up to this we will first formulate some lemmas and a definition.

Lemma 6.1. *Let $R \subset \mathbb{C}$ be a subring. Then R is discrete if and only if $|r| \geq 1$ holds for all $r \in R \setminus \{0\}$. Furthermore, if R is discrete, then R is closed as a subset of $\mathbb{C}$.*

Proof. Suppose there exists $r \in R \setminus \{0\}$ such that $|r| < 1$. Then $\{r^n\}_{n \geq 1}$ is a sequence converging to 0, and 0 is a limit point of R, so R is not discrete.

Now suppose $|r| \geq 1$ does hold for all $r \in R \setminus \{0\}$. Then for any two points $x, y \in R$ that are not equal we have $|x - y| \geq 1$, so R is discrete. This also gives us that R is closed, since any converging sequence is eventually constant, which implies that R is closed under taking limits. □

Corollary 6.2. *Let $R \subset \mathbb{C}$ be a discrete ring. Then an element $r \in R$ is a unit if and only if $|r| = 1$.*

Proof. Let $r \in R$ and suppose r is a unit. Then there exists $s \in R$ such that $rs = 1$. By the previous lemma we find $|r|, |s| \geq 1$, as neither can be equal to zero. By the multiplicativity of the norm we find $|r| \cdot |s| = 1$, and hence $|r| = |s| = 1$.

Conversely, suppose $|r| = 1$. Then the set $\{r^n : n \in \mathbb{Z}\}$ is a closed and discrete subset of the unit circle $\{z \in \mathbb{C} : |z| = 1\}$, which is compact. Therefore, $\{r^n : n \in \mathbb{Z}\}$ is a finite set, and there exist $m, n \in \mathbb{Z}$ with $m > n$ such that $r^m = r^n$. This implies $r^{m-n} = 1$, so r is a unit. □

Suppose $R \subset \mathbb{C}$ is a discrete subring of $\mathbb{C}$. If we forget the multiplication of R, then we obtain an discrete abelian subgroup of $\mathbb{C}$. We can use the following lemma from Algebra 1 by Peter Stevenhagen [9].

Lemma 6.3. *Let $n \geq 1$ and let $A \subset \mathbb{R}^n$ be a discrete supgroup. Then A is free of rank $k \leq n$.*

The terms *free* and *rank* are defined as follows:

Definition 6.4. An abelian group A is called *free* if A has a generating set S such that every element $a \in A$ can be written uniquely as a $\mathbb{Z}$-linear combination of elements of S. In that case S is called a *basis* for A and we call the cardinality of S the *rank* of A. [9]

If a free group A has a finite basis $S = \{s_1, \ldots, s_n\}$, then there exists an isomorphism $\mathbb{Z}^n \cong A$ given by $(n_i)_{i=1}^n \mapsto \sum_{i=1}^n n_i s_i$. Using Lemma 6.3 we obtain the following result:

Corollary 6.5. *Let $R \subset \mathbb{C}$ be a discrete ring. Then $R = \mathbb{Z}$ or $R = \mathbb{Z} + z\mathbb{Z}$ for some $z \in \mathbb{C}$.*

Proof. As an abelian group $\mathbb{C}$ is isomorphic to $\mathbb{R}^2$. If we forget the multiplication on R, then it is a discrete subgroup of $\mathbb{C}$. Therefore R is free of rank either 1 or 2 as an abelian group.

Suppose it has rank 1. Then $R = a\mathbb{Z}$ for some $a \in \mathbb{C}$ with $|a| \geq 1$. Since $1 \in R$, there exists $n \in \mathbb{Z}$ such that $na = 1$. The inequality $|a| \geq 1$ then gives $n = \pm 1$ and therefore $a = \pm 1$, so $R = \mathbb{Z}$.

Suppose R has rank 2. Then $R = a\mathbb{Z} + b\mathbb{Z}$ for some $a, b \in \mathbb{C}$. Since $1 \in R$, there exist $m, n \in \mathbb{Z}$ such that $ma + nb = 1$. Suppose m, n are not coprime in $\mathbb{Z}$. Then define $m' = m/\gcd(m, n)$ and $n' = n/\gcd(m, n)$. We find that $m'a + n'b = 1/\gcd(m, n) \in R$. However R contains no non-zero elements of norm smaller than 1. Therefore m, n are coprime in $\mathbb{Z}$ and there exist $x, y \in \mathbb{Z}$ such that $my - nx = 1$. Define $z \in \mathbb{C}$ such that the following equality holds:

$$\begin{pmatrix} m & n \\ x & y \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 1 \\ z \end{pmatrix}. \tag{6.6}$$

Because $my - nx = 1$ holds, we find

$$\begin{pmatrix} m & n \\ x & y \end{pmatrix}^{-1} \begin{pmatrix} 1 \\ z \end{pmatrix} = \begin{pmatrix} y & -n \\ -x & m \end{pmatrix} \begin{pmatrix} 1 \\ z \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}. \tag{6.7}$$

Equations (6.6) and (6.7) together imply $R = a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z} + z\mathbb{Z}$. □

We can now give a complete characterisation of the discrete subrings of $\mathbb{C}$. Let $D < 0$ be a negative integer with $D \equiv 0$ or $D \equiv 1 \mod 4$. If $D \equiv 0 \mod 4$, define $\alpha_D = \frac{\sqrt{D}}{2}$, and if $D \equiv 1 \mod 4$, define $\alpha_D = \frac{1+\sqrt{D}}{2}$. In both cases let $R_D = \mathbb{Z}[\alpha_D]$. For example α_{-3} is equal to the sixth root of unity ζ_6, and $\alpha_{-4} = i$.

Proposition 6.8. *All discrete subrings R of $\mathbb{C}$ are equal to $\mathbb{Z}$ or R_D for some negative integer D with $D \equiv 0, 1 \mod 4$.*

Proof. Let $R \neq \mathbb{Z}$ be a discrete subring of $\mathbb{C}$. By Corollary 6.5 we find that $R = \mathbb{Z} + z\mathbb{Z}$ holds for some $z \in \mathbb{C}$. Without loss of generality we may assume that $\mathrm{Re}(z) \in [0, 1)$, since we can translate z with elements of $\mathbb{Z}$. As R is closed under multiplication we find that z^2 is an element of $R = \mathbb{Z} + z\mathbb{Z}$, and thus that there exist integers $b, c \in \mathbb{Z}$ such that $z^2 + bz + c = 0$. Using the quadratic formula we find $z = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$. Define $D = b^2 - 4c$. The point z cannot be real, as then R would be equal to $\mathbb{Z}$. Thus z has non-zero imaginary part, and we have $b^2 - 4c < 0$ and $\mathrm{Re}(z) = -b/2$. Since $\mathrm{Re}(z) \in [0, 1)$, the only possible values of b are $b = 0$ and $b = -1$. If $b = 0$ then $z = \pm\sqrt{D}/2$ and $R = \mathbb{Z}[\frac{\sqrt{D}}{2}]$ with $D = -4c \equiv 0 \mod 4$, and if $b = -1$, then $z = \frac{1}{2} \pm \frac{1}{2}\sqrt{D}$, which implies $R = \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$ and $D = 1 - 4c \equiv 1 \mod 4$.

Conversely suppose D is a negative integer congruent to 0 or 1 mod 4. If $D \equiv 0 \mod 4$ then $\alpha_D^2 = -D/4$, where $\alpha_D \in R$ is defined as above. If $D \equiv 1 \mod 4$ then $\alpha_D^2 = \alpha_D + (D-1)/4 \in R$. In both cases we have $R_D = \mathbb{Z}[\alpha_D] = \mathbb{Z} + \alpha_D\mathbb{Z}$. This is discrete in $\mathbb{C}$ because α_D has non-zero imaginary part. □

We continue with a lemma about the action of discrete rings on the upper half-space.

Lemma 6.9. *Let $R \subset \mathbb{C}$ be a discrete ring and let $\omega \in \mathcal{H}_3$. Then the set*

$$\{\pi_j(\gamma\omega) : \pi_j(\gamma\omega) \geq \pi_j(\omega), \gamma \in \mathrm{SL}_2(R)\}$$

is finite.

Proof. Let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(R)$. Then we have $\pi_j(\gamma\omega) = \pi_j(\omega)/|c\omega + d|^2$. Thus an element of this set corresponds to a pair of coprime elements $c, d \in R$ with $|c\omega + d|^2 \leq 1$. If we write $\omega = \tau + uj$ for $\tau \in \mathbb{C}$ and $u > 0$, then we have the equality

$$|c\omega + d|^2 = |c\tau + d|^2 + u^2|c|^2. \tag{6.10}$$

Since R is closed and discrete, there are at most finitely many $c \in R$ such that $|c| \leq u^{-1}$. And for each c, there are only finitely many $d \in R$ such that $|c\tau + d| \leq 1$. Therefore, there are only finitely many pairs $c, d \in R$ such that $|c\omega + d|^2 \leq 1$. □

6.2 Norm-Euclidean rings

For reduction over discrete subrings of $\mathbb{C}$, the simplest case will be when R is *norm-Euclidean*.

Definition 6.11. We call a discrete ring $R \subset \mathbb{C}$ *norm-Euclidean* if it is Euclidean with respect to the norm map on $\mathbb{C}$. That is, for all $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ with $|r| < |b|$ such that $a = qb + r$.

With Proposition 6.8 we can determine exactly which discrete subrings are norm-Euclidean.

Proposition 6.12. *The discrete subrings $R \subset \mathbb{C}$ that are norm-Euclidean are precisely the rings R_D for $D = -3, -4, -7, -8, -11$.*

Proof. This proof is largely taken from Algebra II by Peter Stevenhagen [8, Stelling 12.19], where he shows where he shows that $\mathbb{Z}[i] = R_{-4}$ is a principal ideal domain by showing it is norm-Euclidean. We extend this proof to the rings R_D for $D = -3, -7, -8, -11$.

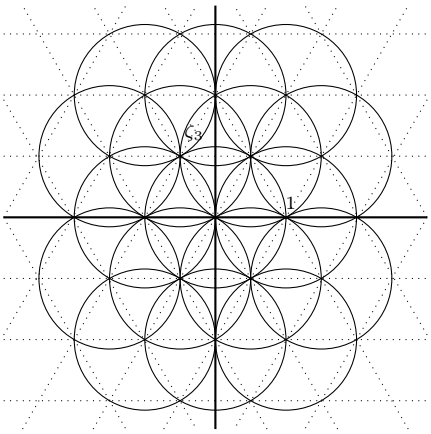
Suppose $R = R_D$ for $D = -3, -4, -7, -8, -11$. Then in Figure 3 it can be seen that the open unit discs centered around elements of R_D cover the entire complex plane. So for all $\tau \in \mathbb{C}$ there exists $r \in R_D$ such that $|\tau + r| < 1$. Now let $a, b \in R$ with $b \neq 0$. There exists $q \in R$ such that $|a/b - q| < 1$. Define $r = a - qb \in R$. We then find $a = qb + r \in R$ and $|r| = |b| \cdot |a/b - q| < |b|$.

For $D = -12$ the element $\frac{1+\sqrt{-3}}{2} \in Q(R_{-12}) = \mathbb{Q}[\sqrt{-3}]$ does not lie in any of the open unit discs, only in the boundary. Therefore there do not exist $q, r \in R$ with $|r| < 2$ such that $1 + \sqrt{-3} = 2q + r$ holds, and thus R_{-12} is not norm-Euclidean.

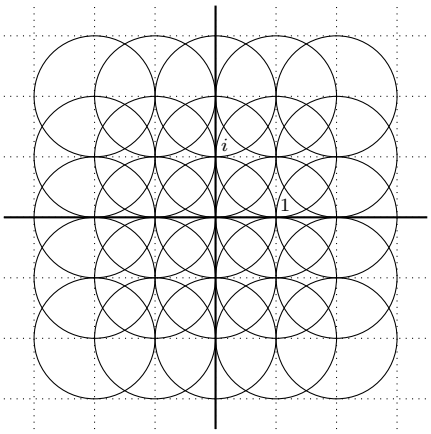
For all $D < -12$, the unit discs will be spaced farther apart and they will leave gaps in the complex plane with non-empty interior. As $Q(R_D) = \mathbb{Q}[\sqrt{-D}]$ is dense in $\mathbb{C}$, there exist $a, b \in R$ with $b \neq 0$ and where a/b does not lie in any of the open unit discs. By the same argument as for $D = -12$, we find that R_D is not norm-Euclidean if $D < -12$. □

In this proof we see that for all discrete norm-Euclidean rings $R \subset \mathbb{C}$, and for all $\tau \in \mathbb{C}$, there exists $r \in R$ such that $|\tau - r| < 1$. This property will make it so that we can fairly directly generalise the reduction of real binary over $\mathrm{SL}_2(\mathbb{Z})$, to the reduction of complex binary forms over $\mathrm{SL}_2(R)$. In order to generalise the fundamental domain $\mathcal{F}_\mathbb{Z}$ for the action of $\mathrm{SL}_2(\mathbb{Z})$, consider the following region in the upper half-space:

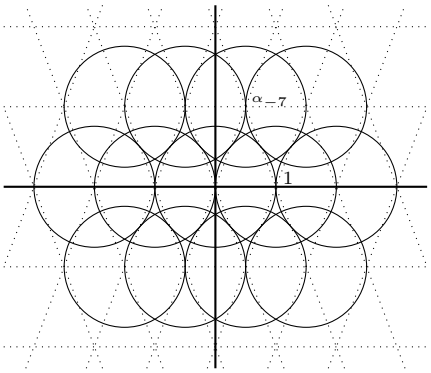
$$\mathcal{G}_R = \{\omega \in \mathcal{H}_3 : |\omega| \geq 1, |\omega| \leq |\omega + r| \text{ for all } r \in R\}. \tag{6.13}$$



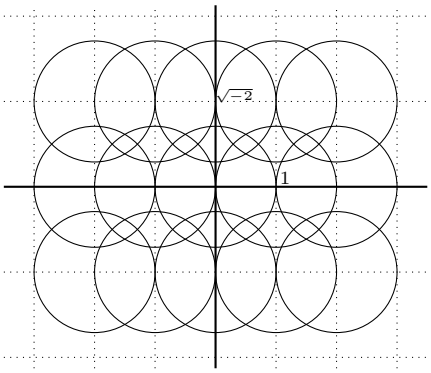
(a) Unit circles centered around elements of $\mathbb{Z}[\zeta_3] = R_{-3}$



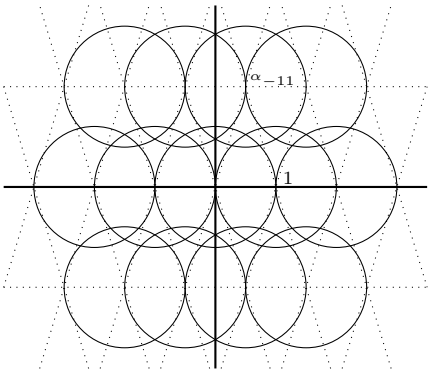
(b) Unit circles centered around elements of $\mathbb{Z}[i] = R_{-4}$



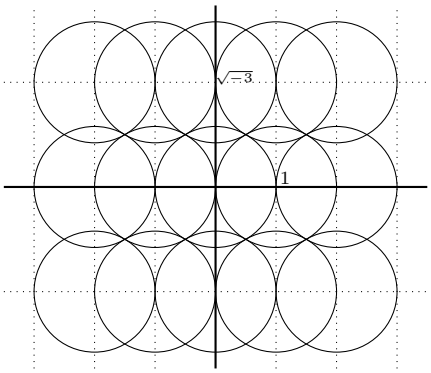
(c) Unit circles centered around elements of R_{-7}



(d) Unit circles centered around elements of R_{-8}

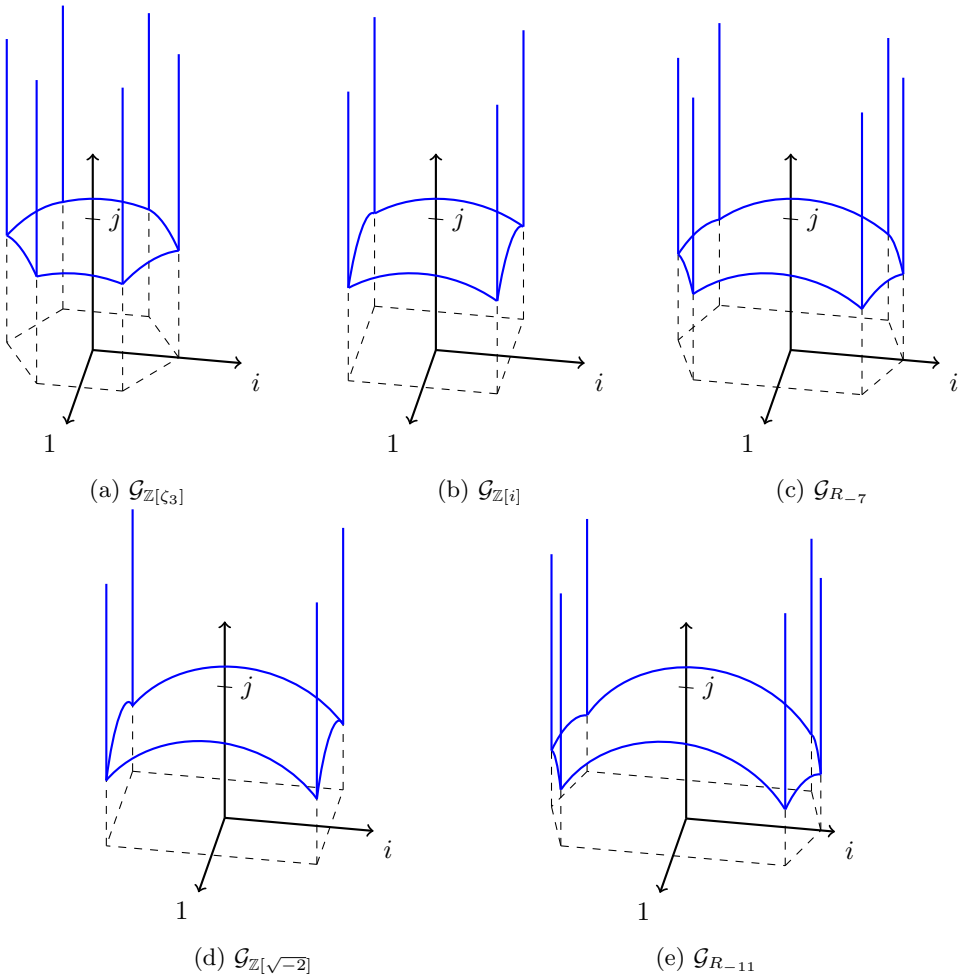


(e) Unit circles centered around elements of R_{-11}



(f) Unit circles centered around elements of R_{-8}

Figure 3: Unit circles centered around elements of R_D for $D = -3, -4, -7, -8, -11, -12$. Intersections of the dotted lines denote these elements.



(a) $\mathcal{G}_{\mathbb{Z}[\zeta_3]}$ (b) $\mathcal{G}_{\mathbb{Z}[i]}$ (c) $\mathcal{G}_{R_{-7}}$

(d) $\mathcal{G}_{\mathbb{Z}[\sqrt{-2}]}$ (e) $\mathcal{G}_{R_{-11}}$

Figure 4: The regions $\mathcal{G}_{R_D}$ for $D = -3, -4, -7, -8, -11$

The regions $\mathcal{G}_R$ for $R = R_D$ with $D = -3, -4, -7, -8, -11$ are portrayed in Figure 4. These regions will not all be fundamental domains for the action of $\mathrm{SL}_2(R)$, so we will denote them with $\mathcal{G}_R$ instead of $\mathcal{F}_R$ to avoid confusion. If we write $\omega = \tau + uj$, then the condition $|\omega| \leq |\omega + r|$ for all $r \in R$ is equivalent to $|\tau| \leq |\tau + r|$ for all $r \in R$. As the ring R contains $-1, 1$, this condition implies $|\operatorname{Re}(\tau)| \leq \frac{1}{2}$. If $R = R_D$ for $D < 0$ with $D \equiv 1 \mod 4$, then the region in the complex plane for which $|\tau| \leq |\tau + r|$ holds for all $r \in R$ is a hexagon. The sides of this hexagon are perpendicular bisectors between 0 and the points $-1, 1, \alpha_D, \overline{\alpha}_D, -\overline{\alpha}_D, -\alpha_D$. The corners of this hexagon are points which have equal distance to 0 and two of these elements. A small exercise in geometry shows that the distance from the origin to one of the corners is equal to $(-D+1)\sqrt{-D}/(-4D)$. Therefore $|\tau| \leq (-D+1)\sqrt{-D}/(-4D)$ for all $\tau + uj \in \mathcal{G}_{R_D}$ with $D \equiv 1 \mod 4$.

If on the other hand $D \equiv 0 \mod 4$, then the region in $\mathbb{C}$ for which $|\tau| \leq |\tau + r|$ holds for all $r \in R$ is a rectangle. The edges are perpendicular bisectors between 0 and the points $1, -1, \alpha_D, -\alpha_D$

So two sides have length 1, and the other two have length $|\alpha_D| = \frac{1}{2}\sqrt{-D}$. The distance from the origin to one of the corners is equal to $\frac{1}{2}\sqrt{1+D}$. This is also the maximal value for $|\tau|$ in this region.

Proposition 6.14. *Let R be a discrete norm-Euclidean subring of $\mathbb{C}$. Then we can rewrite $\mathcal{G}_R$ as follows:*

$$\mathcal{G}_R = \{\omega \in \mathcal{H}_3 : \pi_j(\omega) \geq \pi_j(\gamma\omega), |\omega| \leq |\omega + r| \text{ for all } \gamma \in \mathrm{SL}_2(R), r \in R\}. \tag{6.15}$$

Furthermore, for all $\omega \in \mathcal{H}_3$, there exists $\gamma \in \mathrm{SL}_2(R)$ such that $\gamma\omega \in \mathcal{G}_R$.

Proof. For the first statement, let $\omega \in \mathcal{G}_R$ and $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(R)$. Then by equation (3.20) we have $\pi_j(\gamma\omega) = \pi_j(\omega)/|c\omega + d|^2$. Now $\pi_j(\gamma\omega) > \pi_j(\omega)$ is equivalent to $|c\omega + d|^2 < 1$ with $c, d \in R$ coprime. We will show that no coprime c, d with this property exist. For each norm-Euclidean ring R we will reduce the possibilities to finitely many cases, and then check each case. First, by definition of $\mathcal{G}_R$, we have $|\omega + r| \geq |\omega| \geq 1$ which covers the case of $|c| = 1$. For other cases, we can rewrite $|c\omega + d|^2$ as follows. Let $\tau \in \mathbb{C}$ and $u > 0$ be such that $\omega = \tau + uj$. We than have

$$|c\omega + d|^2 = |c\tau + d|^2 + |c|^2u^2 = |c|^2|\omega|^2 + c\tau\overline{d} + \overline{c\tau}d + |d|^2. \tag{6.16}$$

Secondly, for all $r \in R$ we have

$$|\tau + r|^2 \geq |\tau|^2 \implies \tau\overline{r} + \overline{\tau}r \geq -|r|^2. \tag{6.17}$$

The main idea to show that $|c\omega + d| \geq 1$ holds for all coprime pairs $c, d \in R$, is to first find some bounds on $|c|$ and $|d|$. Afterwards we will only have finitely many cases left. For these cases we will apply $|\omega| \geq 1$ to equation (6.16), and then use equation (6.17) for suitable values of r. Due to the amount of cases needed to be checked, this part of the proof is moved to Appendix A.

For the second statement, let $\omega \in \mathcal{H}_3$. Then by Lemma 6.9 there exist only finitely many possible values of $\pi_j(\gamma\omega)$ such that $\pi_j(\gamma\omega) \geq \pi_j(\omega)$. Therefore there exists $\gamma \in \mathrm{SL}_2(R)$ such that $\pi_j(\gamma\omega)$ is maximal in its orbit. Because R is discrete in $\mathbb{C}$, the set $\{\gamma\omega + r : r \in R\}$ is discrete in $\mathcal{H}_3$ using the subspace topology obtained from the embedding $\mathcal{H}_3 \hookrightarrow \mathbb{R}^3$. Therefore there exists $r \in R$ such that $|\gamma\omega + r|$ is minimal. Now define $\gamma' = T_r\gamma$, where $T_r = \left(\begin{smallmatrix} 1 & r \\ 0 & 1 \end{smallmatrix}\right)$. Then we have $\gamma'\omega \in \mathcal{G}_R$. □

This proposition tells us that for all $\omega \in \mathcal{H}_3$ there exists $\gamma \in \mathrm{SL}_2(R)$ such that $\gamma\omega \in \mathcal{G}_R$. However, it does not give us a way to compute γ. The following algorithm can be used to do this:

Algorithm 6.18 Given $\omega \in \mathcal{H}_3$ and a discrete complex norm-Euclidean ring R not equal to $\mathbb{Z}$, find $\gamma \in \mathrm{SL}_2(R)$ such that $\gamma\omega \in \mathcal{G}_R$.

Let $\gamma = I_2$
while $\omega \notin \mathcal{G}_R$ **do**
    Determine $r \in R$ such that $|\omega + r| \leq |\omega + r'|$ for all $r' \in R$
    Update $\gamma \leftarrow \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} \cdot \gamma$
    Update $\omega \leftarrow \omega + r$
    if $|\omega| < 1$ **then**
        Update $\gamma \leftarrow \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \gamma$
        Update $\omega \leftarrow -\omega^{-1}$
    end if
end while

Proof. Let $\omega \in \mathcal{H}_3$. By Lemma 6.9 there exist only finitely many possible values of $\pi_j(\gamma\omega)$ for which $\pi_j(\gamma\omega) \geq \pi_j(\omega)$ holds, with $\gamma \in \mathrm{SL}_2(R)$. In line 8 of the algorithm, the value of $\pi_j(\omega)$ increases to $\pi_j(\omega)/|\omega|^2 > \pi_j(\omega)$. This can only be done finitely many times, so at some point $|\omega| \geq 1$ holds at line 6 of the algorithm. In that case ω lies in $\mathcal{G}_R$. Note that this ω is equal to γ multiplied by the original value of ω. □

It is not immediately clear how to find $r \in R$ such that $|\omega + r| \leq |\omega + r'|$ for all $r' \in R$ in line 3 of this algorithm. If $R = R_D$ with $D < 0$ and $D \equiv 0 \mod 4$, this can be done as follows. First write $\omega = \tau + uj$. Then $|\omega + r| \leq |\omega + r'|$ holds if and only if $|\tau + r| \leq |\tau + r'|$ holds for $r, r' \in R$. Let $r = a + b\alpha_D$ with a and b be equal to $-\operatorname{Re}(\tau)$ and $-2\operatorname{Im}(\tau)/\sqrt{-D}$ both rounded to the nearest integer. Now for all $r' = c + d\alpha_D$ we find by definition of a, b:

$$|\tau + r'|^2 = (\operatorname{Re}\tau + c)^2 + (\operatorname{Im}(\tau) + d \cdot \sqrt{-D}/2)^2 \geq (\operatorname{Re}\tau + a)^2 + (\operatorname{Im}(\tau) + b \cdot \sqrt{-D}/2)^2 = |\tau + r|^2.$$

Otherwise if $R = R_D$ with $D < 0$ and $D \equiv 1 \mod 4$ this process is slightly more involved. Again using rounding we can find $r \in R$ such that $|\operatorname{Re}(\tau + r)| \leq \frac{1}{2}$ and $|\operatorname{Im}(\tau + r)| \leq \frac{1}{4}\sqrt{-D}$. This holds for $r = a + b\alpha_D$ with b being the nearest integer to $-\operatorname{Im}(\tau)/\frac{1}{2}\sqrt{-D}$ and a being the nearest integer to $-\operatorname{Re}(\tau + b\alpha_D)$. For this value of r we know that $|\tau + r| \leq \sqrt{(1-D)}/2$. Now for all $r' \in R$ with $|r'| \geq \sqrt{1-D}$ we have $|\tau + r + r'| \geq |r'| - |\tau + r| \geq \sqrt{(1-D)}/2 \geq |\tau + r|$. Therefore we only need to check finitely many values of r' to find an element that minimizes the value of $|\tau + r + r'|$.

Algorithm 6.18 will be very useful in the reduction of binary forms over $\mathrm{SL}_2(R)$, with R a discrete complex norm-Euclidean domain. We will use this algorithm to find that $\mathcal{G}_R$ consists of points with minimal distance to j in their $\mathrm{SL}_2(R)$ orbit, and to find generators of $\mathrm{SL}_2(R)$. First we will need the following proposition.

Proposition 6.19. *Let R be a discrete norm-Euclidean ring and let ω be an element of the interior $\mathcal{G}_R^\circ$ of $\mathcal{G}_R$. Suppose $\gamma\omega \in \mathcal{G}_R$ for some $\gamma \in \mathrm{SL}_2(R)$. Then we have*

$$\gamma \in \left\{ \begin{pmatrix} r & 0 \\ 0 & r^{-1} \end{pmatrix} : r \in R^* \right\}. \tag{6.20}$$

Proof. Let $\omega \in \mathcal{G}_R^\circ$ and let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ be such that $\gamma\omega \in \mathcal{G}_R$. In the proof of Proposition 6.14 we have seen that $|c\omega + d|^2 \geq 1$. Using the strict inequality $|\omega|^2 > 1$, we can use the same method as in the proof of this proposition to find that the inequality $|c\omega + d| > 1$ is strict if $c \neq 0$. As both ω and $\gamma\omega$ are elements of $\mathcal{G}_R$, they have maximal j-part. Thus $\pi_j(\omega) = \pi_j(\gamma\omega)$. This gives $|c\omega + d|^2 = 1$. Therefore $c = 0$ and $|d| = 1$ holds. Because $\det\gamma = 1$, we find $a = d^{-1}$. Then For γ we have

$$\gamma = \begin{pmatrix} d^{-1} & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} 1 & d^{-1}b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} d^{-1} & 0 \\ 0 & d \end{pmatrix}.$$

If we write $\omega = \tau + uj$, then $\left(\begin{smallmatrix} d^{-1} & 0 \\ 0 & d \end{smallmatrix}\right)\omega = d^{-2}\tau + uj$. This is also an element of $\mathcal{G}_R^\circ$, so if $b \neq 0$ we have

$$\left| \begin{pmatrix} d^{-1} & 0 \\ 0 & d \end{pmatrix} \omega + d^{-1}b \right| > \left| \begin{pmatrix} d^{-1} & 0 \\ 0 & d \end{pmatrix} \omega \right|,$$

which leads to a contradiction as $\gamma\omega \in \mathcal{G}_R$. Therefore $\gamma \in \{\left(\begin{smallmatrix} r & 0 \\ 0 & r^{-1} \end{smallmatrix}\right) : r \in R^*\}$. □

The only discrete rings with $R^* \neq \{\pm I_2\}$ are equal to $\mathbb{Z}[\zeta_3] = R_{-3}$ and $\mathbb{Z}[i] = R_{-4}$. For all other discrete rings, their generator α_D has norm strictly higher than one. Because the matrices $\pm I_2$ act trivially on $\mathcal{H}_3$ we get the following corollary.

Corollary 6.21. *The region $\mathcal{G}_R$ is a fundamental domain for the action of $\mathrm{SL}_2(R)$ on $\mathcal{H}_3$, with $R = R_D$ for $D = -7, -8, -11$.*

Proof. We have already seen that there exists $\gamma \in \mathrm{SL}_2(R)$ such that $\gamma\omega \in \mathcal{G}_R$ for all $\omega \in \mathcal{H}_3$. Secondly, for these rings we have $R^* = \{\pm 1\}$, and the matrices $I_2, -I_2$ both act trivially on $\mathcal{H}_3$, which implies using Proposition 6.19 that if ω is an element of the interior $\mathcal{G}_R^\circ$, then ω is the unique point in its orbit that lies in $\mathcal{G}_R$. So, the region $\mathcal{G}_R$ is a fundamental domain. □

To obtain a fundamental domain for $R = \mathbb{Z}[i], \mathbb{Z}[\zeta_3]$, we can do the following. If $r \in R$ is a unit, then the matrix $\left(\begin{smallmatrix} r & 0 \\ 0 & r^{-1} \end{smallmatrix}\right)$ rotates the upper half-space by an angle of $2\arg(r)$ around the j-axis. More precisely, if $\omega = \tau + u_j$, then $\left(\begin{smallmatrix} r & 0 \\ 0 & r^{-1} \end{smallmatrix}\right)\omega = r^2\tau + uj$. Thus for $R = \mathbb{Z}[i]$ we need to leave out half of $\mathcal{G}_R$. For example the region $\{\omega \in \mathcal{H}_3 : \mathrm{Re}(\omega) \geq 0\} \cap \mathcal{G}_{\mathbb{Z}[i]}$ is a fundamental domain. For $R = \mathbb{Z}[\zeta_3]$, we need to leave one third of $\mathcal{G}_{\mathbb{Z}[\zeta_3]}$ to get a fundamental domain, for example $\{\omega = \tau + uj \in \mathcal{H}_3 : -\frac{1}{6}\pi \leq \arg(\tau) \leq \frac{1}{2}\pi\} \cap \mathcal{G}_{\mathbb{Z}[\zeta_3]}$.

We can use Algorithm 6.18 together with Proposition 6.19 to find generators for $\mathrm{SL}_2(R)$.

Corollary 6.22. *The groups $\mathrm{SL}_2(R_D)$ for $D = -7, -8, -11$ have the following set of generators:*

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad T_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } T_{\alpha_D} = \begin{pmatrix} 1 & \alpha_D \\ 0 & 1 \end{pmatrix}. \tag{6.23}$$

Secondly, the group $\mathrm{SL}_2(\mathbb{Z}[\zeta_3]) = \mathrm{SL}_2(R_{-3})$ is generated by

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad U_{\zeta_6} = \begin{pmatrix} \zeta_6 & 0 \\ 0 & \zeta_6^{-1} \end{pmatrix}, \quad T_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } T_{\zeta_3} = \begin{pmatrix} 1 & \zeta_3 \\ 0 & 1 \end{pmatrix}. \tag{6.24}$$

Lastly, the group $\mathrm{SL}_2(\mathbb{Z}[i]) = \mathrm{SL}_2(R_{-4})$ is generated by

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad U_{\zeta_3} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad T_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } T_i = \begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix}. \tag{6.25}$$

Proof. Let $\gamma \in \mathrm{SL}_2(R)$. Then use Algorithm 6.18 to find $\gamma' \in \mathrm{SL}_2(R)$ such that $\gamma'\gamma \cdot 2j \in \mathcal{G}_R$. Then γ' is an element of $\langle S, T_r : r \in R\rangle$. Using the relation $T_rT_s = T_{r+s}$ we can also write this set as $\langle S, T_1, T_{\alpha_D}\rangle$, because $1, \alpha_D$ generate R as an abelian group. We find $\gamma'\gamma \in \{\left(\begin{smallmatrix} r & 0 \\ 0 & r^{-1} \end{smallmatrix}\right) : r \in R^*\}$, since $2j$ is an element of the interior $\mathcal{G}_R^\circ$. For $R = R_{-7}, R_{-8}, R_{-11}$, the goup R^* is generated by -1, so $\{\left(\begin{smallmatrix} r & 0 \\ 0 & r^{-1} \end{smallmatrix}\right) : r \in R^*\}$ is generated by $-I_2 = S^2$. Therefore $\gamma \in \langle S, T_1, T_{\alpha_D}\rangle$. If $R = R_{-3} = \mathbb{Z}[\zeta_3]$, then ζ_6 generates R^*, and $U_{\zeta_6} = -U_{\zeta_3}^2$ generates $\{\left(\begin{smallmatrix} r & 0 \\ 0 & r^{-1} \end{smallmatrix}\right) : r \in \mathbb{Z}[\zeta_3]^*\}$. Therefore $\gamma \in \langle S, T_1, T_{\zeta_3}, U_{\zeta_3}\rangle$. For $R = R_{-4} = \mathbb{Z}[i]$, the group R^* is generated by i. Thus the matrix U_i generates $\{\left(\begin{smallmatrix} r & 0 \\ 0 & r^{-1} \end{smallmatrix}\right) : r \in \mathbb{Z}[i]^*\}$ and we have $\gamma \in \langle S, T_1, T_i, U_i\rangle$. □

We can also use Proposition 6.19 to prove the following result:

Theorem 6.26. *Let R be a discrete norm-Euclidean domain. Then $\mathcal{G}_R$ consists of points which have minimal distance to j with respect to their $\mathrm{SL}_2(R)$ orbits.*

Proof. This is a generalisation of Proposition 5.8, and the proof will be analogous. Let $\omega \in \mathcal{H}_3$. Then the distance $d(\omega, j)$ is given by $\cosh^{-1}\left(\frac{|\omega|^2+1}{2\pi_j(\omega)}\right)$ [5]. If $|\omega + r| \geq |\omega|$ for $r \in R$, then we also have $d(\omega + r, j) \geq d(\omega, j)$. Let $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. Then $d(S\omega, j) = d(\omega, j)$ because S is an isometry that fixes j. Therefore in every step Algorithm 6.18 the distance does not increase.

If ω is an element of the interior $\mathcal{G}_R^\circ$, and $\gamma \in \mathrm{SL}_2(R)$ is a matrix, then we can use Algorithm 6.18 to find $\gamma' \in \mathrm{SL}_2(R)$ such that $\gamma'\gamma\omega \in \mathcal{G}_R$. By the previous argument we find $d(\gamma'\gamma\omega, j) \leq d(\gamma\omega, j)$. By Proposition 6.19 we find $\gamma'\gamma\omega \in \{\left(\begin{smallmatrix} r & 0 \\ 0 & r^{-1} \end{smallmatrix}\right) : r \in R^*\}$. All of these matrices are isometries that fix j. Hence $d(\omega, j) = d(\gamma'\gamma\omega, j) \leq d(\gamma\omega, j)$.

Now let $\omega \in \mathcal{G}_R \setminus \mathcal{G}_R^\circ$. The interior $\mathcal{G}_R^\circ$ is dense in $\mathcal{G}_R$, so there exists a sequence $\{\omega_n\}_{n\geq 1} \subset \mathcal{G}_R^\circ$ converging to ω. For all $\gamma \in \mathrm{SL}_2(R)$ we find

$$d(\omega, j) = \lim_{n\to\infty} d(\omega_n, j) \leq \lim_{n\to\infty} d(\gamma\omega_n, j) = d(\gamma\omega, j). \qquad \square$$

This theorem gives the motivation for the following reduction algorithm. Let $F \in \mathbb{C}[X, Z]'_n$ be a square-free binary form of degree $n \geq 3$. To find a representative in the $\mathrm{SL}_2(R)$ orbit of F with a small size, we use Algorithm 6.18 to find $\gamma \in \mathrm{SL}_2(R)$ such that $\gamma^{-1}z(F) \in \mathcal{G}_R$. Then by Theorem 6.26 the distance $d(z(F \cdot \gamma), j)$ is minimal in its orbit. Hence, both the lower and upper bound on $\|F \cdot \gamma\|$ obtained from Theorem 4.11 are as small as possible.

For this thesis I have implemented this reduction algorithm into SageMath for all discrete norm-Euclidean subrings of $\mathbb{C}$ not equal to $\mathbb{Z}$. See Appendix B.

6.3 Optimal reduction

For optimal reduction we will again use the lower bound $\|F\|$ to calculate an upper bound $c > 0$ on the distance $d(z(F \cdot \gamma), j)$ such that $d(z(F \cdot \gamma), j) > c$ implies $\|F \cdot \gamma\| > \|F\|$. We can then iterate over all matrices γ for which this the case.

Lemma 6.27. *Let R be a discrete ring and let $M > 0$ and $\omega \in \mathcal{H}_3$. Then there exist only finitely many $\gamma \in \mathrm{SL}_2(R)$ such that $d(\gamma\omega, j) \leq M$.*

Proof. The distance $d(\gamma\omega, j)$ is given by $\cosh^{-1}\left(\frac{|\omega|^2+1}{2\pi_j(\gamma\omega)}\right)$ [5]. Suppose $d(\gamma\omega, j) \leq M$. Then, as cosh is strictly increasing and bijective on $\mathbb{R}_{\geq 0}$ to $\mathbb{R}_{\geq 1}$, we obtain a lower bound for $\pi_j(\gamma\omega)$. Let k be this lower bound. Write $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Then $\pi_j(\gamma\omega) \geq k$ is equivalent to $|c\omega + d|^2 \leq \pi_j(\omega)/k$. By the proof of Lemma 6.9 we find that there are only finitely many $c, d \in R$ for which this is the case. In particular there are finitely many coprime pairs c, d for which this holds.

For each coprime pair $c, d \in \mathrm{SL}_2(R)$ we will show that there exist only finitely many $a, b \in R$ such that $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(R)$ and $d(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\omega, j) \leq M$. As $c, d \in R$ are coprime, there exists at least one pair a, b such that $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(R)$. Now let $a', b' \in R$ be two different elements such that $\gamma' = \left(\begin{smallmatrix} a' & b' \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(R)$. Then we have

$$\gamma\gamma'^{-1} = \begin{pmatrix} ad - bc & a'b - ab' \\ 0 & a'd - b'c \end{pmatrix} = \begin{pmatrix} 1 & a'b - ab' \\ 0 & 1 \end{pmatrix}.$$

It follows that γ and γ' differ by a translation, and $\gamma'\omega = \gamma\omega + r$ for some $r \in R$. The distance $d(\gamma\omega + r, j)$ for $r \in R$ is given by $\cosh^{-1}\frac{|\tau+r|^2+u^2+1}{2u}$. This distance being smaller than M gives an upper bound N on $|\tau + r|^2$. Because R is discrete and closed in $\mathbb{C}$, There exist only finitely many $r \in R$ such that $|\tau + r|^2 \leq N$. This implies that there are finitely many pairs $a, b \in R$ such that $d(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\omega, j) \leq M$. Combining this with the fact that the pair c, d can take on finitely many values, we find that there are only finitely many $\gamma \in \mathrm{SL}_2(R)$ such that $d(\gamma\omega, j) \leq M$. $\square$

Proposition 6.28. *Let $R \subset \mathbb{C}$ be a discrete subring and let $F \in \mathbb{C}[X, Z]'_n$ be a square-free binary form of degree $n \geq 3$. Then there exists $\gamma_{\min} \in \mathrm{SL}_2(R)$ such that $\|F \cdot \gamma_{\min}\| \leq \|F \cdot \gamma\|$ for all $\gamma \in \mathrm{SL}_2(R)$.*

Proof. This proof is analogous to the proof of Proposition 5.9. □

To find this binary form in the orbit F with minimal norm, we do not actually need to check all matrices γ with $d(\gamma z(F), j) \leq c$. Firstly, both $\|F\|$ and $H(F)$ are invariant under the action of the matrix $-I_2$, as it does not change the absolute values of the coefficients. The same holds for the rotation matrices $U_{\zeta_3} = \left(\begin{smallmatrix} \zeta_3 & 0 \\ 0 & \zeta_3^2 \end{smallmatrix}\right)$ and $U_i = \left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right)$. This leads to the following lemma.

Lemma 6.29. *For $R = \mathbb{Z}[i]$ or $R = \mathbb{Z}[\zeta_3]$, let Γ be the subgroup of $\mathrm{SL}_2(R)$ generated by S and T_r for $r \in R$. Let F be a complex square-free binary form of degree $n \geq 3$. Then*

$$\min_{\gamma \in \Gamma} \|F \cdot \gamma\| = \min_{\gamma \in \mathrm{SL}_2(R)} \|F \cdot \gamma\|. \tag{6.30}$$

Proof. We know that there exists $\gamma_{\min} \in \mathrm{SL}_2(R)$ such that $\|F \cdot \gamma_{\min}\|$ is minimal by Proposition 6.28. By Corollary 6.22 we can write γ as a product of matrices of the form S, T_r for $r \in R$ and U where $U = \left(\begin{smallmatrix} r & 0 \\ 0 & r^{-1} \end{smallmatrix}\right)$ for $r = \zeta_3$ or $r = i$. Now using the relations $SU = U^{-1}S$ and $UT_s = T_{sr^2}U$ we can write γ using a matrix in $\langle U \rangle$ at most once, on the right. Removing this matrix on the right has no effect on $\|F \cdot \gamma\|$, and then $\gamma \in \Gamma$ holds. □

To make use of this lemma to reduce the number of matrices we have to iterate over, we do the following. Instead of looking at all matrices with $d(\gamma z(F), j) \leq c$, we only look at the matrices γ that get reduced to the identity matrix when Algorithm 6.18 is applied to the point $\gamma \cdot 2j$. More precisely, if γ' is the matrix we obtain from this algorithm, then we iterate over the matrices with $\gamma'\gamma = I_2$, and $d(\gamma z(F), j)$ small enough.

Algorithm 6.31 Given a discrete norm-Euclidean subring R of $\mathbb{C}$ and a complex square-free binary form $F \in \mathbb{C}[X,Z]'_n$ of degree $n \geq 3$ with $z(F) \in \mathcal{G}_R$, determine a matrix $\gamma_{\min} \in \mathrm{SL}_2(R)$ such that $\|F \cdot \gamma_{\min}\|$ is minimal.

1: Let $\gamma_{\min} = I_2$
2: Let $m = \|F\|$
3: Calculate $\varepsilon(F)$
4: Let $c = \cosh^{-1}\left(\left(\frac{m}{\varepsilon(F)\theta(F)}\right)^{1/(n-2)}\right)$
5: Define the list $L = [(I_2, \text{start})]$
6: **for** $(\gamma, \text{previous action}) \in L$ in ascending order of $d(\gamma z(F), j)$ **do**
7: **if** $\|F \cdot \gamma^{-1}\| < m$ **then**
8: Update $m \leftarrow \|F \cdot \gamma^{-1}\|$
9: Update $\gamma_{\min} \leftarrow \gamma^{-1}$
10: Update $c \leftarrow \cosh^{-1}\left(\left(\frac{m}{\varepsilon(F)\theta(F)}\right)^{1/(n-2)}\right)$
11: Throw out all elements γ' of L for which $d(\gamma' \cdot z(F), j) > c$
12: **end if**
13: **if** the previous action was inversion or start **then**
14: **for** all $\tau \in R \setminus \{0\}$ such that $d(\gamma \cdot z(F) + \tau, j) < c$ **do**
15: Let $T_\tau = \begin{pmatrix} 1 & \tau \\ 0 & 1 \end{pmatrix}$
16: Add $(T_\tau \cdot \gamma, \text{translation})$ to L
17: **end for**
18: **end if**
19: **if** the previous action was translation or start **then**
20: Let $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$
21: **if** $|S\gamma \cdot 2j| < 1$, and $|S\gamma \cdot 2j| \leq |S\gamma \cdot 2j + r|$ for all $r \in R$ **then**
22: Add $(S \cdot \gamma, \text{inversion})$ to L
23: **end if**
24: **end if**
25: **end for**

Proof. Let $F \in \mathbb{C}[X,Z]'_n$ be a square-free binary form of degree $n \geq 3$. By Proposition 6.28 there exists a matrix $\gamma_{\min}$ that minimizes $\|F \cdot \gamma_{\min}\|$. Let c' be the upper bound on $d(\gamma z(F), j)$ obtained from Corollary 4.15. If a matrix γ is considered in the `for` loop from line 6 to 25, we add all matrices γ' with $d(\gamma' \cdot 2j, j) < c$ that get reduced to γ in one step of Algorithm 6.18, where c is as defined in the algorithm. Let now γ be a matrix with $d(\gamma \cdot 2j, j) < c$. If we apply Algorithm 6.18 to the point $\gamma \cdot 2j$, we find a matrix γ' such that $\gamma'\gamma \in \mathcal{G}_R$. Inductively, we find that if $\gamma'\gamma = I_2$, then γ is added to the list L at some point in this algorithm.

Let γ be the matrix obtained from Algorithm 6.18 when applied to the point $\gamma_{\min}^{-1} \cdot 2j$ and let n be the amount of times inversion is applied during the execution of this algorithm. Define $\delta = (-1)^n$. Using Proposition 6.19 we find $\gamma\gamma_{\min}^{-1} \cdot 2j = \left(\begin{smallmatrix} r & 0 \\ 0 & r^{-1} \end{smallmatrix}\right)$ for some $r \in R^*$. Let U be this matrix. Now let γ' be the matrix obtained from Algorithm 6.18 when applied to the point $U^{-\delta} \cdot \gamma_{\min}^{-1} \cdot 2j$. If $|\omega|$ is minimal under translation, then so is $|U\omega|$. Therefore if inversion would be applied to some point ω in Algorithm 6.18, it would also be applied to $U\omega$. Otherwise if $|\omega + s|$ is minimal under translation for some non-zero $s \in R$, then $|U(\omega + s)| = |U\omega + r^2 s|$ is also minimal under translation. Now using the relations $SU = U^{-1}S$ and $T_s U = UT_{r^2 s}$, we find

$\gamma' U^{-\delta} = U^{-1}\gamma$, and hence

$$\gamma' \cdot U^{-\delta} = U^{-1}\gamma\gamma_{\min}^{-1} = I_2.$$

So, at some point $U^{-\delta}\gamma_{\min}^{-1}$ is reached in this algorithm. Because $|r| = 1$, we find $\|F \cdot \gamma_{\min}\| = \|F \cdot \gamma_{min} U^{\delta}\|$. Therefore we have found a matrix that minimizes the size of its corresponding binary form.

The j-part of $S\gamma \cdot 2j$ is smaller than the j-part of $\gamma \cdot 2j$ if $|S\gamma \cdot 2j| < 1$. Therefore this algorithm cannot loop. Furthermore, let c be the value of c as defined in line 4. The value of c cannot increase during this algorithm, so we will never add a matrix γ to the list L such that $d(\gamma \cdot 2j, j) > c$. Because there are only finitely many matrices γ with $d(\gamma \cdot 2j, j) \leq c$, this algorithm will at some terminate, at which point we have found a minimizer of $\|F \cdot \gamma\|$. □

Just like for $R = \mathbb{Z}$, we look at the point $S\gamma \cdot 2j$ instead of $S\gamma \cdot z(F)$ in line 21 of the algorithm. We do this so that we can carry out exact calculations, as we can only approximate the point $z(F)$. This ensures that the algorithm does not loop due to numerical error.

For this thesis I have implemented this algorithm into SageMath for all norm-Euclidean subrings of $\mathbb{C}$ not equal to $\mathbb{Z}$. See Appendix B.

To find the binary form in the $\mathrm{SL}_2(R)$-orbit of F with minimal height, we can use the alternative upper bound obtained from equation (4.17). We then need to replace $m = \|F\|$ with $m = H(F)$ in lines 2 and 8, replace $\|F \cdot \gamma^{-1}\|$ with $H(F \cdot \gamma^{-1})$ in line 7 and replace m with $n \cdot m^2$ in lines 4 and 10.

6.4 Reduction over principal ideal domains

We will generalise the reduction algorithm to all discrete principal ideal domains. This will turn out to be more complicated, and we will also not be able to give an explicit algorithm for optimal reduction. There is a famous result stating which discrete subrings of $\mathbb{C}$ are principal ideal domains.

Theorem 6.32 (Stark-Heegner)**.** *The discrete rings $R \subset \mathbb{C}$ not equal to $\mathbb{Z}$ that are principal ideal domains are precisely the rings R_D for $D = -3, -4, -7, -8, -11, -19, -43, -67, -163$.*

We have already proven the case of $D = -3, -4, -7, -8, -11$, as all (norm-)Euclidean domains are also principal ideal domains. Gauss was able to show that R_D is also a principal ideal domain if $D = -19, -43, -67, -163$. Heegner almost proved that these are the only values of D for which R_D is a principal ideal domain in 1952, but there was a gap in his proof. Stark filled this gap in 1967 [7].

Lemma 6.33. *Let $R \subset \mathbb{C}$ be a discrete principal ideal domain not equal to $\mathbb{Z}$. Then for all $\tau \in \mathbb{C}$ and $K > 0$ there exist coprime elements $c, d \in R$ with $c \neq 0$ such that $|c\tau + d| < K$.*

Proof. We can define an action of R on $\mathbb{C}$ given by addition. Then this action has a fundamental domain given by the closed and filled parallelogram P with corners $0, 1, \alpha, \alpha + 1$, where $\alpha \in \mathbb{C}$ is such that $R = \mathbb{Z} + \alpha\mathbb{Z}$. This is a closed and bounded subset of $\mathbb{C}$, and it is therefore compact.

Let $\tau \in \mathbb{C}$. For all integers $n \geq 0$, there exists an element $r_n \in R$ with $n\tau + r_n \in P$. Consider the sequence $\{n\tau + r_n\}_{n \geq 0} \subset P$. Because P is compact, this sequence has a convergent subsequence. Let $K > 0$. As a convergent sequence is also Cauchy, there exist non-equal $n_1, n_2 \geq 0$ with $|n_1\tau + r_{n_1} - n_2\tau - r_{n_2}| = |(n_1 - n_2)\tau + (r_{n_1} - r_{n_2})| < K$. Let $m = \gcd(n_1 - n_2, r_{n_1} - r_{n_2})$. Then $c = (n_1 - n_2)/m$ and $d = (r_{n_1} - r_{n_2})/m$ satisfy the condition. □

We can generalise the regions $\mathcal{G}_R$ to all discrete subrings of $\mathbb{C}$. For a discrete subring $R \subset \mathbb{C}$ not equal to $\mathbb{Z}$ we define $\mathcal{G}_R$ as follows:

$$\mathcal{G}_R = \{\omega \in \mathcal{H}_3 : |\omega| \leq |\omega + r|, \pi_j(\omega) \geq \pi_j(\gamma\omega) \text{ for all } r \in R, \gamma \in \mathrm{SL}_2(R)\}. \tag{6.34}$$

Again the constraint $|\omega| \leq |\omega + r|$ for all $r \in R$ is equivalent to $|\tau| \leq |\tau + r$ for all $r \in R$ if we write $\omega = \tau + uj$. The region of all $\tau \in \mathbb{C}$ with this property is a hexagon if $R = R_D$ with $D \equiv 1 \mod 4$, and a rectangle if $D \equiv 0 \mod 4$.

This definition of $\mathcal{G}_R$ is equal to our definition when R is norm-Euclidean by Proposition 6.14. Just like in this proposition, the region $\mathcal{G}_R$ also has the following property.

Lemma 6.35. *Let $R \subset \mathbb{C}$ be a discrete ring. For all $\omega \in \mathcal{H}_3$ there exists $\gamma \in \mathrm{SL}_2(R)$ such that $\gamma\omega \in \mathcal{G}_R$.*

Proof. This proof is the same as the second part of the proof of Proposition 6.14. □

For discrete rings $R \subset \mathbb{C}$ that are principal ideal domains we will be able to use this region to define a reduction algorithm. An element $\omega \in \mathcal{H}_3$ has maximal height if there does not exist a matrix $\gamma \in \mathrm{SL}_2(R)$ such that $\pi_j(\omega) < \pi_j(\gamma\omega)$, that is, there are no coprime $c, d \in R$ such that $|c\omega + d| < 1$. Therefore we can reformulate the definition for $\mathcal{G}_R$ as follows:

$$\mathcal{G}_R = \{\omega \in \mathcal{H}_3 : |\omega| \leq |\omega + r| \text{ for all } r \in R\} \setminus \Big(\bigcup_{\substack{c,d \in R \\ \text{coprime}}} \{\omega \in \mathcal{H}_3 : |c\omega + d| < 1\}\Big). \tag{6.36}$$

Lemma 6.37. *Let $R \subset \mathbb{C}$ be a discrete principal ideal domain. Then there exists a finite set N of coprime pairs $(c, d) \in R^2$ such that the following equality holds:*

$$\mathcal{G}_R = \{\omega \in \mathcal{H}_3 : |\omega| \leq |\omega + r| \text{ for all } r \in R\} \setminus \Big(\bigcup_{(c,d) \in N} \{\omega \in \mathcal{H}_3 : |c_j\omega + d_j| < 1\}\Big). \tag{6.38}$$

Proof. Let $T \subset \mathbb{C}$ be the set of all elements which have minimal norm under translation with R. Then T is a bounded set. By Lemma 6.33 there exists a covering of $T \subset \mathbb{C}$ given by the open discs of the form $\{\tau \in \mathbb{C} : |c\tau + d| < \frac{1}{2}\}$ intersected with T for coprime elements $c, d \in R$ with $c \neq 0$. As T is compact there exists a finite subcover. Note that circles of this form have radius $1/2|c|$. Write $\tilde{N}$ for the set of pairs $c, d \in R$ such that $\{\tau \in \mathbb{C} : |c\tau + d| < \frac{1}{2}\} \cap T$ appears in this finite subcover. Now define the set $\mathcal{G}'_R$ as

$$\mathcal{G}'_R = \{\omega \in \mathcal{H}_3 : |\omega| \leq |\omega + r| \text{ for all } r \in R\} \setminus \Big(\bigcup_{(c,d) \in \tilde{N}} \{\omega \in \mathcal{H}_3 : |c\omega + d| < 1\}\Big). \tag{6.39}$$

The region $\mathcal{G}_R$ is clearly a subset of $\mathcal{G}'_R$. Let $\omega = \tau + uj$ be an element of $\mathcal{G}'_R$. Since τ is an element of T, there exists a pair $(c, d) \in \tilde{N}$ such that $|c\tau + d| < \frac{1}{2}$. For this pair (c, d) we find

$$u^2 = \frac{|c\omega + d|^2 - |c\tau + d|^2}{|c|^2} \geq \frac{1 - \frac{1}{2}^2}{|c|^2}. \tag{6.40}$$

Let $\tilde{c}$ be a value of c appearing in a pair $(c, d) \in \tilde{N}$ with maximal norm. Due to the inequality $(1 - \frac{1}{2}^2)/|c|^2 \geq (1 - \frac{1}{2}^2)/|\tilde{c}|^2$ we have the lower bound $\frac{\sqrt{3}}{2|\tilde{c}|}$ for u. Let $r = \sqrt{3}/2|\tilde{c}|$.

If $R = R_D$ for some $D \equiv 0 \mod 4$, then define $M = \frac{1}{2}\sqrt{1-D}$. Otherwise, if $D \equiv 1 \mod 4$ define $M = (1-D)\sqrt{-D}/(-4D)$. In both cases $\tau \in T$ implies $|\tau| \leq M$. Now let N be the finite set of coprime pairs $(c,d) \in R^2$ such that $|c| \leq 1/r$ and $|d| \leq 1 + M/r$. Note that $\tilde{N}$ is a subset of N. We will show that this set satisfies the condition.

Let $\omega \in \mathcal{H}_3$ and suppose $|\omega| \leq |\omega + r|$ for all $r \in R$, and $|c\omega + d| \geq 1$ for all $(c,d) \in N$. Let (c,d) be an arbitrary coprime pair in R. If $(c,d) \in N$, then $|c\omega + d| \geq 1$. If $(c,d) \notin N$, then we either have $|c| > \frac{1}{r}$ or $|d| \geq 1 + M/r$. Write $\omega = \tau + uj$. In the case of $|c| > \frac{1}{r}$ we find $|c\omega + d|^2 \geq |c|^2 u^2 \geq r^2/r^2 = 1$. Otherwise if $|d| \geq 1 + M/r$ and $|c| \leq \frac{1}{r}$ then we have

$$|c\omega + d| \geq |c\tau + d| \geq |d| - |c\tau| \geq 1 + M/r - |c||\tau| \geq 1 + M/r - M/r = 1.$$

Therefore in both cases we find $|c\omega + d| \geq 1$. Hence $\omega \in \mathcal{G}_R$. The other inclusion is trivial. □

We will use this property to generalise Algorithm 6.18, and we will therefore restrict ourselves to discrete complex principal ideal domains.

Algorithm 6.41 Given $\omega \in \mathcal{H}_3$ and a norm-Euclidean ring R find $\gamma \in \mathrm{SL}_2(R)$ such that $\gamma\omega \in \mathcal{G}_R$.

1: Let $\gamma = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
2: **while** $\omega \notin \mathcal{G}_R$ **do**
3: Determine $r \in R$ such that $|\omega + r| \leq |\omega + r'|$ for all $r' \in R$
4: Replace $\gamma \leftarrow \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} \cdot \gamma$
5: Replace $\omega \leftarrow \omega + r$
6: **if** there exist coprime $c, d \in R$ such that $|c\omega + d| < 1$ **then**
7: Determine coprime $c, d \in R$ such that $|c\omega + d|$ is minimal
8: Choose $a, b \in R$ such that $ad - bc = 1$.
9: Let $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$
10: Replace $\omega \leftarrow U\omega$
11: Replace $\gamma \leftarrow U\gamma$
12: **end if**
13: **end while**

Proof. Let $\omega \in \mathcal{H}_3$. By Lemma 6.9 there exist only finitely many possible values of $\pi_j(\gamma\omega)$ for which $\pi_j(\gamma\omega) \geq \pi_j(\omega)$ for $\gamma \in \mathrm{SL}_2(R)$. In line 8 of the algorithm, the value of $\pi_j(\omega)$ increases to $\pi_j(\omega)/|c\omega + d|^2 > \pi_j(\omega)$. This can only be done finitely many times, so at some point at line 6, there will not exist coprime $c, d \in R$ such that $|c\omega + d|^2 < 1$. At this point, $|\omega + r| \geq |\omega|$ for all $r \in R$, so $\omega \in \mathcal{G}_R$. Note that this ω is equal to γ multiplied by the original value of ω. □

Note that determining $r \in R$ such that $|\omega + r| \leq |\omega + r'|$ for all $r' \in R$ is done in the same way as in the norm-Euclidean case.

It is no longer necessarily the case that the distance to j decreases in every step of Algorithm 6.41. Thus we cannot immediately generalise Theorem 6.26 to all discrete complex principal ideal domains. So, it is no longer clear that $\mathcal{G}_R$ consists of points with minimal distance to j with respect to their orbit. However, due to the formula $\cosh^{-1}[(|\omega|^2 + 1)/2\pi_j(\omega)]$ giving the distance between ω and j, we still expect this distance to be small relative to all other points in its

orbit if $\pi_j(\omega)$ is maximal, and $|\omega|$ is minimal under translation. Therefore we can still use this algorithm to find γ such that $z(F \cdot \gamma)$ is close to j, and the upper and lower bound obtained from Theorem 4.11 will be small.

For optimal reduction, we would need to enumerate over all points in the orbit of $z(F)$ for some binary form F, with bounded distance to j. In contrary to the case for norm-Eucldiean rings, the distance to j can increase in some steps of algorithm 6.41. Therefore a point ω in a hyperbolic spehere around j of radius $c > 0$ can exit this hyperbolic sphere during this algorithm. This makes enumerating over all the points in this sphere more complicated. Hutz and Stoll note that this should be workable [5], though they give no way of doing this.

If it is possible to determine an upper bound M on the distance to j of points leaving the hyperbolic sphere in Algorithm 6.41, given that the starting point has distance to j smaller than c, then an algorithm similar to Algorithm 6.31 can be constructed to find a binary form in the orbit of F with minimal size. Note that this upper bound M is dependent on the choice of $a, b \in R$ in line 8 of Algorithm 6.41.

To construct this algorithm similar to Algorithm 6.31, we would need to add all translation matrices $\left(\begin{smallmatrix} 1 & r \\ 0 & 1 \end{smallmatrix}\right)$ such that $d(\omega + r, j) < M$ instead of $d(\omega + r, j) < c$ in line 8 of Algorithm 6.31. Furthermore we would also need to take into account the other inversion matrices $U = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ from line 9 of Algorithm 6.41, apart from only $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$.

References

[1] Lars Ahlfors. Mobius transformations in several dimensions. *Lecture Notes at University of Minnesota*, 1981.

[2] John E Cremona. Reduction of binary cubic and quartic forms. *LMS Journal of Computation and Mathematics*, 2:62–92, 1999.

[3] A Elezi and T Shaska. Reduction of binary forms via the hyperbolic centroid. *Lobachevskii Journal of Mathematics*, 42(1):84–95, 2021.

[4] Charles Hermite. Note sur la réduction des fonctions homogènes à coefficients entiers et à deux indéterminées. 1848.

[5] Benjamin Hutz and Michael Stoll. Smallest representatives of $\mathrm{SL}_2(\mathbb{Z})$ -orbits of binary forms and endomorphisms of $\mathbb{P}^1$. *arXiv preprint arXiv:1805.08579*, 2018.

[6] Gaston Julia. *Étude sur les formes binaires non quadratiques à indéterminées réelles, ou complexes, ou à indéterminées conjugées*. Gauthier-Villars, 1917.

[7] Harold M Stark. A complete determination of the complex quadratic fields of class-number one. *Michigan Mathematical Journal*, 14(1):1–27, 1967.

[8] Peter Stevenhagen. *Algebra 2*. 2017.

[9] Peter Stevenhagen. *Algebra 1*. 2021.

[10] Michael Stoll and John E Cremona. On the reduction theory of binary forms. 2003.

Appendices

A Proof of Proposition 6.14

In the proof of Proposition 6.14 we have postponed the checking of cases to here. We will first repeat the proposition and the first part of the proof.

Proposition A.1 (Proposition 6.14)**.** *Let R be a discrete norm-Euclidean subring of $\mathbb{C}$. Then we can rewrite $\mathcal{G}_R$ as follows:*

$$\mathcal{G}_R = \{\omega \in \mathcal{H}_3 : \pi_j(\omega) \geq \pi_j(\gamma\omega), |\omega| \leq |\omega + r| \text{ for all } \gamma \in \mathrm{SL}_2(R), r \in R\}. \tag{A.2}$$

Furthermore, for all $\omega \in \mathcal{H}_3$, there exists $\gamma \in \mathrm{SL}_2(R)$ such that $\gamma\omega \in \mathcal{G}_R$.

Proof. For the first statement, let $\omega \in \mathcal{G}_R$ and $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(R)$. Then by equation (3.20) we have $\pi_j(\gamma\omega) = \pi_j(\omega)/|c\omega + d|^2$. Now $\pi_j(\gamma\omega) > \pi_j(\omega)$ is equivalent to $|c\omega + d|^2 < 1$ with $c, d \in R$ coprime. We will show that no coprime c, d with this property exist. For each norm-Euclidean ring R we will reduce the possibilities to finitely many cases, and then check each case. First, by definition of $\mathcal{G}_R$, we have $|\omega + r| \geq |\omega| \geq 1$ which covers the case of $|c| = 1$. For other cases, we can rewrite $|c\omega + d|^2$ as follows. Let $\tau \in \mathbb{C}$ and $u > 0$ be such that $\omega = \tau + uj$. We than have

$$|c\omega + d|^2 = |c\tau + d|^2 + |c|^2u^2 = |c|^2|\omega|^2 + c\tau\overline{d} + \overline{c\tau}d + |d|^2. \tag{A.3}$$

Secondly, for all $r \in R$ we have

$$|\tau + r|^2 \geq |\tau|^2 \implies \tau\overline{r} + \overline{\tau}r \geq -|r|^2. \tag{A.4}$$

The main idea to show that $|c\omega + d| \geq 1$ holds for all coprime pairs $c, d \in R$, is to first find some bounds on $|c|$ and $|d|$. Afterwards we will only have finitely many cases left. For these cases we will apply $|\omega| \geq 1$ to equation (6.16), and then use equation (6.17) for suitable values of r.

We will now continue the proof here. First we will cover some general cases. If we apply equation (A.4) to the case of $r = \overline{c}d$ we find $c\tau\overline{d} + \overline{c\tau}d \geq -|c|^2|d|^2$. Combining this with $|\omega| \geq 1$ in (A.3) we find $|c\omega + d|^2 \geq |c|^2 + |d|^2 - |c|^2|d|^2$. Therefore if $|c| \leq 1$ or $|d| \leq 1$ holds, and c, d are not both zero, then $|c\omega + d|^2 \geq 1$ holds.

Denote T for the region of all $\tau \in \mathbb{C}$ which are minimal under translation with elements of R. Then if $\tau \in T$, we also have $-\tau \in T$ and $\overline{\tau} \in T$. Using this we find that if $|c|^2 + c\tau\overline{d} + \overline{c\tau}d + |d|^2 \geq 1$ holds for some pair (c, d) and all $\tau \in T$, then it also holds for the pairs $(\overline{c}, \overline{d})$, $(-c, d)$, (d, c).

We will now cover all the discrete norm-Euclidean subring of $\mathbb{C}$ separately. First consider $R = R_{-3} = \mathbb{Z}[\zeta_3]$. We will calculate an upper bound for $|c|$. As potrayed in Figure 4, $\mathcal{G}_{\mathbb{Z}[\zeta_3]}$ is a hexagonal cylinder with the unit ball taken out. The minimal possible j-part of an element $\omega \in \mathcal{G}_{\mathbb{Z}[\zeta_3]}$ is attained on the unit ball at one of the corners of the hexagon. If $\tau + uj$ is at one of these corners, then τ has equal distance to the three nearest points in $\mathbb{Z}[\zeta_3]$. By symmetry, each of the corners is equally far from the origin. One of the corners is the unique point with equal distance to $0, 1$ and ζ_6. This gives $\tau = \frac{1}{2} + \frac{\sqrt{3}}{6}i$, and therefore $|\tau|^2 \leq \frac{1}{3}$, and $u^2 \geq \frac{2}{3}$. Because $|c\omega + d|^2 \geq |c|^2u^2$, we find $|c|^2 \leq \frac{3}{2}$ if $|c\omega + d|^2 < 1$. The only possible values of $|c|$ are now $|c| = 0$ or $|c| = 1$, which we have both covered already.

For $R = R_{-4} = \mathbb{Z}[i]$, the maximal value of $|\tau|^2$ is $\frac{1}{2}$, so the minimal value of u^2 is also $\frac{1}{2}$, and therefore $|c\omega + d|^2 < 1$ implies $|c|^2 < \frac{1}{2}$, which also leaves $|c| = 0$ and $|c| = 1$ as the only possibilities.

For $R = R_{-7} = \mathbb{Z}[\alpha_{-7}]$ with $\alpha_{-7} = \frac{1}{2} + \frac{\sqrt{7}}{2}i$, the maximal value of $|\tau|^2$ is $\frac{4}{7}$. Therefore the minimal value of u^2 is $\frac{3}{7}$, and we find $|c|^2 < \frac{7}{3}$. This leaves the options $|c| = 0$, $|c| = 1$, and $c = \alpha, \overline{\alpha}, -\alpha, -\overline{\alpha}$, with $\alpha = \alpha_{-7} = \frac{1}{2} + \frac{\sqrt{-7}}{2}$. If $|c|^2 = |\alpha|^2 = 2$, we will find an upper bound for $|d|$. Firstly we know $|c\omega + d|^2 = |c\tau + d|^2 + |c|^2u^2$. Therefore if $|c\omega + d|^2 < 1$ then $|c\tau + d| < \sqrt{1 - |c|^2u^2}$. The triangle inequality applied to $|d + c\tau - c\tau|$ gives:

$$|d| \leq |c\tau + d| + |c\tau| \leq \sqrt{1 - 2 \cdot \frac{3}{7}} + \sqrt{2}\frac{2}{\sqrt{7}}.$$

The only values of d for which this holds are $d = 0, 1, -1, \alpha_D, \overline{\alpha}_D, -\alpha_D, -\overline{\alpha}_D$. By symmetry and because c, d have to be coprime, we only have to check $c = \alpha_D$ and $d = \overline{\alpha}_D$. Applying (A.4) to $r = \overline{\alpha} - 1$ and $r = -1$ we find $\tau(\alpha - 1) + \overline{\tau}(\overline{\alpha} - 1) \geq -2$ and $-\tau - \overline{\tau} \geq -1$. Using this in equation (A.3) we get:

$$\begin{aligned} |\alpha\omega + \overline{\alpha}|^2 &= |\alpha|^2|\omega|^2 + \tau\alpha^2 + \overline{\tau}\overline{\alpha}^2 + |\alpha|^2 \\ &\geq 4 + \tau(\alpha - 1) + \overline{\tau}(\overline{\alpha} - 1) - \tau - \overline{\tau} \geq 4 - 2 - 1 = 1, \end{aligned}$$

as $\alpha^2 = \alpha - 2$ and $\overline{\alpha}^2 = \overline{\alpha} - 2$.

For $R = R_{-8} = \mathbb{Z}[\sqrt{-2}]$ the maximal value of $|\tau|^2$ is $\frac{1}{4} + \frac{1}{2} = \frac{3}{4}$. Therefore the minimal value of u^2 is $\frac{1}{4}$. This gives $|c|^2 < 4$. The possible values for c are then $c = 0, 1, \sqrt{-2}, 1 + \sqrt{-2}$ up to sign and conjugation. If $c = \sqrt{-2}$, we get the following upper bound for $|d|$:

$$|d| \leq |c\tau + d| + |c\tau| \leq \sqrt{1 - 2 \cdot \frac{1}{4}} + \sqrt{2}\frac{1}{2}\sqrt{3}.$$

This leaves the options $d = 0, 1, \sqrt{-2}, 1 + \sqrt{-2}, -1 + \sqrt{-2}$ up to sign. By symmetry and because c, d have to be coprime, we only have the pair $(\sqrt{-2}, 1 + \sqrt{-2})$ left to check. If we apply (A.4) to $r = -\sqrt{-2}$ we find $\tau\sqrt{-2} - \overline{\tau}\sqrt{-2} \geq -2$. If we apply it to $r = 1$ we find $\tau + \overline{\tau} \geq -1$. We can use these equalities in (A.3) to find:

$$|\sqrt{-2}\omega + \sqrt{-2} + 1|^2 = 2|\omega|^2 + \tau\sqrt{-2} - \overline{\tau}\sqrt{-2} + 2(\tau + \overline{\tau}) \geq 5 - 2 - 2 = 1.$$

If $c = 1 + \sqrt{-2}$ we have the following upper bound for $|d|$:

$$|d| \leq |c\tau + d| + |c\tau| \leq \sqrt{1 - 3 \cdot \frac{1}{4}} + \sqrt{3} \cdot \frac{1}{2}\sqrt{3}.$$

This leaves $d = 0, 1, \sqrt{-2}, 1 + \sqrt{-2}, -1 + \sqrt{-2}$ up to sign. By symmetry this leaves the pair $(1 + \sqrt{-2}, -1 + \sqrt{-2})$. Using the inequalities $\tau + \overline{\tau} \geq -1$ and $-\sqrt{-2}\tau + \sqrt{-2}\overline{\tau} \geq -2$ in equation (A.3) we find

$$|(1 + \sqrt{-2})\omega - 1 + \sqrt{-2}|^2 \geq 6 + (\tau + \overline{\tau}) + 2(-\sqrt{-2}\tau + \sqrt{-2}\overline{\tau}) \geq 1.$$

For $R = R_{-11} = \mathbb{Z}[\alpha]$ with $\alpha = 1/2 + \sqrt{-11}/2$, the maximal value of $|\tau|^2$ is $\frac{9}{11}$. Therefore the minimal value for u^2 is $\frac{2}{11}$. Hence for c we find $|c|^2 < \frac{11}{2}$. Up to sign and conjugation this leaves $c = 0, 1, 2, \alpha, \alpha + 1$. We have already covered the case of $c = 0, 1$. First we will check all cases for $c = 2$. We will first determine an upper bound for $|d|$.

$$|d| \leq |c\tau + d| + |c\tau| \leq \sqrt{1 - 4 \cdot \frac{2}{11}} + 2 \cdot \frac{3}{\sqrt{11}}.$$

Up to symmetry this leaves $d = 0, 1, 2, \alpha, \alpha + 1$ with $\alpha = \alpha_{-11} = \frac{1}{2} + \frac{\sqrt{-11}}{2}$. We have already covered the case of $d = 0, 1, 2$. For $d = \alpha$ we find

$$|2\omega + \alpha|^2 \geq 4 + 2(\tau\overline{\alpha} + \overline{\tau}\alpha) + |\alpha|^2 \geq 4 - |\alpha|^2 = 1.$$

For $d = \alpha + 1$ we find

$$|2\omega + \alpha|^2 \geq 4 + (\tau\overline{\alpha} + \overline{\tau}) + (\tau + \overline{\tau}) + |\alpha + 1|^2 = 9 - 6 - 1 = 2.$$

In the case of $c = \alpha$ we will again check an upper bound for $|d|$:

$$|d| \leq |c\tau + d| + |c\tau| \leq \sqrt{1 - 3 \cdot \frac{2}{11}} + \sqrt{3} \cdot \frac{3}{\sqrt{11}}.$$

This leaves up to sign $d = 0, 1, 2, \alpha - 2, \alpha - 1, \alpha, \alpha + 1$. By symmetry and earlier cases we have already covered $d = 0, 1, 2$. For $d = \alpha - 2$ we find

$$\begin{aligned} |\alpha\omega + \alpha - 2|^2 &\geq 3 + 3(\tau + \overline{\tau}) - 2(\overline{\alpha}\tau + \alpha\overline{\tau}) + |\alpha - 2|^2 \\ &= 8 + (\tau + \overline{\tau}) - 2((\overline{\alpha} - 1)\tau + (\alpha - 1)\overline{\tau}) + |\alpha - 2|^2 \geq 8 - 1 - 6. \end{aligned}$$

For $d = \alpha - 1$ we find

$$|\alpha\omega + \alpha - 1|^2 \geq 3 + 2(\tau + \overline{\tau}) - ((\overline{\alpha} - 1)\tau + (\alpha - 1)\overline{\tau}) + |\alpha - 1|^2 \geq 6 - 2 - 3 = 1.$$

For $d = \alpha + 1$ we find

$$|\alpha\omega + \alpha + 1|^2 \geq 3 + 3(\tau + \overline{\tau}) + (\overline{\alpha}\tau + \alpha\overline{\tau}) + |\alpha + 1|^2 \geq 8 - 3 - 3 = 2.$$

In the case of $c = \alpha + 1$ we get the following upper bound for $|d|$:

$$|d| \leq |c\tau + d| + |c\tau| \leq \sqrt{1 - 5 \cdot \frac{2}{11}} + \sqrt{5} \cdot \frac{3}{\sqrt{11}}.$$

Up to sign this leaves $d = 0, 1, 2, \alpha - 2, \alpha - 1, \alpha, \alpha + 1$. Using symmetry and earlier cases we have already coverd all of these except $d = \alpha - 2$. We find

$$|(\alpha + 1)\omega + (\alpha - 2)|^2 \geq 10 - 2\tau(\alpha - 1) - 2\overline{\tau}(\overline{\alpha} - 1) + \tau(\overline{\alpha} - 1) + \overline{\tau}(\alpha - 1) \geq 10 - 6 - 3 = 1.$$

We have now covered all cases of coprime $c, d \in R$, for $R = R_{-3}, R_{-4}, R_{-7}, R_{-8}, R_{-11}$. We omit the proof of the second statement, as this has already been proven. □

B Implementation of algorithms into SageMath

```
def covariant_z0 (F):
    '''
    Calculates the covariant z_0 defined by Stoll and Cremona
    INPUT:
        - ``F`` -- square-free Binary form, a polynomial in two variables
        defined over a discrete norm-Euclidean subring of CC

    OUTPUT: The point z0(F) in the upper half space, i.e. a tuple of a
    complex number and a positive real number.

    TODO:
    Make it so that this also works for polynomials in one variable
    Make sure that covariant_z0(F) outputs two real numbers if F is real
    '''

    n = F.degree()
    zeros = find_projective_zeros(F)

    # determine Q_0, as a 2x2 matrix representing a hermitian quadratic form
    MatCC = MatrixSpace(CC, 2, 2)
    Q_0 = MatCC(0)
    for j in range(n):
        #determine the the coefficients of hermitian form
        alphaj, betaj = zeros[j] # (alphaj : betaj) is the jth zero of F
        factor = 1
        for k in range(n):
            if k != j:
                alphak, betak = zeros[k]
                factor *= norm(alphaj*betak - alphak*betaj)
        factor = factor^(-1/(n-2))

        # add the term |betaj X - alphaj Z|^2 to Q_0
        add_to_Q_0 = factor * MatCC([norm(betaj), -alphaj*conjugate(betaj),
                                    -conjugate(alphaj)*betaj, norm(alphaj)])
        Q_0 += add_to_Q_0

    # apply the zero map to convert Q_0 to z_0
    disc = det(Q_0)
    return (-Q_0[0, 1] / Q_0[0, 0] , sqrt(disc) / Q_0[0, 0])

def covariant_z (F):
    '''
    Calculates the covariant z defined by Stoll and Cremona
    INPUT:
        - ``F`` -- square-free Binary form, a polynomial in two variables
        defined over a discrete norm-Euclidean subring of CC
```

```
OUTPUT: The point z(F) in the upper half space, i.e. a tuple of a
complex number and a positive real number.

TODO:
Make it so that this also works for polynomials in one variable
Make sure that covariant_z(F) outputs two real numbers if F is real
'''

n = F.degree()
zeros = find_projective_zeros(F)

w = var(','.join('w%s'%i for i in range(n-1))) #create (n-1) variables

# nth variable is -sum(other variables)
missing_w = sum(-w[i] for i in range(n-1))
w_total = [w[i] for i in range(n-1)]
w_total.append(missing_w)

# Define D
D = 0
for k in range(n):
    for j in range(k):
        #print(j, ", ", k)
        #print(zeros[j], zeros[k])
        # a zero (alpha : beta) corresponds to a factor (beta*X - alpha*Z)
        (alphaj, betaj) = zeros[j]
        (alphak, betak) = zeros[k]
        D += norm(betaj*alphak - betak*alphaj)*exp(w_total[j] + w_total[k])

#make initial guess (doesn't matter what, since D is convex)
w_initial = [0 for i in range(n-1)]
minimal = minimize(D, w_initial)
minimal = [wi for wi in minimal] #convert w to list
minimal.append(-sum(minimal)) # append the missing variable
t = [exp(wi) for wi in minimal]

# Create positive definite quadratic hermitian form with the ti
# A positive definite hermitian form
# a|X|^2 + bX conj(Z) + conj(b)conj(X)Z + c|Z|^2, with a, c > 0 and b in CC
# is represented by a 2x2 matrix with with coefficients a, b, conj(b), c
# then (-)disc(Q) is the determinant of the corresponding matrix
# (up to sign depending on definition)
MatCC = MatrixSpace(CC, 2, 2)
Q = MatCC(0)
for i in range(n):
    root = zeros[i]
    if root == (1, 0): # root is at infinity
        add_to_Q = MatCC([0, 0, 0, t[i]])
    else:
```

```
            add_to_Q = t[i] * MatCC([1, -root[0],
            -conjugate(root[0]), norm(root[0])])
        Q += add_to_Q

    #convert Q to z
    disc = det(Q)
    return (-Q[0, 1] / Q[0, 0] , sqrt(disc) / Q[0, 0])

def z0_reduce(F):
    '''
    Find matrix A such that z0(F*A) is in the region G_R

    INPUT: square-free Binary form, a polynomial in two variables defined over
        a discrete norm-Euclidean subring of CC

    OUTPUT: - binary form G with z0(G) in the region G_R
            - 2x2 matrix over R such that F*A = G
    '''
    ring = F.coefficients()[0].parent()
    generator = find_second_generator(ring)
    M = MatrixSpace(ring, 2, 2)
    z0 = covariant_z0(F)
    keep_going = True
    Ainv = M([1, 0, 0, 1])
    A = M([1, 0, 0, 1])
    S = M([0, -1, 1, 0])
    while(keep_going):
        z0 = covariant_z0(F)
        # translate such that norm(tau) is minimal
        translate = determine_minimal_translation(z0[0], generator)
        T = M([1, translate, 0, 1])
        Ainv = T*Ainv
        Tinv = M([1, -translate, 0, 1])
        A = A*Tinv
        F = actb(F, Tinv)
        z0 = acth(T, z0)
        if( norm(z0[0]) + z0[1]^2 < 1):
            z0 = acth(S, z0)
            Ainv = S*Ainv
            A = -A*S
            F = actb(F, -S)
        elif (translate == 0): #if both translate == 0 and norm(z) >= 1, z in F
            keep_going = False

    return F, A

def z_reduce(F):
    '''
    Find matrix A such that z(F*A) is in the region G_R
```

```
    INPUT: square-free Binary form, a polynomial in two variables defined over
        a discrete norm-Euclidean subring of CC
    OUTPUT: - binary form G with z(G) in the region G_R
            - 2x2 matrix over R such that F*A = G
    '''
    ring = F.coefficients()[0].parent()
    generator = find_second_generator(ring)
    M = MatrixSpace(ring, 2, 2)
    keep_going = True
    Ainv = M([1, 0, 0, 1])
    A = M([1, 0, 0, 1])
    S = M([0, -1, 1, 0])
    while(keep_going):
        z = covariant_z(F)
        # translate such that norm(tau) is minimal
        translate = determine_minimal_translation(z[0], generator)
        T = M([1, translate, 0, 1])
        Ainv = T*Ainv
        Tinv = M([1, -translate, 0, 1])
        A = A*Tinv
        F = actb(F, Tinv)
        z = acth(T, z)
        # invsersion if necessary
        if( norm(z[0]) + z[1]^2 < 1):
            z = acth(S, z)
            Ainv = S*Ainv
            A = -A*S
            F = actb(F, -S)
        elif (translate == 0): #if both translate == 0 and norm(z) >= 1, z in F
            keep_going = False
    return F, A


def optimal_red(F_start):
    '''
    Find matrix A such that size(F_start * A) is minimal
    Uses Algorithm 6.30 to find the binary form and corresponding matrix with
    minimal size
    INPUT: square-free Binary form, a polynomial in two variables defined over
        a discrete norm-Euclidean subring of CC
    OUTPUT: - the binary form F*A
            - 2x2 matrix over the same ring such that size(F * A) is minimal
    '''
    n = F_start.degree()
    ring = F_start.coefficients()[0].parent()
    generator = find_second_generator(ring)
    M = MatrixSpace(ring, 2, 2)
    (F_opt, A) = z0_reduce(F_start)
    (F_opt, B) = z_reduce(F_opt)
```

```
A = A*B
best_size = size(F_opt)

#compute epsilon and theta:
z = covariant_z(F_opt)

S = M([0, -1, 1, 0])
I = M([1, 0, 0, 1])

beginning_node = (F_opt, I, z, "start", cosh_distance_to_j(z))
# node[0] = binary form
# node[1] = matrix to get from f_start to f
# node[2] = sc_z(f)
# node[3] = previous action
# node[4] = distance from sc_z(f) to j
theta = calculate_theta(F_opt)
epsilon = calculate_epsilon(F_opt)
upper_bound_c = calculate_c(size(F_opt), epsilon, theta, n)

queue = [beginning_node]
B = I
for node in queue:
    queue.pop(0)

    # check if norm is smaller than the previous optimal
    G = node[0]
    if (size(G) < best_size):
        F_opt = G
        B = node[1]
        best_size = size(G)
        upper_bound_c = calculate_c(size(G), epsilon, theta, n)
        # throw out all points with distance too high

        laatste = -1
        while (queue[laatste][4] < upper_bound_c):
            laatste -= 1
        if laatste < -1:
            queue = queue[:laatste+1]

    #add adjacent nodes:
    if (node[3] in ["inversion", "start"]):
        translations = determine_translations(node[2], upper_bound_c,
                                              generator)
        for r in translations:
            Tr = M([1, -r, 0, 1])
            add_to_queue(node, Tr, "translation", queue)

    if (node[3] in ["translation", "start"]):
        z = acth(S*node[1]^-1, (0, 2))
```

```
            if norm(z[0]) + z[1]^2 < 1
                and minimal_under_translation(z[0], generator):
                add_to_queue(node, S, "inversion", queue)

    #done checking points
    return (F_opt, A * B)

'''
AUXILIARY FUNCTIONS
'''

def height(F):
    '''
    calculates the height H(F) of F
    INPUT: polynomial in two variables
    OUTPUT: maximal absolute value of the coefficients
    '''
    return max(abs(ai) for ai in F.coefficients())

def size(F):
    '''
    calculates the height H(F) of F
    INPUT: polynomial in two variables
    OUTPUT: sum of norm of the coefficients
    '''
    return sum(norm(ai) for ai in F.coefficients())

def acth(A, z):
    '''
    left action of matrix ring on upper half space H3
    direct implementation of the formula on
    https://www.lmfdb.org/knowledge/show/mf.bianchi.bianchimodularforms
    INPUT:

        - ``A`` -- 2x2 Matrix

        - ``z`` -- tuple of complex number and positive real number

    OUTPUT: A*z, a tuple of a complex number and a positive real number
    '''
    a = A[0, 0]
    b = A[0, 1]
    c = A[1,0]
    d = A[1,1]
    tau = z[0]
    u = z[1]


    #action on the complex number:
```

```
    first_coordinate = (a*tau + b)*conjugate(c*tau+d) + a * conjugate(c)*u^2
    first_coordinate /= norm(c*tau + d) + norm(c) * u^2 # norm(c) = |c|^2

    second_coordinate = u/(norm(c*tau + d) + norm(c) * u^2)
    return (first_coordinate, second_coordinate)


def actb(F, A):
    '''
    right action of matrix ring on upper half space H3
    INPUT:
        - ``F`` -- Binary form, a polynomial in two variables
        - ``A`` -- 2x2 Matrix

    OUTPUT: F(aX + bZ, cX + dZ)
    NOTE::
    Make sure the binary form and matrix are defined over the same ring
    '''
    a = A[0, 0]
    b = A[0, 1]
    c = A[1,0]
    d = A[1,1]
    X, Z = F.parent().gens()
    return F.subs({X: a*X + b*Z, Z: c*X + d*Z})

def find_projective_zeros(F):
    '''
    Given a binary form, gives the projective zeros of the homogenised version
    of F
    First it calculates the affine zeros. Then it checks
    the multiplicity of the zero at infinity.
    INPUT:
        - ``F`` -- Binary form, a polynomial in two variables

    OUTPUT: list of tuples of complex numbers (alpha, beta) that are zeros of F
    '''
    n = F.degree()
    X, Z = F.parent().gens()
    C.<z> = PolynomialRing(CC) # create polynomial ring over CC in one variable
    f = F.subs({X:z, Z:1})
    roots = f.roots() # roots are represented as (root, multiplicity)
    zeros = []
    for root in roots:
        # add root multiplicity times to zeros
        zeros.extend([(root[0], CC(1)) for i in range(root[1])])

    # find multiplicity of infinity
    mult = 0
    while F.coefficient(X^(n-mult)* Z^mult) == 0:
```

```
        zeros.append((CC(1), CC(0)))
        mult += 1

    return zeros

def determine_minimal_translation(tau, generator):
    '''
    Finds r in ZZ + generator*ZZ such that |tau + r| is minimal
    INPUT: - complex number tau
           - complex number generator that is integral over ZZ
    OUTPUT: complex number r such that |tau + r| <= |tau + r'|
            for all r' in ZZ + generator*ZZ
    '''
    if generator == 0:  #R = ZZ
        return(round(-real(tau)))

    m = -round(imag(tau)/imag(generator))
    if real(generator) == 0: #R = ZZ[sqrt{D}] for D<0
        n = -round(real(tau))
        return(n + m*generator)

    #R = ZZ[1/2 + 1/2sqrt(D)]
    n = -round(real(tau + m*generator))
    translate = n + m*generator
    #it is still possible that the norm is not minimal, check four elements
    if imag(tau + translate) > 0:
        if norm(tau + translate - generator) < norm(tau + translate):
            return (translate -generator)
        if norm(tau + translate - generator+1) < norm(tau + translate):
            return (translate -generator+1)

    if norm(tau + translate + generator) < norm(tau + translate):
        return (translate +generator)
    if norm(tau + translate + generator-1) < norm(tau + translate):
        return (translate +generator-1)

    return (translate)


def find_second_generator(ring):
    '''
    finds r in CC such that R = ZZ + r*ZZ and im(r) > 0 and re(z) in [0, 1/2]
    INPUT:  discrete subring of CC
    OUTPUT: complex number r
    '''
    generators = ring.gens()
    if len(generators) == 1:
        return(0)
    else:
```

```
        generator = generators[1] #Ring = ZZ + generator* ZZ
        if imag(generator) < 0:
            generator *= -1
        generator -= floor(real(generator))
        return ring(generator)


'''
Functions used in optimal_red:
'''
def r(F, z):
    '''
    The function R(F, z) as defined by Stoll and Cremona
    function solely used to calculate theta(F)
    INPUT: - Binary form, homogeneous polynomial in two variables
           - point in the upper half-space, a tuple of a complex number and a
           positive real number

    OUTPUT: positive real number R(F, z)
    '''
    r = 1
    n = F.degree()
    zeros = find_projective_zeros(F)
    #F = prod (beta_i x - alpha_i Z) up to some scaling error
    # with (alpha_i, beta_i) the zeros of F
    for i in range(n):
        (alphai, betai) = zeros[i]
        r *= (norm(betai*z[0] - alphai) + norm(betai)*z[1]^2)
    r = r / (z[1]^n)

    #find a non-zero coefficient
    x, y = F.parent().gens()
    for i in range(n):
        ai = F.coefficient(x^(n-i)*y^i)
        if ai != 0:
            first_nonzero_coeff = ai
            first_nonzero_coeff_place = i
            break

    #check scaling error
    scale = CC(first_nonzero_coeff)
    r *= norm(scale)
    return real(r)

def calculate_theta(f):
    '''
    calculate theta(F) = R(F, z(F)
    INPUT: stable binary form
    Output: positive real number equal to theta(F)
```

```
    '''
    return r(f, covariant_z(f))

def inverse_stereographic(zero):
    '''
    zero in PP^1(CC), output embedding of zero from Riemann spehere into R^3
    Used in calculate_epsilon
    INPUT: tuple of two complex numbers, not both equal to zero
    OUTPUT: tuple of three real numbers in the unit sphere
    '''
    alpha = zero[0]
    beta = zero[1]
    if beta == 0:
        return ((0, 0, 1))
    else:
        tau = alpha/beta
        first_coordinate = (2*real(tau))/(norm(tau) + 1)
        second_coordinate = (2*imag(tau))/(norm(tau) + 1)
        third_coordinate = (norm(tau)-1)/(norm(tau) + 1)
        return ((first_coordinate, second_coordinate, third_coordinate))

def move_to_j(F):
    '''
    Calculate binary form F0 in orbit of F with z(F0) = j
    Used in the calculation of epsilon
    INPUT: square-free binary form
    OUTPUT: binary form in orbit of F with z(F0) = j
    '''
    M = MatrixSpace(CC, 2, 2)
    z = covariant_z(F)
    translate = M([1, -z[0], 0, 1])
    scale = M([z[1]^(-1/2), 0, 0, z[1]^(1/2)])
    A = scale * translate
    return actb(F, A^-1)

def calculate_epsilon(F):
    '''
    Calculates epsilon(F) for square-free binary forms as defined by
    Hutz and Stoll
    INPUT: square-free binary form
    OUTPUT: positive real number equal to epsilon(F)
    '''
    F0 = move_to_j(F)
    F0 = move_to_j(F0)
    n = F.degree()
    zeros = find_projective_zeros(F0)
    #determine max_{i != j} <phi_i, phi_k>
    max_inproduct = -2
    for i in range(n):
```

```
        phi_i = inverse_stereographic(zeros[i])
        for j in range(i):
            phi_j = inverse_stereographic(zeros[j])
            inproduct = 0
            for k in range(3):
                inproduct += phi_i[k] * phi_j[k]
            if inproduct > max_inproduct:
                max_inproduct = inproduct


    eps = (max_inproduct + 1)/2
    eps = (1 - eps)^(n-1)
    eps /= 2
    return eps

def calculate_c(size, epsilon, theta, n):
    '''
    Calculates upper bound c for cosh dist(z(F), j)
    Used in optimal_red
    INPUT:  - positive real number size
            - positive real number epsilon
            - positive real number theta
            - positive integer n >= 3

    OUTPUT: - positive real number
    '''
    c = 2 * ((2 * size)/(epsilon * theta))^(1/(n-2))
    return c


def cosh_distance_to_j(z):
    '''
    calculates cosh of the hyperbolic distance between z and j
    Used in optimal_red
    INPUT:  point in the upper halfspace - tuple of complex number and positive
            real number
    OUTPUT: positive real number
    '''
    return (norm(z[0]) + z[1]^2 + 1)/(2*z[1])




def determine_translations(z, upper_bound, generator):
    '''
    Determine all r in R not equal to 0 such that coshd(z + r, j) < c
    Auxiliary function for optimal_red
    INPUT:  - point in upper half-space - tuple of complex number and positive
              real number
```

```
            - positive real number upper_bound
            - integral complex number such that ZZ + generator*ZZ is a discrete
            norm euclidian subring of CC, and im(generator) > 0 and
            re(generator) = 0, 1/2
        OUTPUT: list of elements r such that cosh d(z + r, j) < upper_bound
        '''

        tau = z[0]
        u = z[1]
        M = upper_bound*2*u + -u^2-1
        translations = []
        if generator == 0:
            #R = ZZ
            min_i = ceil(-tau-M)
            max_i = floor(-tau+M)
            for i in range(min_i, max_i+1):
                if (i != 0):
                    translations.append(i)


        else: #R = ZZ + generator* ZZ
            max_i = floor((-imag(tau)+sqrt(M))/imag(generator))
            min_i = ceil((-imag(tau)-sqrt(M))/imag(generator))
            for i in range(min_i, max_i+1):
                M2 = sqrt(M - imag(tau + i*generator)^2)
                max_j = floor(-real(tau + i*generator)+ M2)
                min_j = ceil(-real(tau + i*generator)- M2)
                for j in range(min_j, max_j+1):
                    if i != 0 or j != 0:
                        translations.append(j + i*generator)


        return (translations)


    def minimal_under_translation(tau, generator):
        '''
        Check whether a complex number is minimal under translation with elements
        of ZZ + generator* ZZ
        INPUT:  - complex number
                - integral complex number such that ZZ + generator*ZZ is a discrete
        OUTPUT: boolean
        '''
        if 2 * real(tau) > 1 or 2 * real(tau) < -1:
            return False

        if generator == 0:
            return True
```

```
    if 2 * imag(tau) > imag(generator) or 2 * imag(tau) < -imag(generator):
        return False

    if real(generator) == 0:
        return True

    minimal = True
    minimal = minimal and norm(tau) < norm(tau + generator)
    minimal = minimal and norm(tau) < norm(tau + generator -1)
    minimal = minimal and norm(tau) < norm(tau - generator)
    minimal = minimal and norm(tau) < norm(tau - generator +1)
    return minimal

def add_to_queue(previous_node, matrix, action_name, queue):
    '''
    Auxiliary function to optimal_red that adds new nodes to list queue
    Calculates the new values for the node, and puts it in the right spot
    INPUT:  - previous_node: node as described in optimal_red
            - matrix: 2x2 matrix, action to be done on node
            - action_name: string, name of the action, equal to "translation"
            or "inversion"
            - queue: current list of nodes to be considered
    '''
    old_f = previous_node[0]
    new_f = actb(old_f, matrix)
    if (action_name == "inversion"):
        #recalculate covariant point
        z = covariant_z(new_f)
    else:
        z = covariant_z(new_f)
    a = previous_node[1] * matrix
    delta = cosh_distance_to_j(z)
    new_node = (new_f, a, z, action_name, delta)

    #check where to put new node
    i = 0
    while (i < len(queue) and queue[i][4] < delta):
        i += 1

    #add new node to queue

    queue.insert(i, new_node)
```