UNIVERSITY OF CALIFORNIA
SANTA CRUZ

CONWAY'S TOPOGRAPH AND SQUARE FORM FACTORIZATION

A thesis submitted in partial satisfaction
of the requirements for the degree of

MASTER OF ARTS

in

MATHEMATICS

by

Brian Ma

June 2022

The Thesis of Brian Ma is
approved:

Professor Martin Weissman, Chair

Professor Robert Boltje

Professor Junecue Suh

Peter Biehl
Vice Provost and Dean of Graduate Studies

Table of Contents

List of Figures

Abstract

Conway's Topograph and Square Form Factorization

Brian Ma

Conway's topograph gives a geometric perspective of binary quadratic forms. Square form factorization is an integer factoring algorithm. We present a description of the algorithm using binary quadratic forms, and translate those steps in terms of the topograph. In particular, we illustrate the reduction operator and relate it to the quadratic progression around an infinity-gon in the topograph by using the connection between reduced forms and riverbends.

Acknowledgements

I would like to thank by advisor Professor Martin Weissman for all of the help that he has provided throughout this entire process. From choosing a topic in the beginning to the writing process in the end, his guidance made things much easier to understand. Furthermore, I appreciated the general career advice he has given as well as always finding time to meet and talk about the thesis. I would also like to express my thanks to Professor Robert Boltje and Professor Junecue Suh for their time and agreeing to serve on my reading committee. Lastly, thank you to all my friends and family that have helped me on this journey.

Introduction

John H. Conway introduces a tool called the topograph in [Con97]. The topograph is used to visualize and provide a simpler way of understanding binary quadratic forms. Daniel Shanks invented Square Form Factorization (SQUFOF), a factoring algorithm using binary quadratic forms. Using this relation, we will illustrate the steps of the algorithm on the topograph in the hopes of making it easier to understand. We give an outline below.

In Chapter 1, we introduce binary quadratic forms and their properties. We then introduce Conway's definitions of lax and strict regarding vectors and bases, leading to the construction of the topograph. We end the chapter with topograph properties, focusing on the case where the discriminant is positive and non-square.

In Chapter 2, we first give the binary quadratic form description from [GW08]. We then describe the algorithm on the topograph. The rest of the chapter is used to connect these two descriptions. In particular, we describe the reduction operation in terms of the topograph.

In Chapter 3, we give a short overview of a variation of Conway's topograph; the dilinear topograph, as presented in [MSW19]. We introduce many analogous properties in the dilinear case. We end by considering an implementation of SQUFOF on the dilinear topograph.

Chapter 1

Preliminaries

1.1 Binary quadratic forms

In this section, we provide the basic definitions and properties on binary quadratic forms, which can be found in the beginning of *Square Form Factorization* [GW08].

Definition 1.1.1. A **binary quadratic form** is a function $Q : \mathbb{Z}^2 \to \mathbb{Z}$ of the form $Q(x, y) = ax^2 + bxy + cy^2$ for some coefficients $a, b, c \in \mathbb{Z}$.

We will also use the notation $Q = (a, b, c)$. We will use $(*, *, c)$ when we want to focus on a particular entry, like the third entry above.

Definition 1.1.2. An integer m is said to be **represented** by a binary quadratic form Q if there exists a vector $(x, y) \in \mathbb{Z}^2$ such that $Q(x, y) = m$.

Definition 1.1.3. The **discriminant** of a binary quadratic form $Q(x, y) = ax^2 + bxy + cy^2$ is given by $\Delta = b^2 - 4ac$.

Definition 1.1.4. A discriminant Δ is called **fundamental** if either of the following holds:

1. $\Delta \equiv 1 \pmod 4$ and square-free.

2. $\Delta \equiv 0 \pmod 4$, $\frac{\Delta}{4}$ is square-free, and $\frac{\Delta}{4} \equiv 2$ or $3 \bmod 4$.

Definition 1.1.5. Let Q be a binary quadratic form and let Δ be its discriminant. If $\Delta < 0$, then Q is called a **definite** form. If $\Delta > 0$, then Q is called an **indefinite** form.

If Q is a definite form, then Q takes on only positive values or only negative values. If Q is an indefinite form, we have two cases depending on the discriminant Δ. If Δ is a square, then Q represents positive values, negative values, and 0. If Δ is non-square, then Q represents positive and negative values only.

We now point out some special types of binary quadratic forms. Let $Q = (a, b, c)$. Then $(a, -b, c)$ is called the **opposite** of Q and (c, b, a) is called the **associate** of Q. If $Q = (k, kn, c)$, then Q is called an **ambiguous** form. If $Q = (*, *, c^2)$, then Q is called a **square form**.

Definition 1.1.6. Let Q_1, Q_2 be binary quadratic forms. We say Q_1 is **equivalent** to Q_2 if there exists a matrix $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in GL_2(\mathbb{Z})$ such that

$$Q_1(x, y) = Q_2(\alpha x + \beta y, \gamma x + \delta y).$$

More specifically, if $\det(A) = -1$, we say the equivalence is **improper**; if $\det(A) = 1$, we say the equivalence is **proper**.

We mention that a form (a, b, c) and its opposite $(a, -b, c)$ are improperly equivalent to each other. The same is true for a form and its associate. An ambiguous form (k, kn, c) is improperly equivalent to itself. Furthermore, a form (a, b, c) is properly equivalent to the opposite of its associate $(c, -b, a)$.

The next definition will play an important part in translating the algorithm in terms of the topograph.

Definition 1.1.7. Let $Q = (a, b, c)$ be an indefinite binary quadratic form with discriminant Δ. We say Q is **reduced** if $|\sqrt{\Delta} - 2|a|| < b < \sqrt{\Delta}$.

Equivalently, Q is reduced if $|\sqrt{\Delta} - 2|c|| < b < \sqrt{\Delta}$. Thus, there is a sort of symmetry in regards to switching a and c. We will see this sort of symmetry again in the next chapter.

1.2 Conway's topograph

In this section, we introduce Conway's notion of strict and lax vectors and bases to construct the topograph. This process can be found in the first chapter of *The Sensual (Quadratic) Form* [Con97].

Definition 1.2.1. Let $\vec{v} = (a, b) \in \mathbb{Z}^2$. The vector $\vec{v}$ is called **primitive** if $\gcd(a, b) = 1$.

Primitive vectors and bases have the following relation:

Proposition 1.2.2 ([Wei17], *pg.231*)**.** *Let $(\vec{v_1}, \vec{v_2})$ be a basis of $\mathbb{Z}^2$. Then both $\vec{v_1}$ and $\vec{v_2}$ are primitive vectors. Conversely, if a vector $\vec{v_1}$ is a primitive vector, there exists another primitive vector $\vec{v_2}$ such that $(\vec{v_1}, \vec{v_2})$ is a basis of $\mathbb{Z}^2$.*

Let Q be a binary quadratic form. We have the property $Q(\vec{v}) = Q(-\vec{v})$. Thus, we can think of $\vec{v}$ and $-\vec{v}$ as almost the same vector. To treat this property, we introduce Conway's notions of lax and strict. Below, $e_i \in \mathbb{Z}^2$ denotes a primitive vector.

Definition 1.2.3. A **lax vector** is a pair of vectors $\pm\vec{v}$, where $\vec{v} \in \mathbb{Z}^2$ is a primitive vector. A **lax basis** is a set $\{\pm e_1, \pm e_2\}$, where the ordered tuple (e_1, e_2) is a basis of $\mathbb{Z}^2$.

We use strictness when making a distinction between the signs; that is, we say $\vec{v}$ (or $-\vec{v}$), is a **strict** vector. Similarly, after a choice of signs, (e_1, e_2) is called a **strict basis**, i.e., a basis of $\mathbb{Z}^2$.

Definition 1.2.4. A **lax superbasis** is a set $\{\pm e_1, \pm e_2, \pm e_3\}$ where any two distinct lax vectors $\{\pm e_i, \pm e_j\}$ form a lax basis.

Let $\{\pm e_1, \pm e_2, \pm e_3\}$ be a lax superbasis. After a choice of signs such that $e_1 + e_2 + e_3 = 0$, we say that the ordered tuple (e_1, e_2, e_3) is called a **strict superbasis**.

We note some important relations between bases and superbases. Given a lax superbasis $\{\pm e_1, \pm e_2, \pm e_3\}$, it contains precisely 3 lax bases, with each lax vector contained in exactly 2 of the 3 lax bases:

$$\{\pm e_1, \pm e_2\},\ \{\pm e_1, \pm e_3\},\ \{\pm e_2, \pm e_3\}.$$

Conversely, given a lax basis $\{\pm e_1, \pm e_2\}$, it is contained in precisely 2 lax superbases:

$$\{\pm e_1, \pm e_2, \pm(e_1 + e_2)\},\ \{\pm e_1, \pm e_2, \pm(e_1 - e_2)\}.$$

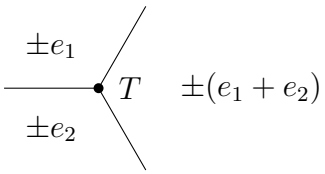
We now introduce Conway's topograph to illustrate these relations.

Definition 1.2.5 (Conway's Topograph)**.** The **topograph** consists of regions, edges, and vertices that represent lax vectors, bases, and superbases respectively. Incidence between the regions, edges, and vertices are given by containment among the vectors, bases, and superbases.

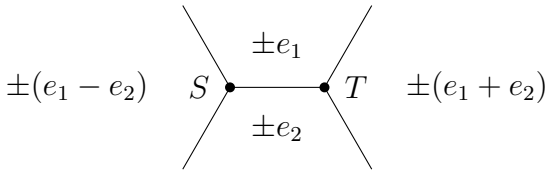
Using the relations, we see each edge divides 2 regions:

$$\pm e_1$$
$$\text{———}$$
$$\pm e_2$$

Here, the edge represents the lax basis $\{\pm e_1, \pm e_2\}$. Extending this, we have a **triad**:



Above, $T = \{\pm e_1, \pm e_2, \pm(e_1 + e_2)\}$ denotes the superbasis. Adding the second superbasis, we have a **cell**:



Following the relations, we can extend the topograph infinitely. Below illustrates how the pattern continues.

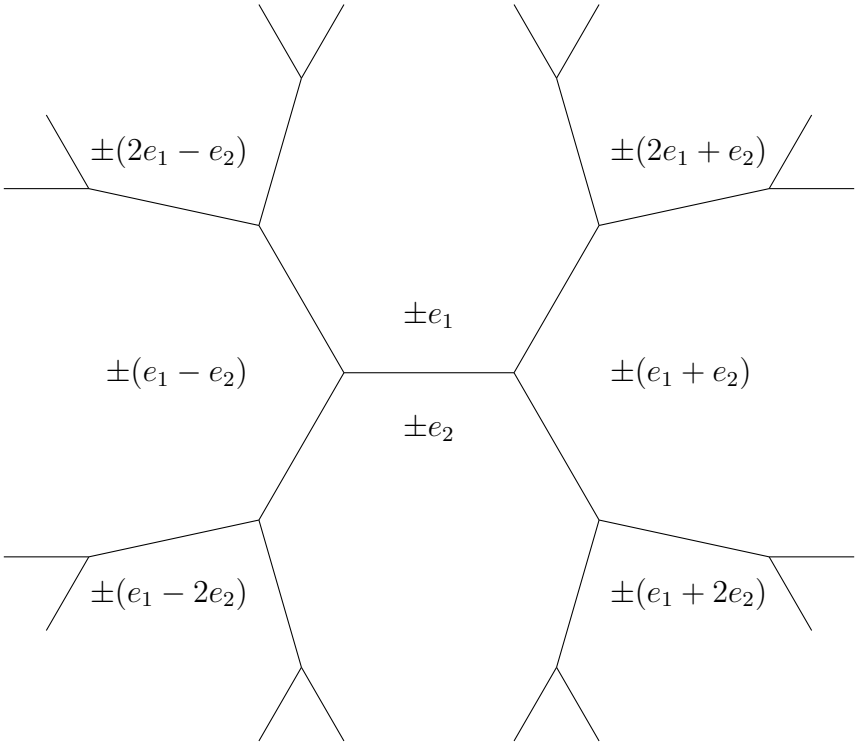


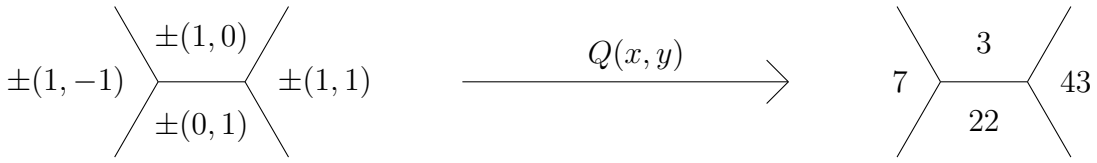
Figure 1.1: The (domain) topograph

We have shown how to construct the topograph. In particular, we have constructed the **domain topograph** above. Instead of labeling the regions by lax vectors, we can label them by the integers represented by those lax vectors.

Definition 1.2.6. Let Q be a binary quadratic form. The **range topograph** of Q is obtained from the domain topograph of Q by labeling each region by the value represented by Q at that region.

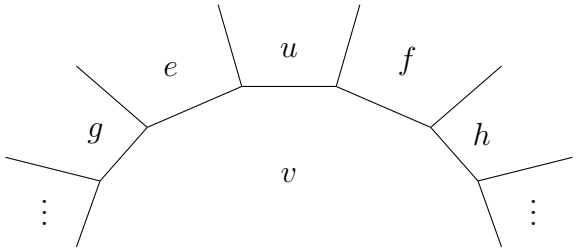
On the domain topograph, the location where $e_1 = \pm(1, 0)$ and $e_2 = \pm(0, 1)$ is called **home basis**. We provide an example to illustrate.

Let $Q(x, y) = 3x^2 + 18xy + 22y^2$. We start at home basis on the domain topograph and apply $Q(x, y)$ to get the range topograph:



We note that in the example above, we have made a choice in the placement of the lax vectors in the cell. That is, by placing $\pm(1,1)$ to the right, the sequence $(\pm(1,0), \pm(0,1), \pm(1,1))$ occurs counterclockwise around a triad. Placing $\pm(1,1)$ to the left would have resulted in the same sequence occurring clockwise around a triad.

In addition to a triad and cell, the topograph also has an **infinity-gon**:

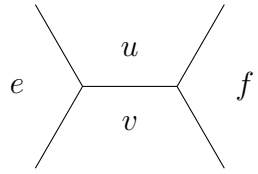


Above, the infinity-gon consists of the fixed region labeled v and all the regions around v.

1.3 Topograph properties

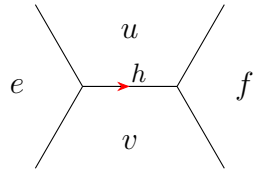
Throughout this section, we will refer to the range topograph by just topograph. In this section, we list several properties of the topograph as well as how properties of binary quadratic forms translate to the topograph. In particular, we will take a further look at the topograph of indefinite forms. These properties and their proofs can be found in *An Illustrated Theory of Numbers* [Wei17]. We first state two very important properties regarding the topograph.

Proposition 1.3.1 (Arithmetic progression rule). *([Wei17], pg.246) Let e, u, v, f be the values around a cell in the topograph as below:*



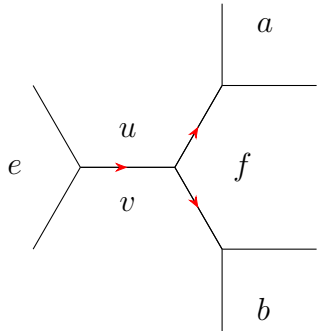
Then the sequence $e, u+v, f$ forms an arithmetic progression; that is, the numbers in the sequence have a common difference.

Let h be this common difference. Then $f - (u + v) = h = (u + v) - e$. Thus, we can write $f = u + v + h$ and $e = u + v - h$. On the topograph, we label the edge between u and v with this common difference:



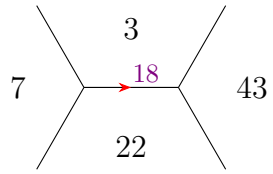
We will also use the notation (u, h, v) to denote a cell such as the one above. We note that the binary quadratic form $Q(x, y) = ux^2 + hxy + vy^2$ has the above cell at home basis, again with the placement such that $Q(1, 1) = f$.

Proposition 1.3.2 (Conway's climbing principle). *([Wei17], pg.259) Consider a region in the topograph as below:*

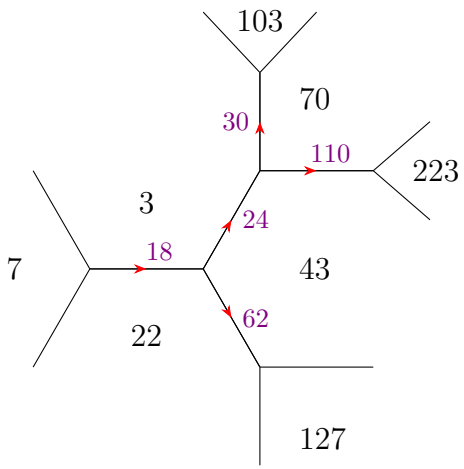


Suppose $u, v > 0$. If the arithmetic progression $e, u+v, f$ increases, then the arithmetic progressions $v, u+f, a$ and $u, v+f, b$ also increases.

We go back to our example $Q(x, y) = 3x^2 + 18xy + 22y^2$. At the cell containing home basis, the values on the topograph were:

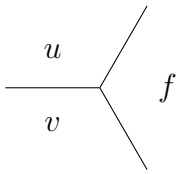


Since $43 = 3 + 22 + h$, we see that the common difference is $h = 18$. We see the increase in the arithmetic progression as we expand towards the right:

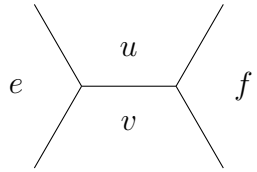


We now state how the discriminant Δ of a binary quadratic form Q can be seen on the topograph and how all three definitions are equivalent.

Definition 1.3.3. Let



be a triad. Then the **discriminant** is given by $u^2 + v^2 + f^2 - 2(uf + fv + vu)$. Let



be a cell. Then the **discriminant** is given by $(u - v)^2 - ef$.

Proposition 1.3.4 ([Wei17], *pg.251*)**.** *In the topograph of a binary quadratic form $Q = (a, b, c)$, the discriminant at any cell and at any triad is equal to Δ.*

We now state some facts regarding the general structure of the topograph. We first introduce some terminology. Let P_1 and P_2 be two vertices in the topograph. A **simple path** is a path of edges between P_1 and P_2 that does not repeat any vertices or edges. A **simple loop** is a simple path such that $P_1 = P_2$. A **tree** is a graph with no simple loops.

Proposition 1.3.5. *The topograph is a tree, i.e., it is simply-connected: Given any lax basis, we can get to home basis along a unique simple path.*

The following states how equivalence of binary quadratic forms can be seen on the topograph.

Proposition 1.3.6. *Two binary quadratic forms are equivalent if they share a triad in common.*

In terms of the topograph, rotation symmetries are proper equivalences, while reflection symmetries are improper equivalences. We now turn to some further properties on the topograph of an indefinite form. Recall that we have the discriminant $\Delta > 0$. We will focus on the case where Δ is also non-square.

Definition 1.3.7. The **river** consists of the edge segments that separate positive regions from negative regions.

Proposition 1.3.8. *A topograph has exactly one river. The river is endless, non-branching, and periodic.*

We note that by the periodicity of the river, the values along the river will also be periodic.

On the river, reflection symmetries can occur at two different places: an edge or a vertex. At an edge, we have a symmetric cell; at a vertex, we have a symmetric triad. We make note of these locations.

Definition 1.3.9 ([Wei17], *pg.289*)**.** A symmetric cell or a symmetric triad of the river is called an **ambiguous river segment**.

Figure 2.1 illustrates the two types of ambiguous river segments in the context of the algorithm. Furthermore, we make note of another type of cell on the river.

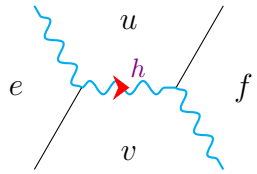
Definition 1.3.10. Riverbends are cells of the topograph consisting of three river segments as below:

The riverbend on the left will be called an **up-down riverbend** and the riverbend on the right will be called a **down-up** riverbend.

We can be more specific by including the direction of the edge weight, i.e., the common difference h.

Definition 1.3.11. An **oriented cell** is a cell where the direction of the edge weight is given. An oriented cell that is also a riverbend is called an **oriented riverbend**.

We will often denote an oriented riverbend by R. For example, let R be the oriented riverbend below:

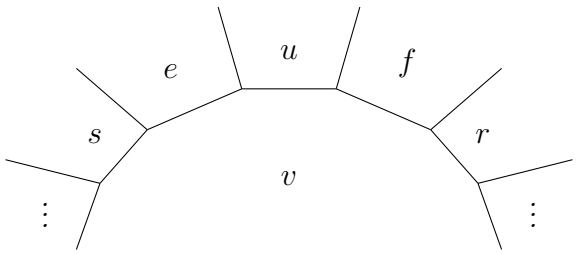


Then $f = u + v + h$ and $e = u + v - h$. So the indefinite form (u, h, v) has the sequence $(\pm(1,0), \pm(0,1), \pm(1,1))$ occurring counterclockwise around a triad back in the domain topograph. Unless stated otherwise, we will assume this orientation of the topograph.

We remark that the edge weight h can positive, negative, or zero. In fact, if a river segment has edge weight $h = 0$, then it is an ambiguous river segment as $e = f$ and the direction would not matter.

We now state an important property regarding an infinity-gon of a topograph. Recall that a sequence of numbers has an arithmetic progression if they have a common difference. A sequence of numbers has a quadratic progression if the sequence of their differences has a common difference.

Proposition 1.3.12 ([Wei17], *pg.290*)**.** *Consider an infinity-gon in a topograph with fixed region labeled v:*



Then the sequence of values around the infinity-gon form a quadratic progression with acceleration $2v$.

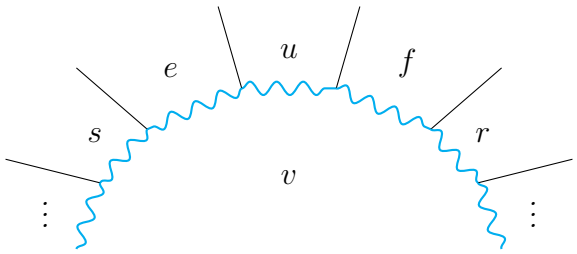
We describe this quadratic progression. First, let h be the edge weight between u and v. Consider the cell (u, h, v). Then the equation $a(t) = vt^2 + ht + u$ indexes the values around the infinity-gon. That is, $a(t)$ gives the value of the region at location t. For example, at $t = 0$, $a(0) = u$. At $t = 1$, we have $a(1) = v + h + u = f$. At $t = -1$, we have $a(-1) = v - h + u = e$. We get the last equality in the previous two equations by the arithmetic progression rule. We also note that the acceleration is $a''(t) = 2v$.

Now, suppose an infinity-gon is given as above in Proposition 1.3.12. We see that as we increment t, we move clockwise around the infinity-gon. Similarly, as we decrement t, we move counterclockwise around the infinity-gon.

Furthermore, we emphasize that in defining $a(t)$, a choice was made in picking a cell along the infinity-gon; in the above case the cell being (u, h, v). However, the quadratic progression does not depend on this choice. It only changes the location of the starting position. For example, let h' denote the edge weight between e and v, and pick the cell (e, h', v). Then defining $a(t) = vt^2 + h't + e$, we still have $a''(t) = 2v$, but now we have $a(0) = e$.

We now take a closer look in the indefinite case (with positive non-square discriminant), and the behavior of the river around an infinity-gon due to the quadratic progression.

Theorem 1.3.13 ([Wei17], *pg.291*)**.** *Let Q be an indefinite binary quadratic form, with discriminant Δ non-square. Consider an infinity-gon in the topograph of Q, with fixed region labeled v and the river traveling around the infinity-gon:*



Then the river cannot move along the infinity-gon indefinitely, i.e., only finitely many edges of the infinity-gon are river segments.

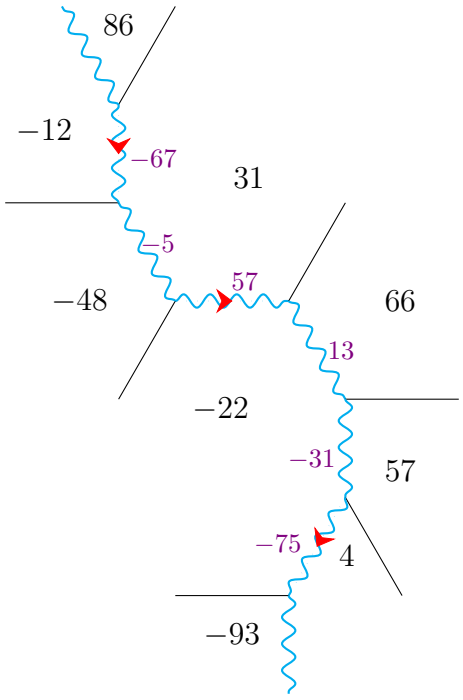
From this theorem, we see that for a given infinity-gon, there must be cells along it which are riverbends. In fact, each infinity-gon will have exactly two such cells which are riverbends.

As the river is endless, starting at a riverbend on the topograph, we find other riverbends as we travel in either direction along the river. We now introduce some notation.

Definition 1.3.14. Let R be an oriented riverbend. The first riverbend we encounter as we travel in the direction of the edge weight will be called the **next riverbend**, denoted $\rho(R)$. The first riverbend we encounter traveling in the reverse direction of the edge weight will be called the **previous riverbend**, denoted $\rho^{-1}(R)$.

Furthermore, we remark that the type of riverbend alternates as we travel along the river. That is, if R is an up-down riverbend, then $\rho(R)$ will be a down-up riverbend. The next riverbend after $\rho(R)$ will then be an up-down riverbend again.

We illustrate this below. Consider the following topograph, where cells with edges marked with arrows are riverbends:



So, if $R = (31, 57, -22)$, then $\rho(R) = (4, -75, -22)$ and $\rho^{-1}(R) = (31, -67, -12)$.

Chapter 2

Square Form Factorization

In the first two sections, we describe the factorization algorithm SQUFOF as invented by Shanks and studied in [GW08]. Then we describe those steps in terms of the topograph and note some differences. In the next three sections, we relate the reduction operator and the quadratic progression around an infinity-gon to riverbends on the topograph. We then make an analogous relation with the inverse reduction operator. We end the chapter by giving an example.

2.1 Description of the algorithm

SQUFOF uses indefinite reduced binary quadratic forms to factor integers. The discriminant plays a key part. If $N = pq$ is a factorization of N, then the indefinite binary quadratic forms $x^2 - Ny^2$ and $px^2 - qy^2$ have the same discriminant. This coincidence, and others that look like it, suggest one might stumble upon such a factorization by applying transformations to a binary quadratic form which preserve the discriminant.

We now define a key transformation used in SQUFOF, as presented in

Binary Quadratic Forms [Bue89].

Definition 2.1.1 ([Bue89], *pg.22, pg.199*)**.** Let $f = (a, b, c)$ be an indefinite binary quadratic form, with $ac \neq 0$. Let Δ be the discriminant of f. Then the **reduction operator** ρ is defined by

$$\rho(a, b, c) = (c, -b + n(2c), n^2c - nb + a)$$

where

$$n = \begin{cases} -\left\lfloor \dfrac{-(\sqrt{\Delta} + b)}{2c} \right\rfloor & \text{if } c < 0 \\ \\ \left\lfloor \dfrac{\sqrt{\Delta} + b}{2c} \right\rfloor & \text{if } c > 0 \end{cases}$$

Although not used in the description of SQUFOF that we give, we also give the definition of ρ^{-1}, the **inverse reduction operator**. We have $\rho^{-1}(a, b, c) = (n^2a - nb + c, -b + n(2a), a)$, where n is defined as in the above definition switching c with a.

We state several important properties of the reduction operator. First, the reduction operator preserves the discriminant; if f is an indefinite binary quadratic form with discriminant Δ, the $\rho(f)$ also has discriminant Δ. Furthermore, $\rho(f)$ is properly equivalent to f. If f is a reduced form, then $\rho(f)$ is also reduced. If f is not reduced, then $\rho^k(f)$ is reduced for some finite number k. That is, we apply the reduction operator k times. The above properties also hold true for ρ^{-1}. Additionally, if f is reduced, we have $\rho(\rho^{-1}(f)) = \rho^{-1}(\rho(f)) = f$.

For square forms, we have another transformation.

Definition 2.1.2. Let $f = (a, b, c^2)$ be a square form. Then the **inverse square root** of f is defined as $(-c \cdot a, -b, -c)$.

We note that the inverse square root also preserves the discriminant. However, the inverse square root of a square form f may not be (properly) equivalent to f.

We now list the steps of the algorithm, following the notation presented in [GW08]. We will focus on the main steps, omitting the optimization parts.

1. **Initialize:** Let N be an odd positive integer. If $N \equiv 1 \bmod 4$ set the discriminant $\Delta \leftarrow N$. Then set

$$b \leftarrow 2 \left\lfloor \frac{\lfloor \sqrt{\Delta} \rfloor - 1}{2} \right\rfloor + 1$$

and

$$F \leftarrow \left(1, b, \frac{b^2 - \Delta}{4}\right).$$

Otherwise, $N \equiv 3 \bmod 4$. Set $\Delta \leftarrow 4N$ and

$$b \leftarrow 2 \left\lfloor \frac{\lfloor \sqrt{\Delta} \rfloor}{2} \right\rfloor$$

and

$$F \leftarrow \left(1, b, \frac{b^2 - \Delta}{4}\right).$$

Set $i \leftarrow 2$.

2. **Cycle Forward:**

(a) Set $F = (A, B, C) \leftarrow \rho(F)$, where ρ is the reduction operator.

(b) If i is odd, or i is even and C is not a square, set $i \leftarrow i + 1$ and go back to Step 2a. If i is even, and C is a perfect square, move to Step 3.

3. **Compute inverse square root:** Set $G = (a, b, c) \leftarrow (-A\sqrt{C}, -B, -\sqrt{C})$.

4. **Cycle Backward:**

   (a) Set $b' \leftarrow b$ and $G = (a, b, c) \leftarrow \rho(G)$.

   (b) If $b' = b$, go to Step 5, else go back to Step 4a.

5. **Output factor of N:** If c is even, set $c \leftarrow c/2$. Output $|c|$.

2.2 Description on the topograph

In this section, we give a general description of the steps of the algorithm in terms of the topograph, similar to the one presented in [Wei17]. We start on the topograph of the ambiguous form $Q_1(x, y) = x^2 - Ny^2$, travel along the river, and end near an ambiguous river segment on the topograph of the ambiguous form $Q_2(x, y) = px^2 - qy^2$.

To match the steps in the algorithm, we start at the home basis of the form $-Nx^2 + y^2$. Note that this is the opposite of the associate of Q_1, and hence properly equivalent to Q_1.

1. **Initialize:** Let N be an odd positive integer. Set $F = (A, B, C) \leftarrow (-N, 0, 1)$

2. **Cycle Forward:** Travel along the river until we find a square form (a, b, c^2).

3. **Compute the inverse square root:** Set $G = (A, B, C) \leftarrow (-ca, -b, -c)$.

4. **Cycle Backward:** Continue traveling on the river until an ambiguous river segment is found.

5. **Output factor N:** Output factor of N.

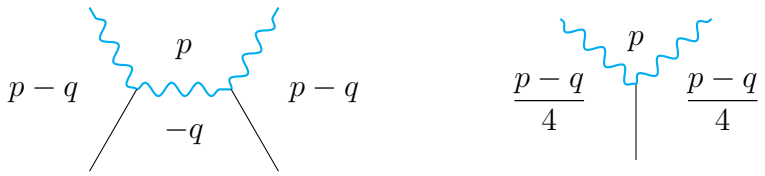
We make a note of some of the differences between the two descriptions. Since we start at home basis of $Q_1(x, y) = -Nx^2 + y^2$, the topograph description always uses discriminant $\Delta = 4N$. This contrasts with the [GW08] description, where Δ is determined such that it is fundamental.

Furthermore, in Step 1, we start the initialization at the ambiguous river segment $(-N, 0, 1)$. Now, consider the case where $N \equiv 3 \bmod 4$, i.e., both descriptions have $\Delta = 4N$. Applying the reduction operator ρ to $(-N, 0, 1)$, we have $\rho(-N, 0, 1) = (1, 2n, n^2 - N)$, where $n = \left\lfloor \frac{\sqrt{\Delta}}{2} \right\rfloor$. This matches with the initialization in the first description. We remark that this will not be the case when $N \equiv 1 \bmod 4$. However, as noted in [GW08], the algorithm will still work for non-fundamental discriminant.

Steps 2 and 4 regarding traveling along the river involve the quadratic progression around an infinity-gon.

For Step 5, the algorithm ends at a cell in the topograph near an ambiguous river segment of $Q_2(x, y) = px^2 - qy^2$. In fact, it will be the nearest cell that is a riverbend. We show the two possible ambiguous river segments that the algorithm ends near.

Recall that an ambiguous river segment is a symmetric cell or symmetric triad, i.e, where the reflection occurs. Up to symmetry, we have:



(a) Type H

(b) Type Y

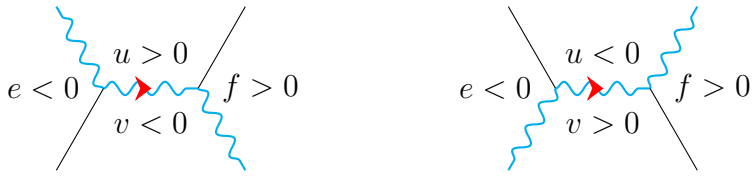
Figure 2.1: Types of ambiguous river segments

We will go into further detail regarding these steps in the next few sections and in the example in Section 2.7.

2.3 Reduced forms and riverbends

In this section, we take a deeper look at the reduction operator and the cycling step of SQUFOF, and how that translates on the topograph. We will first need a relation regarding reduced forms. The main theorem and its proof can be found in *Arithmetic of arithmetic Coxeter groups* [MSW19].

We recall the two types of riverbends given in Definition 1.3.10. Up to orientation, we have:



(a) up-down (b) down-up

Figure 2.2: Types of riverbends

Let h denote the edge weight between u and v. In both cases above, we have $h > 0$. If R is an oriented riverbend such that the edge weight is negative, we can take the opposite of the associate of R to get a form properly equivalent to R with positive edge weight. We use this to make the connection between reduced forms and riverbends.

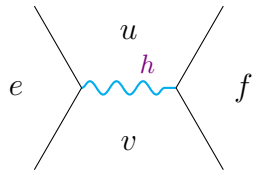
Theorem 2.3.1. *Let (u, h, v) denote a cell on the topograph, where h is the edge weight between u and v. Assume the discriminant $\Delta = h^2 - 4uv$ is positive and*

non-square. Then the cell (u, h, v) is a riverbend if and only if the binary quadratic form $Q(x, y) = ux^2 + hxy + vy^2$ is reduced.

Proof. The forward direction is given in [MSW19, *pg. 443*]. In fact, we use the proof given there to explicitly show the reverse direction.

Now, suppose $Q(x, y) = ux^2 + hxy + vy^2$ is a reduced form. So, $0 \leq |\sqrt{\Delta} - 2|u|| < h < \sqrt{\Delta}$. We want to show that the cell (u, h, v) is a riverbend. First, let $\text{sgn}(x)$ denote the sign of a number x.

Using the discriminant, we have $h^2 = \Delta + 4uv$. Since $Q(x, y)$ is reduced, we have $h = \sqrt{\Delta + 4uv} < \sqrt{\Delta}$. Then we must have $4uv < 0$, and so $\text{sgn}(u) \neq \text{sgn}(v)$. Thus, the edge between u and v must be a river segment. So far, we have (where $e = u + v - h$ and $f = u + v + h$):



What is left to show is $\text{sgn}(e) \neq \text{sgn}(f)$. Again by the reduced property, we have $|\sqrt{\Delta} - 2|u|| < h$. So, $(\sqrt{\Delta} - 2|u|)^2 < h^2$. Then,

$$\begin{aligned}
\Delta - 4|u|\sqrt{\Delta} + 4u^2 &< h^2 \\
4u^2 + \Delta - h^2 &< 4|u|\sqrt{\Delta} \\
4u^2 - 4uv &< 4|u|\sqrt{\Delta}, \text{ by the discriminant} \\
4u(u - v) &< 4|u|\sqrt{\Delta} \\
4|u|\text{sgn}(u)(u - v) &< 4|u|\sqrt{\Delta} \\
\text{sgn}(u)(u - v) &< \sqrt{\Delta} \\
(u - v)^2 &< \Delta
\end{aligned}$$

But we also have $\Delta = (u-v)^2 - ef$, the discriminant at a cell. So, $(u-v)^2 < (u-v)^2 - ef$. Hence, $ef < 0$ and we must have $\text{sgn}(e) \neq \text{sgn}(f)$. So the cell (u, h, v) must be a riverbend as given in Figure 2.2. □

Thus, for every riverbend on the topograph, there is an associated reduced form. And for every reduced form, there is an associated riverbend.

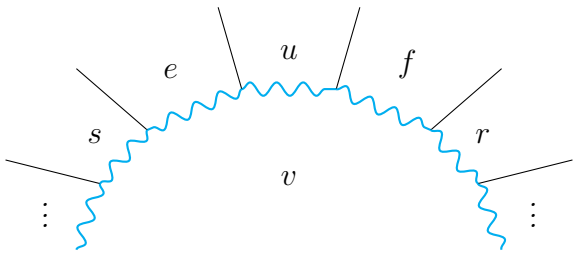
Using this relation, we now see that as the reduction operator is applied, we not only travel along the river, but we travel the river by jumping from riverbend to riverbend.

2.4 Roots and riverbends

In this section, we show how to locate the riverbends on an infinity-gon using the quadratic progression.

We recall from Section 1.3 that given an infinity-gon with fixed region v, a cell along the infinity-gon (u, h, v), the quadratic progression around the infinity-gon is given by $a(t) = vt^2 + ht + u$. We also recall that the choice of cell does not change the quadratic progression.

Theorem 2.4.1. *Let Q be an indefinite binary quadratic form with discriminant Δ non-square. Consider an infinity-gon in the range topograph of Q, with fixed region labeled v. Suppose the river is traveling along this infinity-gon as illustrated below:*



Let (u, h, v) be a cell on the infinity-gon, such that the edge between u and v is a river segment, where h denotes the edge weight between u and v. Define $a(t) = vt^2 + ht + u$. Then $a(t)$ has one negative root, denote with r_1, and one positive root, denote with r_2. Suppose that $\lceil r_1 \rceil \neq \lfloor r_2 \rfloor$. Then the riverbends on this infinity-gon will be located at $t = \lceil r_1 \rceil$ and $t = \lfloor r_2 \rfloor$.

Proof. Recall from Theorem 1.3.13 that we know the existence of riverbends at infinity-gons. Also note that u and v have opposite signs, since the edge between u and v is part of the river. So $vu < 0$. Then the discriminant of $a(t)$ is $\delta = h^2 - 4vu > 0$. Thus, $a(t)$ does indeed have two distinct roots which have opposite signs.

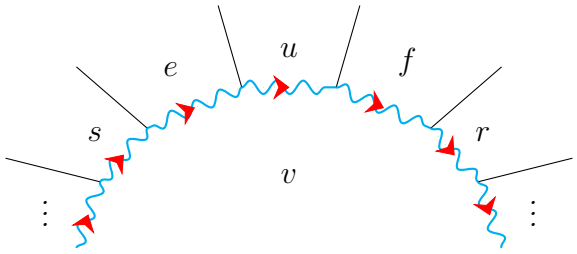
Now, the roots $r_1, r_2 \notin \mathbb{Z}$, as that would imply $a(r_1) = a(r_2) = 0$ appears on the range topograph of Q. But Δ is non-square, so that is not possible. Thus, $\lfloor r_1 \rfloor \neq \lceil r_1 \rceil$. Since $a(t)$ indexes the regions around the infinity-gon, $a(\lfloor r_1 \rfloor)$ and $a(\lceil r_1 \rceil)$ will be values along the infinity-gon. Similarly for r_2. Since $\lceil r_1 \rceil \neq \lfloor r_2 \rfloor$, we have four distinct integers:

$$\lfloor r_1 \rfloor < \lceil r_1 \rceil < \lfloor r_2 \rfloor < \lceil r_2 \rceil$$

Evaluating $a(t)$ at these four integers yields a pattern of signs: either $(-, +, +, -)$ or $(+, -, -, +)$. So we have exactly two sign switches as we travel along the regions around the infinity-gon. Then the edge where the sign switch occurs must be a river segment. Thus, the roots of $a(t)$ locates the riverbends on the infinity-gon. □

We can say more on how the roots locate the riverbends.

Corollary 2.4.2. *Keep the assumptions of Theorem 2.4.1. Furthermore, assume that the infinity-gon is oriented as below:*



Then $t = \lceil r_1 \rceil$ locates the up-down riverbend and $t = \lfloor r_2 \rfloor$ locates the down-up riverbend.

Proof. We know that the infinity-gon has two riverbends. In this orientation, the up-down riverbend is on the left and the down-up riverbend is on the right. We have the quadratic progression as $a(t) = vt^2 + ht + u$. When we increment t, we move clockwise around the infinity-gon, i.e., in the same direction as the orientation. □

We illustrate this below:

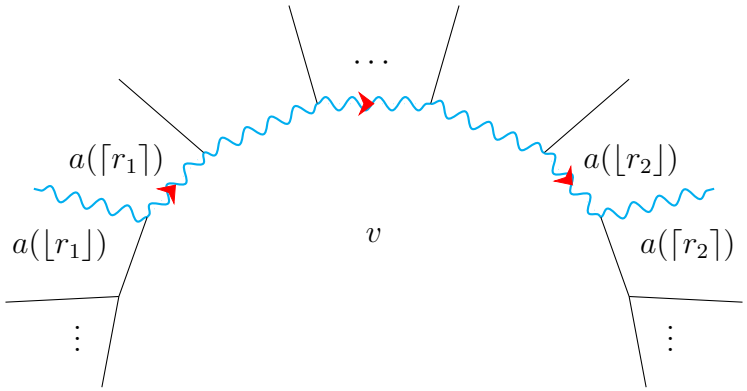


Figure 2.3: Locating riverbends

We now write the riverbends in terms of the quadratic progression $a(t)$. We have the cell $(a(\lceil r_1 \rceil), h_1, v)$ as the up-down riverbend, and the cell $(a(\lfloor r_2 \rfloor), h_2, v)$

as the down-up riverbend.

To find h_1 and h_2, we use the arithmetic progression in the orientation given above. We have

$$\begin{aligned} a(\lceil r_1 \rceil) + v - h_1 &= a(\lfloor r_1 \rfloor) \\ h_1 &= a(\lceil r_1 \rceil) - a(\lfloor r_1 \rfloor) + v \end{aligned}$$

Similarly,

$$\begin{aligned} a(\lfloor r_2 \rfloor) + v + h_2 &= a(\lceil r_2 \rceil) \\ h_2 &= a(\lceil r_2 \rceil) - a(\lfloor r_2 \rfloor) - v \end{aligned}$$

Thus,

$$(a(\lceil r_1 \rceil), a(\lceil r_1 \rceil) - a(\lfloor r_1 \rfloor) + v, v) \tag{2.1}$$

denotes the up-down riverbend and

$$(a(\lfloor r_2 \rfloor), a(\lceil r_2 \rceil) - a(\lfloor r_2 \rfloor) - v, v) \tag{2.2}$$

denotes the down-up riverbend.

2.5 Reduction operator and quadratic progression

In this section, we show how the reduction operator ρ relates to the quadratic progression $a(t)$ of an infinity-gon.

Corollary 2.5.1. *Let (u, h, v) be a reduced form with discriminant $\Delta > 0$ and non-square. Let R be the associated oriented riverbend. Then $\rho(u, h, v)$ is the next riverbend $\rho(R)$.*

Proof. We have two cases, depending on the type of riverbend we start with.

Case 1: R is an up-down riverbend.

In this case, we have that $v < 0$ (Figure 2.2). Then

$$\rho(u, h, v) = (v, -h + n(2v), n^2 v - nh + u) \tag{2.3}$$

with

$$n = -\left\lfloor \frac{-(\sqrt{\Delta} + h)}{2v} \right\rfloor$$

Since R is an up-down riverbend, $\rho(R)$ will be a down-up riverbend. So, we use (2.2). We first take the opposite of the associate:

$$(v, v + a(\lfloor r_2 \rfloor) - a(\lceil r_2 \rceil), a(\lfloor r_2 \rfloor))$$

Evaluating and simplifying:

$$(v, -h + (-\lfloor r_2 \rfloor)2v, \lfloor r_2 \rfloor^2 v + \lfloor r_2 \rfloor h + u) \tag{2.4}$$

Now, $a(t) = vt^2 + ht + u$ with roots $r_1 < 0 < r_2$. As $h > 0$ and $v < 0$, we must have

$$r_2 = \frac{-(\sqrt{\Delta} + h)}{2v}$$

Then $\lfloor r_2 \rfloor = -n$. Substituting into (2.4), we have:

$$(v, -h + (n)2v, n^2 v - nh + u)$$

matching the reduction operation in (2.3).

Case 2: R is a down-up riverbend.

This case is analogous, with some extra steps. Using Figure 2.2, we now have $v > 0$. Applying the reduction operator ρ, we still get (2.3), but with

$$n = \left\lfloor \frac{\sqrt{\Delta} + h}{2v} \right\rfloor$$

As $\rho(R)$ is an up-down riverbend, we use (2.1). Taking the opposite of the associate and simplifying:

$$(v, -h + (-\lceil r_1 \rceil)2v, \lceil r_1 \rceil^2 v + \lceil r_1 \rceil h + u) \tag{2.5}$$

with

$$r_1 = \frac{-(\sqrt{\Delta} + h)}{2v}$$

Note that since $v > 0$ and $h > 0$, we indeed have $r_1 < 0$.

Then,

$$\lceil r_1 \rceil = \left\lceil \frac{-(\sqrt{\Delta} + h)}{2v} \right\rceil$$

We use the fact that for $x \in \mathbb{R}$, $\lceil -x \rceil = -\lfloor x \rfloor$. So,

$$\lceil r_1 \rceil = -\lfloor -r_1 \rfloor = -\left\lfloor \frac{\sqrt{\Delta} + h}{2v} \right\rfloor = -n$$

Substituting in (2.5), we have

$$(v, -h + (n)2v, n^2 v - nh + u)$$

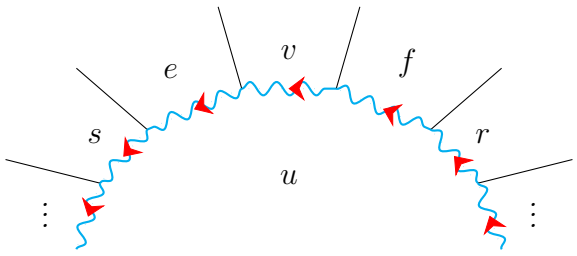
Once again, that matches (2.3). □

Thus, in the description of SQUFOF (assuming the same starting form), we can switch the reduction operator ρ with the quadratic progression $a(t)$ and the behavior of the algorithm would be the same.

2.6 The inverse reduction operator

We now make a similar relation using the inverse reduction operator ρ^{-1}. The idea is that if we switch the positions of u and v, then the infinity-gon would now have fixed region labeled u. That is, as we travel along the river, we will be traveling against the direction of the edge weight.

Corollary 2.6.1. *Keep the assumptions of Theorem 2.4.1. Furthermore, assume that the infinity-gon is oriented as below:*



Then $t = \lfloor r_2 \rfloor$ locates the up-down riverbend and $t = \lceil r_1 \rceil$ locates the down-up riverbend.

Remark. The proof is analogous to Corollary 2.4.2. In this case, the quadratic progression is given by $a(t) = ut^2 + ht + v$, with the roots still being $r_1 < 0 < r_2$.

Using this corollary, we can now describe the up-down riverbend as

$$(u, -u - a(\lfloor r_2 \rfloor) + a(\lceil r_2 \rceil), a(\lfloor r_2 \rfloor)) \tag{2.6}$$

and the down-up riverbend as

$$(u, u - a(\lfloor r_1 \rfloor) + a(\lceil r_1 \rceil), a(\lceil r_1 \rceil)) \tag{2.7}$$

This leads us to an analogous statement of Corollary 2.5.1.

Corollary 2.6.2. *Let (u, h, v) be a reduced form with discriminant $\Delta > 0$ and non-square. Let R be the associated oriented riverbend. Then $\rho^{-1}(u, h, v)$ is the previous riverbend $\rho^{-1}(R)$.*

Remark. The proof is similar as before. In this case, we use the definition of the inverse reduction operator ρ^{-1} and take the opposite of the associate of (2.6) and of (2.7).

So, on the topograph, the reduction operation moves in the same direction as the edge weight, and the inverse reduction operation moves in the reverse direction of the edge weight. That is, given an oriented riverbend R, we use the reduction operator to get to the next riverbend $\rho(R)$ and the inverse reduction operator to get to the previous riverbend $\rho^{-1}(R)$. Hence, the overloaded use of notation.

2.7 An example

In this section, we give an example of SQUFOF factoring. We show the steps using the [GW08] description, and then illustrate them on the topograph.

Let $N = 11111 \equiv 3 \bmod 4$. So, the discriminant $\Delta = 4N$. Denote the form with (a, b, c). We have:

1. **Initialize:** $(1, 210, -86)$

2. **Cycle Forward:**

   $(-86, 134, 77)$

   $(77, 174, -46)$

   $(-46, 194, 37)$

   $(37, 176, -91)$

   $(-91, 188, 25) = (-91, 188, 5^2)$

3. **Inverse square root:** $(-91 \cdot -5, -188, -5) = (455, -188, -5)$

4. **Cycle Backward:**

   $(-5, 208, 59)$

   $(59, 146, -98)$

   $(-98, 50, 107)$

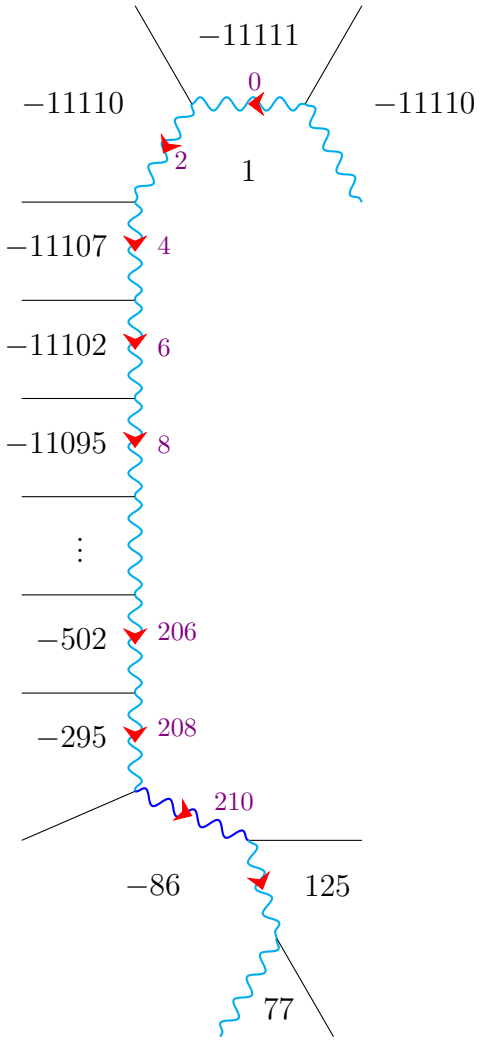
   $(107, 164, -41)$

   $(-41, 164, 107)$

5. **Output factor of N:** Since the last two forms in Step 4 both have $b = 164$, we take $|c| = 41$ of the second to last form. Thus, $N = 41 \cdot 271$.

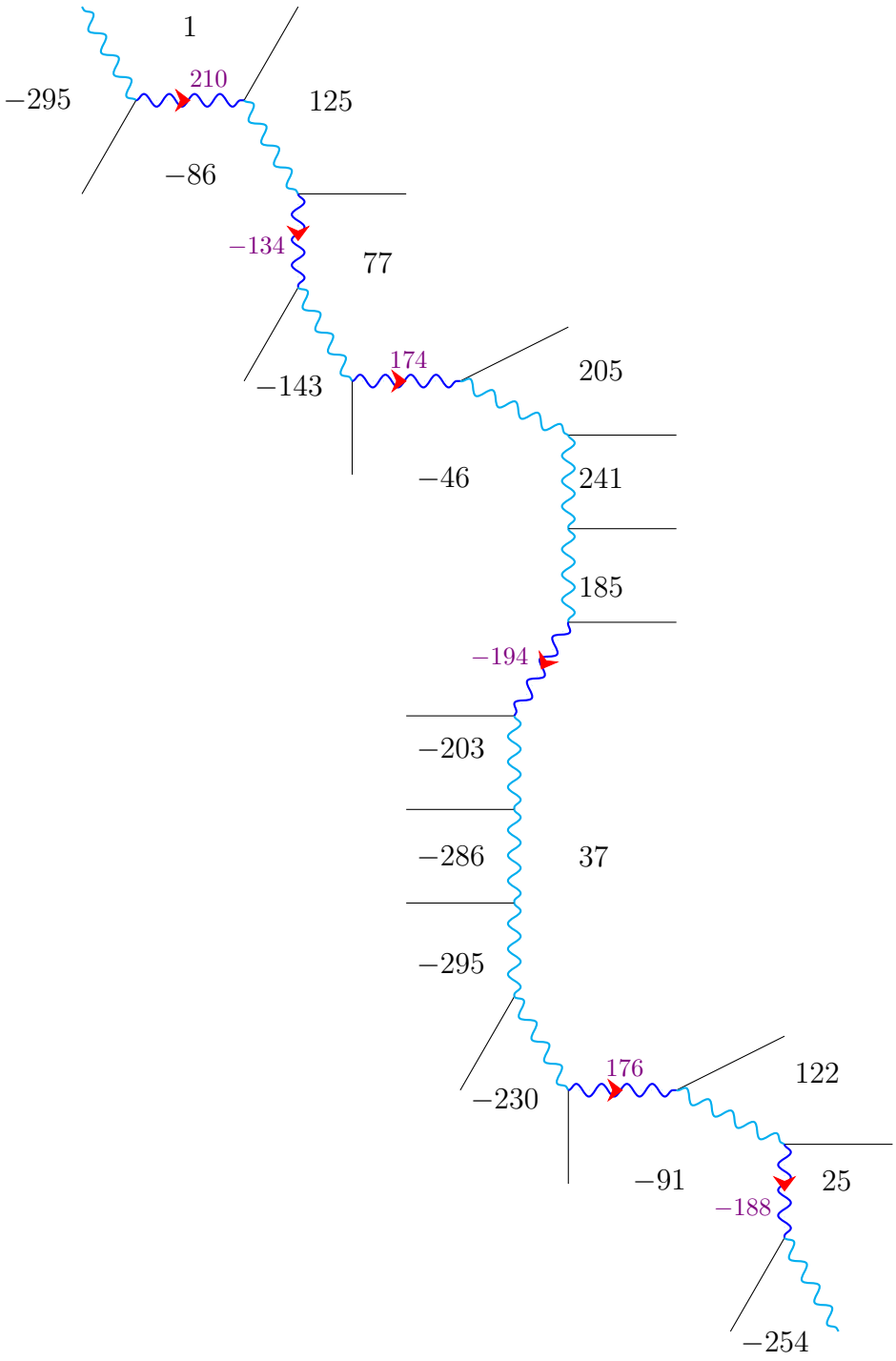
In the illustration that follows, we note that riverbends can have negative edge weights. However, the algorithm uses the opposite of the associate in those cases. For example, the first reduced form in Step 2 is $(-86, 134, 77)$, which will appear on the topograph as the riverbend $(77, -134, -86)$.

On the topograph, we start at home basis of $Q_1(x, y) = -11111x^2 + y^2$ and proceed to find the nearest riverbend. Since we are starting at an ambiguous river segment, traveling left or right is the same. Also note the edge weights illustrating the acceleration of 2 at this infinity-gon:



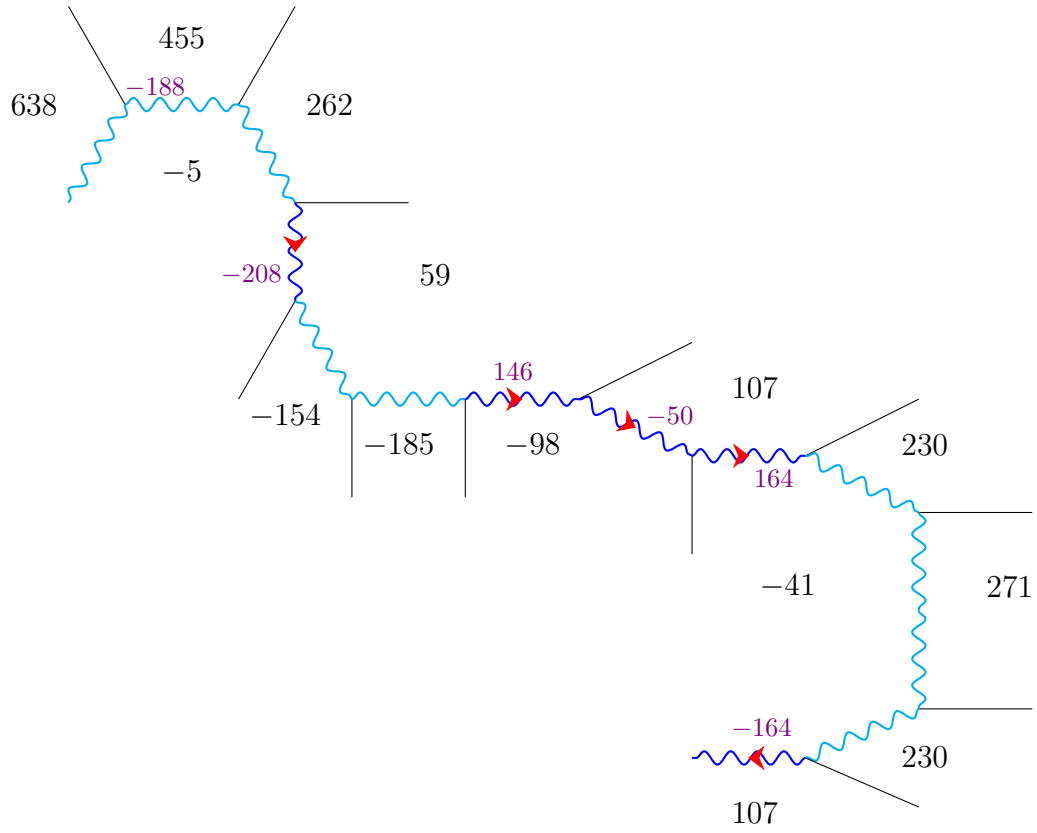
(a) Finding nearest riverbend

After finding the nearest riverbend, $(1, 210, -86)$, we proceed to find a square form (cells with edge weight labeled are riverbends):



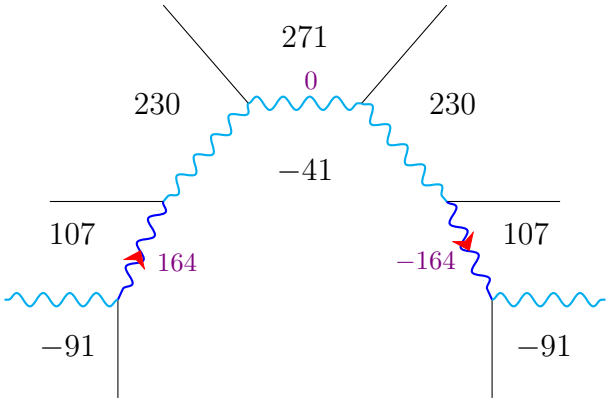
(b) Cycling Forward

Taking the inverse square root of the square form $(-91, 188, 25)$, we now cycle backward starting at $(455, -188, -5)$:



(c) Cycling Backward

We have now arrived at the ambiguous river segment $(271, 0, -41)$, which is the home basis for the ambiguous form $Q_2(x, y) = 271x^2 - 41y^2$. Taking a closer look:



(d) Output factor of N

Figure 2.4: SQUFOF on the topograph

We see in this case that we are at a Type H ambiguous river segment (Figure 2.1a). Furthermore, the last two riverbends were $(107, 164, -41)$ and $(-41, 164, 107)$. This illustrates the end condition $b' = b$ for the algorithm, which is due to the reflection symmetry at $(271, 0, -41)$. Outputting $|c| = 41$, we once again have $N = 41 \cdot 271$.

Chapter 3

Dilinear Topograph

We now introduce a variation of Conway's topograph. Instead of taking vectors $\vec{v} \in \mathbb{Z}^2$, we take vectors $\vec{v} \in \mathbb{Z}[\sqrt{2}]^2$. These, along with further details on the construction of the dilinear topograph and more general results can be found in [MSW19].

3.1 Dilinear topograph properties

In this section, we illustrate how the structure of the dilinear topograph differs from the regular topograph. We then show how many of the topograph properties have analogues in the dilinear case.

We begin with the vectors. We first define two subsets of $\mathbb{Z}[\sqrt{2}]^2$, referring to them by different types of colors. Let $D_{\text{blue}} = \{(u\sqrt{2}, v) \in \mathbb{Z}[\sqrt{2}]^2 : u, v \in \mathbb{Z}\}$ and $D_{\text{red}} = \{(u, v\sqrt{2}) \in \mathbb{Z}[\sqrt{2}]^2 : u, v \in \mathbb{Z}\}$.

Definition 3.1.1. A vector $\vec{d} \in D = D_{\text{blue}} \cup D_{\text{red}}$ is called a **dilinear vector**, or **divector** for short. If $\vec{d} \in D_{\text{blue}}$, then $\vec{d}$ is a **blue divector**. If $\vec{d} \in D_{\text{red}}$, then $\vec{d}$ is a **red divector**.

Definition 3.1.2. A red divector $(u, v\sqrt{2})$ is called **primitive** if $\gcd(u, 2v) = 1$. Similarly, a blue divector $(u\sqrt{2}, v)$ is called **primitive** if $\gcd(2u, v) = 1$.

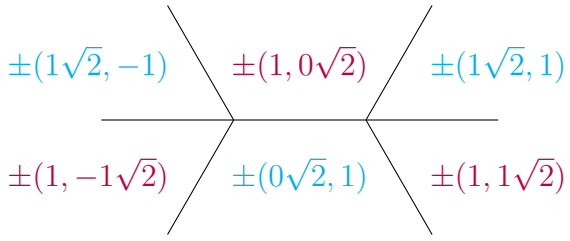
Definition 3.1.3. A **binary quadratic diform** is a function $Q : D \to \mathbb{Z}$ of the form $Q(x, y) = ax^2 + b\sqrt{2}xy + cy^2$, for some coefficients $a, b, c \in \mathbb{Z}$. The **discriminant** of Q is $\Delta = 2(2b^2 - 4ac)$.

Definite and **indefinite** diforms are defined analogously. We note that a diform still (and only) represents integers. Furthermore, $Q = (a, b, c)$ will also be used to denote a binary quadratic diform, with the $\sqrt{2}$ is omitted in the middle term.

Now, a **lax divector** is analogous to a lax vector and a **lax dibasis** is analogous to a lax basis. Note that given any lax dibasis $\{\pm d_1, \pm d_2\}$, $\pm d_1$ and $\pm d_2$ must be different colors. The next definition gives the analogue to a superbasis:

Definition 3.1.4 (Pinwheel)**.** ([MSW19], *pg. 445*) Let $\pm d_1, \pm d_3$ be blue divectors and $\pm d_2, \pm d_4$ be red divectors. A **pinwheel** is an ordered tuple $(\pm d_1, \pm d_2, \pm d_3, \pm d_4)$ such that any two distinct divectors $\{\pm d_i, \pm d_j\}$ forms a dibasis whenever $\pm d_i, \pm d_j$ has different colors.

Construction of the (domain) dilinear topograph follows from the construction of the regular (domain) topograph. The cell containing home basis now looks like:



Let $Q(x, y) = ax^2 + b\sqrt{2}xy + cy^2$ be a diform. If we restrict Q to either D_{red} or D_{blue}, we get back a binary quadratic form:

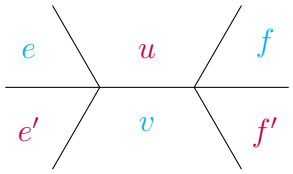
$$Q_{\text{red}}(u, v) := Q(u, v\sqrt{2}) = au^2 + 2buv + 2cv^2$$

$$Q_{\text{blue}}(u, v) := Q(u\sqrt{2}, v) = 2au^2 + 2buv + cv^2$$

Thus, a dilinear topograph can be considered as two regular topographs combined with each other, where regions of the same color belong to the same topograph (see [MSW19, *pg.445*]).

As with the regular topograph, we get the range dilinear topograph by labeling each region with the values instead of the divectors. We will be referring to the range dilinear topograph below.

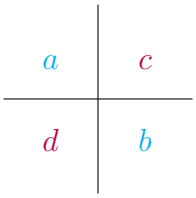
Definition 3.1.5. Let



be a cell in the dilinear topograph of Q. Then the **discriminant** is given by $(2u - v)^2 - ef$.

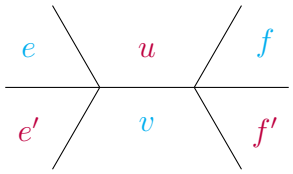
At a vertex (pinwheel) of the dilinear topograph, we have the following property:

Proposition 3.1.6. *Let*



be a vertex in the dilinear topograph. Then we have $a + b = c + d$.

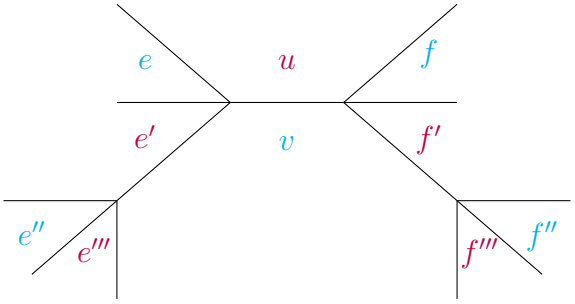
Proposition 3.1.7 (Arithmetic progression rule)**.** *Let*



be a cell of the dilinear topograph. Then the sequence $e, 2u + v, f$ *and the sequence* $e', u+2v, f'$*, both form an arithmetic progression with the same common difference.*

We will also denote this common difference with h, and label the edge with this number. Now, using the two arithmetic progressions, we show the two quadratic progressions around an infinity-gon on the dilinear topograph.

Proposition 3.1.8. *Let*



be an infinity-gon on the dilinear topograph with fixed region labeled v*. Suppose* v *is blue (resp. red). Consider the numbers around this infinity-gon. The red (resp. blue) numbers form a quadratic progression with acceleration* $4v$ *and the blue (resp. red) numbers form a quadratic progression with acceleration* $8v$.

Proof. The proof will be analogous to the proof of Proposition 1.3.12 given in [Wei17]. Without loss of generality, assume v is blue as above in the diagram. Consider the sequence of red numbers:

$$e''', e', u, f', f'''$$

Now, consider the sequence of their differences:

$$e' - e''', u - e', f' - u, f''' - f'$$

Without loss of generality, consider the difference between $u - e'$ and $f' - u$,

$$(f' - u) - (u - e') = f' + e' - 2u$$

But by the red arithmetic progression at the cell $(u, *, v)$,

$$\begin{aligned} f' - (u + 2v) &= (u + 2v) - e' \\ f' + e' &= 2(u + 2v) \\ f' + e' - 2u &= 4v \end{aligned}$$

Similarly, now consider the sequence of blue numbers:

$$e'', e, f, f''$$

Their sequence of differences is:

$$e - e'', f - e, f'' - f$$

Without loss of generality, consider the difference between $e - e''$ and $f - e$,

$$(f - e) - (e - e'') = f + e'' - 2e$$

We use the blue quadratic progression at the cell $(e', *, v)$ and $(u, *, v)$ to get

$$e - (2e' + v) = (2e' + v) - e''$$
$$e + e'' = 4e' + 2v$$

and

$$f - (2u + v) = (2u + v) - e$$
$$f + e = 4u + 2v$$

respectively. Adding the two equations, we have

$$f + e'' + 2e = 4(u + e') + 4v$$
$$f + e'' - 2e = 4(u + e') + 4v - 4e$$
$$f + e'' - 2e = 4(e + v) + 4v - 4e, \text{ by Prop. 3.1.6}$$
$$f + e'' - 2e = 8v$$

Note that in this case, we used the vertex relation $e + v = e' + u$. □

Consider an infinity-gon as in the previous proposition. Suppose v is blue. Pick the cell (u, h, v), where h is the edge weight between u and v. Then $a_{\text{red}}(t) = 2vt^2 + ht + u$ describes the red quadratic progression, indexing the red numbers around the infinity-gon. Similarly, $a_{\text{blue}}(t) = v(2t-1)^2 + h(2t-1) + 2u$ describes the blue quadratic progression.

3.2 Dilinear topograph riverbends

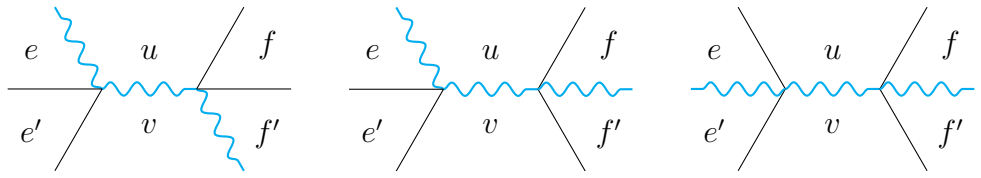
In this section, we take a closer look at the dilinear topograph of an indefinite diform. We illustrate the different possible riverbends.

The **river** is defined analogously on the dilinear topograph of an indefinite diform. In the case with discriminant non-square, we have the same property.

Proposition 3.2.1 ([MSW19], *pg.447*)**.** *Let Q be an indefinite binary quadratic diform with discriminant Δ non-square. Then the dilinear topograph of Q has a river. It is unique, endless, and non-branching.*

We now describe the riverbends on the dilinear topograph.

Definition 3.2.2. On the dilinear topograph, **riverbends** are cells consisting of three river segments as below:



(a) Sharp (b) Shallow (c) Thru

Figure 3.1: Types of dilinear topograph riverbends

Note that the riverbends above are the possible riverbends on the dilinear topograph up to symmetry. That is, we also have riverbends that are reflections and rotations of those above.

3.3 Conclusion and further directions

Given the many similarities between Conway's topograph and the dilinear topograph, one can also consider SQUFOF on the latter. We start out the same: if $N = pq$ is a factorization of N, then the indefinite binary quadratic *diforms* $x^2 - Ny^2$ and $px^2 - qy^2$ have the same discriminant. Note that in the dilinear case, the discriminant is always $\Delta = 2(4N) = 8N$.

Thus, we use diforms to factor integers instead of binary quadratic forms. We proceed through the rest of the steps of SQUFOF analogously. The main difference will be using the dilinear quadratic progression instead. Several possible issues arise.

The first is the presence of two different quadratic progressions on the dilinear topograph. Although it would appear that both will locate the same riverbends at a given infinity-gon, the behavior of algorithm may differ, i.e., the number of steps taken to find the riverbends.

A larger issue is the wider variety of riverbends in the dilinear case, in particular, encountering a thru riverbend. The description of SQUFOF on the topograph relies on the use of the quadratic progression around an infinity-gon. However, at a thru riverbend, one may not have a viable quadratic progression to use. That is, the quadratic progression might have roots that are too close to locate the riverbends. Lastly, it remains unknown whether an implementation of SQUFOF using diforms will run faster or more efficiently.

Bibliography

[Bue89] Duncan A. Buell. *Binary quadratic forms*. Classical theory and modern computations. Springer-Verlag, New York, 1989, pp. x+247. ISBN: 0-387-97037-1. DOI: 10.1007/978-1-4612-4542-1. URL: https://doi.org/10.1007/978-1-4612-4542-1.

[Con97] John H. Conway. *The Sensual (Quadratic) Form*. Vol. 26. Carus Mathematical Monographs. With the assistance of Francis Y. C. Fung. Mathematical Association of America, Washington, DC, 1997, pp. xiv+152. ISBN: 0-88385-030-3.

[GW08] Jason E. Gower and Samuel S. Wagstaff Jr. "Square form factorization". In: *Math. Comp.* 77.261 (2008), pp. 551–588. ISSN: 0025-5718. DOI: 10.1090/S0025-5718-07-02010-8. URL: https://doi.org/10.1090/S0025-5718-07-02010-8.

[MSW19] Suzana Milea, Christopher D. Shelley, and Martin H. Weissman. "Arithmetic of arithmetic Coxeter groups". In: *Proc. Natl. Acad. Sci. USA* 116.2 (2019), pp. 442–449. ISSN: 0027-8424. DOI: 10.1073/pnas.1809537115. URL: https://doi.org/10.1073/pnas.1809537115.

[Wei17] Martin H. Weissman. *An Illustrated Theory of Numbers*. American Mathematical Society, Providence, RI, 2017, pp. xv+323. ISBN: 978-1-4704-3493-9.