Optimal exponent for some problems in Diophantine Approximation

Benoît Arbour

Department of Mathematics and Statistics,
McGill University, Montréal
Québec, Canada

June, 2003

A thesis submitted to the Faculty of Graduate Studies and Research
in partial fulfillment of the requirements of the degree of
Master of Science

Acknowledgments

First of all, I would like to thank my supervisors; Damien Roy at the University of Ottawa, for all the help and support he gave me over the last two years. The long distance relationship we had to deal with could, at times, complicate my study of Diophantine Approxmation, but overall, he was always there to help me and would always free his schedule for a full day when I went to Ottawa to visit him. Also, his love of the subject and willingness to introduce me to it is something I will never forget. At McGill, I would like to thank Dimitry Jakobson, for being there when I had some problems, and obviously, for his overall support.

I also want to thank McGill University and in particular, the Mathematics and Statistics Department and its professors who taught me over the years: I gained valuable knowledge from them in number theory and other branches of mathematics.

On a personal note, I would like to thank my parents for the help and support they offered at all stages of my school career. I would never have got this far without them. I also have to thank my friends, who kept me distracted long enough so that I don't go crazy with mathematics, and obviously, Deidre, who let me (sometimes) work at night and on weekends.

Abstract

An important aspect of Diophantine Approximation deals with the problem of approximating real or complex numbers by rational numbers or, more generally, by algebraic numbers of bounded degree. This study provides criteria to decide whether a given real or complex number is algebraic or transcendental. In this thesis we present several such results. Following Davenport & Schmidt we look at the approximation of a real number by rational numbers, by quadratic irrational numbers and by algebraic integers of degree at most 3. We also look at the related problem of simultaneous approximation of a real number and its square by rational numbers with the same denominator. We conclude with a new Gel'fond type criterion in degree 2 and show that it involves an optimal exponent of approximation.

Résumé

Un aspect important de l'Approximation Diophantienne concerne le problème d'approximer un nombre réel ou complexe par des nombres rationnels ou, de manière plus générale, par des nombres algébriques de degré borné. L'étude de ces problèmes fournit des critères pour décider si un nombre réel ou complexe donné est algébrique ou transcendant. Dans ce mémoire, on présente quelques résultats sur le sujet. En suivant Davenport & Schmidt, on considère l'approximation d'un nombre réel par des nombres rationnels, par des nombres irrationnels quadratiques et par des entiers algébriques de degré au plus 3. On étudie aussi le problème connexe de l'approximation simultanée d'un nombre réel et de son carré par des nombres rationnels de même dénominateur. Enfin, on démontre un nouveau critère de type Gel'fond en degré 2 avec un exposant d'approximation optimal.

Table of Contents

Introduction

A complex number satisfying an irreducible integral polynomial of degree d is called *algebraic* of degree d. If a complex number is not algebraic of any degree, it is called *transcendental.* The *height* of an algebraic number is the maximum absolute value of the coefficients of its irreducible polynomial. It is usually a hard problem to decide whether a given real or complex number is algebraic, and if so, to bound its degree. Some sophisticated tools have been devised to examine these problems.

It is known at least since Euler that a real number ξ which is not rational can be approximated by infinitely many rational numbers p/q satisfying

$$\left|\xi - \frac{p}{q}\right| \leq \frac{1}{q^2}. \tag{1}$$

This result can be used as a criterion for irrationality since, for a rational number α, there exists a constant $c_0 > 0$ such that for all rational numbers $p/q \neq \alpha$ we have $|\alpha - p/q| \geq c_0/q$. Since rational numbers are algebraic numbers of degree 1, this is a very basic criterion to decide for algebraicity. Moreover, the exponent 2 in (1) cannot be replaced by $2+\epsilon$ for any $\epsilon > 0$, since for a quadratic irrational number ξ, there exists a constant $c_1 > 0$ such that $|\xi - p/q| \geq c_1 q^{-2}$ for all rationals p/q. Thus, we say that 2 is the *optimal exponent* of approximation of an irrational number by rational numbers.

It is also possible to express the above result in terms of height, by saying that for an irrational number ξ, there exists a constant $c_2 = c_2(\xi) > 0$ such that ξ admits infinitely many rational approximations α with $|\xi - \alpha| \leq c_2 H(\alpha)^{-2}$. This estimate has again an optimal exponent, since it is possible to find irrational real numbers ξ for which there exists only finitely many solutions $\alpha \in \mathbb{Q}$ to $|\xi - \alpha| \leq H(\alpha)^{-2-\epsilon}$ for every $\epsilon > 0$.

The next step is to look at algebraic numbers of arbitrary degree d. In 1961, Wirsing proved that if ξ is a real number not algebraic of degree at most d, then, for any $\epsilon > 0$, there exists infinitely many algebraic numbers α of degree at most d such that $|\xi - \alpha| \leq H(\alpha)^{-(d+3)/2+\epsilon}$. Wirsing also pondered if the statement would remain true if the exponent $(d+3)/2$ was replaced by $d+1$. In the case $d = 1$, this follows from the above mentionned result of approximation by rational numbers, and hence the answer to Wirsing's question is affirmative. In 1967, this question was answered positively in the case $d = 2$ by Davenport & Schmidt. Schmidt also conjectured the question to be true for all d. This conjecture is still open for $d \geq 3$.

In fact, Davenport & Schmidt showed that if $\xi \in \mathbb{R}$ is not algebraic of degree at most 2, then there exists infinitely many algebraic numbers α of degree at most 2 satisfying $|\xi - \alpha| \leq c_3 H(\alpha)^{-3}$ for a constant $c_3 > 0$. This estimate has the optimal exponent 3. They also established in 1969 that for a real number ξ which is not algebraic of degree at most 2, there exist infinitely many pairs $(m/q, n/q) \in \mathbb{Q}^2$ with $q > 0$ such that $|\xi - m/q| \leq c_4 q^{-\gamma}$ and $|\xi^2 - n/q| \leq c_4 q^{-\gamma}$ where $c_4 > 0$ is a constant and $\gamma = (1+\sqrt{5})/2$ denotes the golden number.

Davenport & Schmidt also showed a connection between the approximation by algebraic integers of degree at most $d+1$ of a real number ξ not algebraic of degree at most d, and the simultaneous approximation of the first d powers of ξ by rational numbers with the same denominator. In particular, they also proved in 1969 that if ξ is a real number which is not algebraic of degree at most 2, then there exists infinitely algebraic integers α of degree at most 3 satisfying $0 < |\xi - \alpha| \leq c_5 H(\alpha)^{-1-\gamma}$ for a constant $c_5 > 0$.

In a paper to appear, Roy [17] proves that the optimal exponent for approximating a real number ξ, not algebraic of degree at most 2, and its square ξ^2 by rational numbers with the same denominator is in fact $1/\gamma = 0.618\ldots$. He demonstrates the optimality of this exponent by constructing real numbers which attain the above mentionned exponent. Examples of such numbers are the real numbers $\xi_{a,b}$ whose continued fraction expansion is the Fibonacci word on two letters.

The results mentionned above pertain to the approximation of a real number, but they can also be used to determine if a given real number is algebraic of bounded degree. However, there exist other methods to determine if a real number ξ is algebraic of bounded degree. For example, Gel'fond, in 1960, developped a criterion to determine if a real number ξ is algebraic by bounding the value of integral polynomials at the point ξ. Jointly with Roy, the author developped a new version of a Gel'fond's type criterion in degree 2 with an optimal approximation exponent: given a real number ξ, if for every large real number $X > 0$ there exists a non-zero integral polynomial of degree at most 2 and height at most X satisfying $|P(\xi)| \leq (1/4)X^{-\gamma^2}$, then ξ is algebraic of degree at most 2. Surprinsingly, the continued fractions $\xi_{a,b}$ constructed by Roy also attain the optimal exponent in this criterion.

The following pages examine in details the results stated above (except for the results of Wirsing and Roy.) The proofs presented below will use a technique, similar to the one of Davenport & Schmidt, [8] and [9], and hence some preliminary results are needed before being able to jump in the heart of the matter. The exposition of the material will be as follows: Chapter 1 contains results about the Geometry of Numbers, polynomials, determinants and resultants. In Chapter 2 is constructed a sequence of polynomials which will be used in Chapter 3 to prove the criteria. Finally, Chapter 4 deals with the optimality of the approximation exponents.

Chapter 1

Preliminaries

1.1 Introduction

This chapter contains results about Geometry of Numbers, determinants, resultants and polynomials. A slight modification of the technique of Davenport & Schmidt, [8] and [9], is used to prove the main theorems, hence it is necessary to start from the ground and build up the tools that will ultimately be needed in the remainder of this text.

Definition 1.1.

1. We say that $\alpha \in \mathbb{C}$ is *algebraic* if it satisfies a polynomial relation

$$P_\alpha(\alpha) = a_d\alpha^d + a_{d-1}\alpha^{d-1} + \cdots + a_0 = 0$$

where $a_d \neq 0$ and $P_\alpha(T) \in \mathbb{Z}[T]$ is irreducible.

2. The polynomial $P_\alpha(T)$ is unique, up to sign, and is called the *minimal polynomial of α.*

3. The *degree* of an algebraic number α is

$$\deg(\alpha) = [\mathbb{Q}(\alpha) : \mathbb{Q}] = d,$$

where d is the degree of its minimal polynomial.

4. We say that a number $\alpha \in \mathbb{C}$ is *transcendental* if it is not algebraic of any degree. In this case, we denote

$$\deg(\alpha) = [\mathbb{Q}(\alpha) : \mathbb{Q}] = \infty.$$

Definition 1.2. Let $P(T) = a_d T^d + a_{d-1} T^{d-1} + \cdots + a_0 \in \mathbb{C}[T]$.

1. The *height* of $P(T)$ is

$$H(P) = \max_{i=0,\ldots,d} \{|a_i|\}.$$

2. The *height* of an algebraic number $\alpha \in \mathbb{C}$ is the height of its minimal polynomial in $\mathbb{Z}[T]$. (See Definition 1.1.)

In addition, it will ease the flow of the text to use the following notations.

Notation 1.3.

1. Let $\xi \in \mathbb{R}$. Then $[\xi]$ denotes the integer part of ξ, and $\{\xi\}$ denotes the fractional part of ξ.

2. If R is a ring, we denote the set of polynomials of degree less or equal to d in $R[T]$ by $R[T]_{\leq d}$.

3. Let A be a square matrix. Then

$$||A|| := |\det(A)|.$$

1.2 Geometry of Numbers

The Geometry of Numbers is a far-reaching theory due to Hermann Minkowski. It consists of the study of n-dimensional figures in Euclidean space along with their connection to number theory. In this section, a brief introduction to the Geometry of Numbers is given, and we prove the existence of integral polynomials with small absolute value at a given point. For more information, see [7].

1.2.1 Lattices and Minkowski's Lemma

We start with the study of lattices and convex bodies of $\mathbb{R}^n$.

Definition 1.4. A *lattice* Λ of $\mathbb{R}^n$ is a subgroup of $\mathbb{R}^n$ generated by n linearly independent vectors. The determinant of a lattice Λ is the absolute value of the determinant of its underlying basis and is denoted by $\det(\Lambda)$.

Definition 1.5. Let $C \subset \mathbb{R}^n$.

1. We say that C is *symmetric about the origin* if $u \in C$ implies that $-u \in C$.
2. We say C is *convex* if $u_1, u_2 \in C$ implies that the line segment between u_1 and u_2 is completely contained in C.

This first lemma is very basic and concerns the determinant of a lattice.

Lemma 1.6. *Let $\Lambda \subset \mathbb{R}^n$ be a lattice and let $A \in \mathrm{GL}_n(\mathbb{R})$. Then $A\Lambda$ is a lattice and*

$$\det(A\Lambda) = ||A|| \det(\Lambda).$$

Given a convex body of $\mathbb{R}^n$, it is sometimes quite difficult to verify directly whether it contains a non-zero point of $\mathbb{Z}^n$. Replacing $\mathbb{Z}^n$ by an arbitrary lattice complicates things further. The following theorem is needed to answer these problems. We state the theorem in its most general form (due to Van der Corput), while the case $m = 1$ is due to Minkowski and is called Minkowski's Theorem on convex bodies. For a proof, see [7, Theorem II, p.71]

Theorem 1.7 (Minkowski-Van der Corput). *Let $C \in \mathbb{R}^n$ be a convex set, symmetric about the origin and of volume $V(C)$ (possibly infinite). Let $m \in \mathbb{Z}_{>0}$ and Λ be a lattice of $\mathbb{R}^n$. Suppose that one of the following two cases occur:*

- $V(C) > m2^n \det(\Lambda)$,
- $V(C) = m2^n \det(\Lambda)$ *and C is compact.*

Then C contains at least m pairs of non-zero lattice points $\pm u_i$ with $u_i \neq u_j$ for $i \neq j$.

Definition 1.8. We say that a set $C \subset \mathbb{R}^n$ is a *convex body* if it is compact, convex, symmetric about the origin and has non-empty interior.

As stated in the theorem, the number of lattice points in a convex body is dependent on the volume of the convex body. What can be said about these points? Minkowski proved another theorem, namely Minkowski's second Theorem on convex bodies, stating "how much bigger" a convex body must be in order to contain n linearly independent lattice points.

Definition 1.9. Let $C \subset \mathbb{R}^n$ be a convex body. Define the *first minimum of C*, $\lambda_1 = \lambda_1(C)$, to be the infimum over all $\lambda \in \mathbb{R}_{>0}$ for which λC contains a non-zero lattice point. Minkowski's Theorem clearly states that λ_1 is finite and provides an upper bound for it. For $2 \leq i \leq n$ let the *i-th minimum of C*, $\lambda_i = \lambda_i(C)$, to be the infimum over all $\lambda \in \mathbb{R}_{>0}$ for which λC contains i linearly independent lattice points. (This must also be finite since C has non-empty interior.) We get a sequence

$$0 < \lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n < \infty$$

and we call $\{\lambda_1, \lambda_2, \ldots, \lambda_n\}$ the *successive minima of C*.

Theorem 1.10 (Minkowski). *Let $C \subset \mathbb{R}^n$ be a convex body. Then*

$$\frac{2^n}{n!} \leq \lambda_1 \lambda_2 \ldots \lambda_n V(C) \leq 2^n.$$

Minkowski's theorems clearly show the importance of being able to evaluate the volume of a convex body.

Theorem 1.11. *Let $A \in \mathrm{GL}_n(\mathbb{R})$. Given n constants $c_1, \ldots, c_n \in \mathbb{R}$ satisfying $c_1 c_2 \ldots c_n > 0$, the convex body $\mathcal{C} \subset \mathbb{R}^n$ defined by*

$$\left| \sum_{j=1}^{n} a_{ij} x_j \right| \leq c_i \qquad (1 \leq i \leq n)$$

has volume

$$V(\mathcal{C}) = \frac{2^n c_1 \ldots c_n}{||A||}.$$

In particular, if $\Lambda \subset \mathbb{R}^n$ is a lattice satisfying

$$\det(\Lambda) \leq \frac{c_1 \ldots c_n}{||A||}$$

then $\mathcal{C}$ contains a non-zero point of Λ.

Proof. Define

$$X_i := \sum_{j=1}^{n} a_{ij} x_j \qquad (1 \leq i \leq n)$$

for $(x_1, \ldots, x_n) \in \Lambda$. Consider the convex body $\mathcal{D}$ defined by the equations

$$|X_i| \leq c_i \qquad (1 \leq i \leq n).$$

It is clear that $V(\mathcal{D}) = 2^n c_1 \ldots c_n$. Since $A\mathcal{C} = \mathcal{D}$ then

$$V(\mathcal{C}) = \frac{V(\mathcal{D})}{||A||}.$$

Thus if $\Lambda \subset \mathbb{R}^n$ is a lattice satisfying

$$\det(\Lambda) \leq \frac{c_1 \ldots c_n}{||A||}$$

then

$$V(\mathcal{C}) \geq 2^n \det(\Lambda).$$

Using Minkowski's Theorem, $\mathcal{C}$ contains a non-zero lattice point. □

Corollary 1.12. *Let $\xi \in \mathbb{C}$ and $\Lambda \subset \mathbb{R}^{n+1}$ be a lattice of determinant* 1*. For all $X \geq 1$ the convex body $\mathcal{C} \subset \mathbb{R}^{n+1}$ defined by*

$$\mathcal{C} := \begin{cases} |x_n\xi^n + x_{n-1}\xi^{n-1} + \cdots + x_0| \leq X^{-n}, \\ |x_i| \leq X \qquad (1 \leq i \leq n) \end{cases}$$

has volume $V(\mathcal{C}) = 2^{n+1}$. In particular $\mathcal{C}$ contains a non-zero lattice point.

Proof. Let $\mathbf{c} = (c_0, c_1, \ldots, c_n) = (X^{-n}, X, \ldots, X)$ and

$$A = (a_{ij}) = \begin{pmatrix} 1 & \xi & \xi^2 & \ldots & \xi^n \\ 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix}.$$

Then the convex body $\mathcal{C}$ can be rewritten as

$$\left|\sum_{j=0}^{n} a_{ij}x_j\right| \leq c_i \qquad (0 \leq i \leq n).$$

Using Theorem 1.11,

$$V(\mathcal{C}) = \frac{2^{n+1}c_0 \ldots c_n}{||A||} = 2^{n+1}$$

and since

$$1 = \det(\Lambda) = \frac{c_0 \ldots c_n}{||A||},$$

the convex body $\mathcal{C}$ contains a non-zero lattice point. □

Corollary 1.13. *Let $\xi \in \mathbb{R}$. For all real numbers $X > 1$ the convex body $\mathcal{C} \subset \mathbb{R}^{n+1}$ defined by*

$$\begin{cases} |a_0| \leq X, \\ |a_0\xi^i - a_i| \leq X^{-1/n} \qquad (1 \leq i \leq n) \end{cases}$$

contains a point $(a_0, a_1, \ldots, a_n) \in \mathbb{Z}^{n+1}$ with $a_0 \neq 0$.

Proof. Similarly to the proof of Corollary 1.12, we let $\mathbf{c} = (X, X^{-1/n}, \ldots, X^{-1/n})$ and

$$A = (a_{ij}) = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 \\ \xi & -1 & 0 & \ldots & 0 \\ \xi^2 & 0 & -1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \xi^n & 0 & 0 & \ldots & -1 \end{pmatrix}$$

to get, using Theorem 1.11, a non-zero integer point in $\mathcal{C}$. Clearly $|a_0| \geq 1$. Otherwise, if $a_0 = 0$, the integers a_i must satisfy $|a_0\xi^i - a_i| = |a_i| \leq X^{-1/n}$ which has the only solution $a_i = 0$ for all i. □

We now translate the question about lattice points in convex bodies into polynomials with small absolute value at a certain point. Notice that $\mathbb{Z}^n$ and $\mathbb{Z}[T]_{\leq n-1}$ are in $1-1$ correspondance under the isomorphism

$$(x_0, \ldots, x_{n-1}) \longleftrightarrow x_{n-1}T^{n-1} + x_{n-2}T^{n-2} + \ldots x_0.$$

Thus, Corollary 1.12 implies that for any $\xi \in \mathbb{C}$ and any $X \geq 1$, there exists a non-zero integral polynomial P of degree at most n satisfying

$$H(P) \leq (1 + |\xi| + \cdots + |\xi|^n)X, \qquad |P(\xi)| \leq X^{-n}.$$

The next Proposition, due to Davenport & Schmidt [8], refines Corollary 1.12 in the case $n = 2$ and $0 < \xi < 1$.

Proposition 1.14. *Let $\xi \in \mathbb{R}$ with $0 < \xi < 1$. For any sufficiently large real number X, there exists a non-zero polynomial $P(T) \in \mathbb{Z}[T]_{\leq 2}$ with*

$$H(P) \leq X \quad \text{and} \quad |P(\xi)| \leq \frac{4}{3}X^{-2}.$$

Proof. Let $\Lambda = \mathbb{Z}^n$. Consider the convex bodies $\mathcal{A}, \mathcal{B}$ and $\mathcal{C}$ defined by

$$\mathcal{A} := \{(x, y, z) \in \mathbb{R}^3 \,|\, |x| \leq X, |y| \leq X, |z| \leq X, |\xi^2 x + \xi y + z| \leq \frac{4}{3}X^{-2}\},$$

$$\mathcal{B} := \left\{(x,y,z) \in \mathbb{R}^3 \middle| |x| \leq X, |y| \leq X, |\xi^2 x + \xi y| \leq X - \frac{4}{3}X^{-2}, |\xi^2 x + \xi y + z| \leq \frac{4}{3}X^{-2}\right\},$$

$$\mathcal{C} := \left\{(x,y,z) \in \mathbb{R}^3 \middle| |x| \leq X, |y| \leq X, |x+y| \leq X, |\xi^2 x + \xi y + z| \leq \frac{4}{3}X^{-2}\right\}.$$

We show that $\mathcal{C} \subset \mathcal{B} \subset \mathcal{A}$ for sufficiently large X. Fix $(x,y,z) \in \mathcal{B}$. Then

$$\begin{aligned}
|z| \leq& |\xi^2 x + \xi y| + |\xi^2 x + \xi y + z| \\
\leq& (X - \frac{4}{3}X^{-2}) + \frac{4}{3}X^{-2} \\
=& X,
\end{aligned}$$

hence $(x,y,z) \in \mathcal{A}$ and $\mathcal{B} \subset \mathcal{A}$. Now let $(x',y',z') \in \mathcal{C}$. There are two cases:

1. x' and y' have the same sign. Then, for X large enough,

$$\begin{aligned}
|\xi^2 x' + \xi y'| =& \xi^2 |x'| + \xi |y'| \\
\leq& \xi |x' + y'| \\
\leq& \xi X \leq X - \frac{4}{3}X^{-2}.
\end{aligned}$$

2. x' and y' have different signs. We get, for X large enough, that

$$\begin{aligned}
|\xi^2 x' + \xi y'| \leq& \max\{\xi^2 |x'|, \xi |y|\} \\
<& \xi X < X - \frac{4}{3}X^{-2}.
\end{aligned}$$

In all cases $(x',y',z') \in \mathcal{B}$ and thus $\mathcal{C} \subset \mathcal{B}$. Since

$$\begin{aligned}
V(\mathcal{C}) =& \int\limits_{|x|<X} \int\limits_{\substack{|y|<X \\ |x+y|<X}} \int\limits_{|\xi^2 x + \xi y + z| < \frac{4}{3}X^{-2}} dz dy dx \\
=& \int\limits_{|x|<X} \int\limits_{\substack{|y|<X \\ |x+y|<X}} \frac{8}{3}X^{-2} dy dx \\
=& 3X^2 \cdot \frac{8}{3}X^{-2} \\
=& 8 = 2^3 \det(\Lambda),
\end{aligned}$$

we can apply Minkowski's Theorem to find out that the convex body $\mathcal{C}$ contains a non-zero integer point for X large enough. This point is also contained in the convex body $\mathcal{A}$, hence for any sufficiently large $X > 0$, there exists a non-zero integral polynomial $P(T)$ of degree at most 2 satisfying

$$H(P) \leq X \quad \text{and} \quad |P(\xi)| \leq \frac{4}{3}X^{-2}.$$

□

1.2.2 Polar bodies

We now consider another object of importance in the Geometry of Numbers: the polar body to a convex body. There exist very interesting relationships between a body and its polar body (with respect to volume and successive minima) which are examined here.

Definition 1.15.

1. Let $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ where $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$. We define

$$\mathbf{x} \cdot \mathbf{y} := x_1 y_1 + \cdots + x_n y_n.$$

2. Let $\mathcal{C} \subset \mathbb{R}^n$ be a convex body. We define the *polar body* $\mathcal{C}^*$ *of* $\mathcal{C}$ to be

$$\mathcal{C}^* := \{\mathbf{y} \in \mathbb{R}^n \big| |\mathbf{x} \cdot \mathbf{y}| \leq 1 \ \forall \ \mathbf{x} \in \mathcal{C}\}.$$

Remark 1.16. *One can show $\mathcal{C}^{**} = \mathcal{C}$. See [7, p.105].*

We start with the interplay between volumes. The following theorem is proved in [7, Theorem VI, p. 118].

Theorem 1.17. *Let $\mathcal{C}, \mathcal{C}^* \subset \mathbb{R}^n$ be mutually polar convex bodies. Then*

$$\frac{4^n}{(n!)^2} \leq V(\mathcal{C})V(\mathcal{C}^*) \leq 4^n.$$

The next theorem explores the successive minima of a body and its polar body. For a proof, see [7, Theorem VI, p.219].

Theorem 1.18 (Mahler). *Let $\mathcal{C}, \mathcal{C}^* \subset \mathbb{R}^n$ be mutually polar bodies. Let $\lambda_1, \ldots, \lambda_n$ and $\lambda_1^*, \ldots, \lambda_n^*$ be the successive minima of $\mathcal{C}$ and $\mathcal{C}^*$ respectively. Then*

$$1 \leq \lambda_j \lambda_{n+1-j}^* \leq n! \qquad (1 \leq j \leq n).$$

We now turn our attention to the calculation of polar bodies. This will be done after this quick definition.

Definition 1.19. We define the *sign* of a real number α to be

$$\operatorname{sgn}(\alpha) := \begin{cases} -1 & \text{if } \alpha < 0, \\ 0 & \text{if } \alpha = 0, \\ 1 & \text{if } \alpha > 0. \end{cases}$$

Proposition 1.20. *Let $\xi \in \mathbb{R}$ and $X, Y \in \mathbb{R}_{>0}$. Then the convex bodies $\mathcal{C}, \mathcal{D} \subset \mathbb{R}^n$ defined by*

$$\mathcal{C} := \begin{cases} |x_0| \leq X, \\ |x_0 \xi^i - x_i| \leq Y^{-1} \qquad (1 \leq i \leq n-1), \end{cases}$$

$$\mathcal{D} := \begin{cases} |y_{n-1}\xi^{n-1} + \cdots + y_1\xi + y_0| \leq X^{-1}, \\ |y_i| \leq Y \qquad (1 \leq i \leq n-1) \end{cases}$$

satisfy $\frac{1}{n}\mathcal{D} \subset \mathcal{C}^* \subset \mathcal{D}$.

Proof. First we note that

$$\begin{aligned} \mathbf{x} \cdot \mathbf{y} =& x_0 y_0 + \cdots + x_{n-1} y_{n-1} \\ =& x_0(y_0 + y_1\xi + \cdots + y_{n-1}\xi^{n-1}) + (x_1 - x_0\xi)y_1 + \cdots + (x_{n-1} - x_0\xi^{n-1})y_{n-1}. \end{aligned}$$

Thus, for $\mathbf{x} \in \mathcal{C}$ and $\mathbf{y} \in \mathcal{D}$ we get

$$|\mathbf{x} \cdot \mathbf{y}| \leq XX^{-1} + (n-1)Y^{-1}Y = n \tag{1.1}$$

which, by definition of the polar body, implies $\frac{1}{n}\mathcal{D} \subset \mathcal{C}^*$.

Conversely, let $\mathbf{y} \in \mathcal{C}^*$ and define

$$\tau = \operatorname{sgn}(y_{n-1}\xi^{n-1} + \cdots + y_1\xi + y_0), \qquad \tau_i = \operatorname{sgn}(y_i) \quad (1 \le i \le n-1).$$

Since the point

$$\mathbf{x} = (\tau X, \tau_1 Y^{-1} + \tau X\xi, \ldots, \tau_{n-1}Y^{-1} + \tau X\xi^{n-1})$$

belongs to $\mathcal{C}$, we necessarily have $|\mathbf{x} \cdot \mathbf{y}| \le 1$. However,

$$\mathbf{x} \cdot \mathbf{y} = X|y_{n-1}\xi^{n-1} + \cdots + y_0| + Y^{-1}(|y_1| + \cdots + |y_{n-1}|)$$

and thus $\mathbf{y} \in \mathcal{D}$. Hence, $\mathcal{C}^* \subset \mathcal{D}$, as the choice of $\mathbf{y} \in \mathcal{C}^*$ is arbitrary.

□

We conclude this section with a concrete example.

Example 1.21. *Let*

$$\mathcal{C} = \{(x_1, \ldots, x_n) \in \mathbb{R}^n \,\big|\, |x_i| \le 1 \ \forall\ i\}$$

be the generalized cube and

$$\mathcal{D} = \left\{ (y_1, \ldots, y_n) \in \mathbb{R}^n \,\Big|\, \sum_{i=1}^{n} |y_i| \le 1 \right\}$$

be the generalized octahedron. Then $\mathcal{C}$ and $\mathcal{D}$ are polar to each other.

1.3 Polynomials

In this section, we study some properties of polynomials. We need to introduce the Mahler measure of a polynomial and relate it to the height of polynomials. It will then be possible to bound the distance of a real number to the closest root of a given polynomial.

1.3.1 Gel'fond's Lemma

Gel'fond's lemma relates the product of the height of given polynomials to the height of their product. We present here the general result and prove optimal estimates in the case of two polynomials of degree at most 1. Before doing so, we introduce Mahler's measure and Jensen's formula for analytic functions.

Definition 1.22. Let $P(T) = a_0(T-\alpha_1)(T-\alpha_2)\dots(T-\alpha_n) \in \mathbb{C}[T]$. We define the *Mahler measure of P* to be

$$M(P) := \begin{cases} |a_0|\prod_{i=1}^{n}\max\{1,|\alpha_i|\} & \text{if} P \neq 0, \\ 0 & \text{if} P = 0. \end{cases}$$

It is clear from the definition that Mahler's measure is multiplicative, i.e., for any $P, Q \in \mathbb{C}[T]$ we have $M(PQ) = M(P)M(Q)$.

Lemma 1.23 (Jensen's Formula). *Let $f(x)$ be a complex function analytic in an open neighborhood of the disk $D = \{x \in \mathbb{C} | |x| \leq \rho\}$. Let $\xi_1, \xi_2, \dots \xi_n$ be the zeros of $f(x)$ in the interior of D. Then*

$$\frac{1}{2\pi}\int_0^{2\pi} \log|f(\rho e^{\theta i})|d\theta = \log|f(0)| + \sum_{i=1}^{n} \log\frac{\rho}{|\xi_i|}.$$

This last result is very important since Jensen's formula provides an analytic expression for the Mahler's measure. The next lemma fully illustrates this equivalence.

Lemma 1.24. *Let $P(T) = a_0(T-\alpha_1)(T-\alpha_2)\dots(T-\alpha_n) \in \mathbb{C}[T]$. Then*

$$|a_0|\prod_{i=1}^{n}\max\{1,|\alpha_i|\} = \exp\left(\int_0^1 \log|P(e^{2i\pi t})|dt\right).$$

Proof. Let $\rho = 1$ and define $\beta_i = 1/\alpha_i$. Let $f(z) = z^n P(1/z)$. On one hand, Jensen's

Formula gives

$$\begin{aligned}\int_0^1 \log|f(e^{2\pi i\theta})|d\theta &= \log|a_0| + \sum_{|\beta_i|<1} \log\left|\frac{1}{\beta_i}\right| \\ &= \log|a_0| + \sum_{|\alpha_i|>1} \log|\alpha_i| \\ &= \log\Big(|a_0| \prod_{|\alpha_i|>1} |\alpha_i|\Big) \\ &= \log\Big(|a_0| \prod_{i=1}^{n} \max\{1, |a_i|\}\Big).\end{aligned}$$

On the other hand, the change of variable $\theta \leftrightarrow -\theta$ gives

$$\begin{aligned}\int_0^1 \log|f(e^{2\pi i\theta})|d\theta &= -\int_0^{-1} \log|f(e^{-2\pi i\theta})|d\theta \\ &= -\int_0^{-1} \log|e^{-2n\pi i\theta}P(e^{2i\pi\theta})|d\theta \\ &= \int_0^1 \log|P(e^{2i\pi\theta})|d\theta.\end{aligned}$$

Thus,

$$\int_0^1 \log|P(e^{2i\pi\theta})|d\theta = \log\Big(|a_0| \prod_{i=1}^{n} \max\{1, |a_i|\}\Big).$$

□

The following theorem is a version of Gel'fond's lemma, proved following Mahler.

Lemma 1.25. *Let $P(T), Q(T) \in \mathbb{C}[T]$ be polynomials of degree m and n respectively. Then*

$$\frac{2^{-(m+n)}}{(m+n+1)} H(P)H(Q) \leq H(PQ) \leq (m+1)H(P)H(Q). \tag{1.2}$$

Proof. The upper bound is obvious as it is obtained by simple multiplication of the two polynomials and by using the height as an upper bound for the coefficients.

For the lower bound, we note that for $P \in \mathbb{C}[T]$ of degree m, the inequality

$$2^{-m}H(P) \leq M(P) \leq (m+1)H(P) \tag{1.3}$$

always holds. This must be so since, when P is expanded as $P = a_0 \prod_{i=1}^{m}(T - \alpha_i)$, the number of terms in the coefficient of T^j is $\binom{m}{j} \leq 2^m$. Moreover, each of these terms is bounded above by $M(P)$, giving us the inequality

$$H(P) \leq 2^m M(P). \tag{1.4}$$

Using Lemma 1.24,

$$\begin{aligned} M(P) =& \exp\left(\int_0^1 \log|P(e^{2\pi i t})|dt\right) \\ \leq& \exp\left(\int_0^1 \log\left((m+1)H(P)\right)dt\right) \\ =& \exp\left(\log\left((m+1)H(P)\right)\int_0^1 dt\right) \\ =&(m+1)H(P). \end{aligned} \tag{1.5}$$

Together, (1.4) and (1.5) give (1.3).

Coming back to the lower bound of (1.2), it follows from equation (1.3) that

$$2^{-m}H(P) \leq M(P), \qquad 2^{-n}H(Q) \leq M(Q), \qquad M(PQ) \leq (m+n+1)H(PQ)$$

while the multiplicity of $M(P)$ implies

$$2^{-m}H(P)2^{-n}H(Q) \leq M(P)M(Q) = M(PQ) \leq (m+n+1)H(PQ),$$

hence giving the desired lower bound. □

Notation 1.26. We denote the *Golden Ratio* by

$$\gamma := \frac{\sqrt{5}+1}{2}.$$

We can now prove the optimal Gel'fond lemma for two polynomials of degree at most 1.

Lemma 1.27. *Let $P(T), Q(T) \in \mathbb{C}[T]$ be polynomials of degree at most 1. Then*

$$\frac{1}{\gamma}H(P)H(Q) \le H(PQ) \le 2H(P)H(Q).$$

Moreover, both lower and upper bounds are optimal.

Proof. Write $P(T) = aT + b$ and $Q(T) = cT + d$. Then

$$H(PQ) = \max\{|ac|, |bc + ad|, |bd|\},$$
$$H(P)H(Q) = \max\{|a|, |b|\} \cdot \max\{|c|, |d|\} = \max\{|ac|, |ad|, |bc|, |bd|\}.$$

Starting with the upper bound, we note that

$$\begin{aligned} H(PQ) &\le \max\{|ac|, |bc| + |ad|, |bd|\} \\ &\le 2\max\{|ac|, |ad|, |bc|, |bd|\} \\ &= 2H(P)H(Q), \end{aligned}$$

giving us the desired result.

Clearly, if $H(P)H(Q) = |ac|$ or $|bd|$ then the lower bound is trivial. So assume, without loss of generality, that $H(P) = |a|$ and $H(Q) = |d|$ and hence, $H(P)H(Q) = |ad|$. We may also assume that $a = d = 1$, since dividing a polynomial by a constant does not affect the inequality. With the present assumptions, we want to show that

$$\frac{1}{\gamma} \le \max\{|b|, |c|, |bc + 1|\}.$$

If $|b| \ge 1/\gamma$ or $|c| \ge 1/\gamma$, we are done. So, we assume $|b|, |c| \le 1/\gamma$ leading us to the equation

$$|1 + bc| \ge 1 - |bc| \ge 1 - \frac{1}{\gamma^2} = \frac{1}{\gamma}$$

which completes the proof of the lower bound.

To show that the upper bound is optimal, we use the example $P(T) = T + 1 = Q(T)$. For the lower bound, we let $P(T) = \gamma T - 1$ and $Q(T) = T + \gamma$. □

Now that we have seen the relation between the height of a polynomial P and the height of the polynomials dividing P, it is interesting to look at the height of a root α of P. The case $\deg(P) = 1$ is trivial as $cH(\alpha) = H(P)$ where c is the gcd of the coefficients of P. In the case $\deg(P) = d \geq 2$, Lemma 1.25 states that $H(\alpha) \leq (d+1)2^d H(P)$. However, the case $d = 2$ can be refined as is shown in the next lemma.

Lemma 1.28. *Let $P(T) \in \mathbb{Z}[T]$ be of degree 2 and let α be a root of P. Then $H(\alpha) \leq H(P)$.*

Proof. This is clear if $\deg(\alpha) = 2$. Otherwise, for $mT - n$ the minimal polynomial of α, we get that m divides the leading coefficient of P and that n divides the constant coefficient of P. Thus $H(\alpha) = \max\{|m|, |n|\} \leq H(P)$. □

1.3.2 Distance to the closest root of a polynomial

Having studied the height of polynomials, it is now possible to bound the distance between a given real or complex number ξ and the closest root of a polynomial to ξ. Our study remains at a basic level.

Lemma 1.29. *Let $P(T) \in \mathbb{C}[T]$ be a polynomial of degree d. Let $\xi \in \mathbb{C}$ with $P'(\xi) \neq 0$. Then there exists a root α of P satisfying*

$$|\xi - \alpha| \leq d\frac{|P(\xi)|}{|P'(\xi)|}.$$

Proof. If $P(\xi) = 0$, the result is trivial. So assume that $P(\xi) \neq 0$ and write $P(T) = a_0(T - \alpha_1)\ldots(T - \alpha_d)$ with the roots ordered so that

$$|\xi - \alpha_1| \leq |\xi - \alpha_2| \leq \cdots \leq |\xi - \alpha_d|.$$

Applying logarithmic differentiation on the polynomial P gives

$$\frac{|P'(\xi)|}{|P(\xi)|} = \frac{1}{|\xi - \alpha_1|} + \cdots + \frac{1}{|\xi - \alpha_d|} \leq \frac{d}{|\xi - \alpha_1|}$$

and the lemma follows. □

Lemma 1.30. *Let $\xi \in \mathbb{R}$ with $[\mathbb{Q}(\xi) : \mathbb{Q}] > 2$ and let $0 < \epsilon < 1/3$. Any $P(T) \in \mathbb{Z}[T]$ of degree 2 with non-zero discriminant satisfying $|P(\xi)| \leq (\epsilon/4)H(P)^{-1}$ has a root $\alpha \in \mathbb{C}$ with*

$$|\xi - \alpha| \leq (1+\epsilon)\frac{|P(\xi)|}{|P'(\xi)|}.$$

Proof. Let $P(T) = a(T-\alpha)(T-\beta)$ where $|\xi - \alpha| \leq |\xi - \beta|$. Since the discriminant of P is a non-zero integer and can be written as

$$\triangle = P'(\xi)^2 - 4aP(\xi),$$

we get

$$1 \leq |P'(\xi)|^2 + 4H(P)|P(\xi)| \leq |P'(\xi)|^2 + \epsilon$$

and thus

$$\sqrt{1-\epsilon} \leq |P'(\xi)|. \tag{1.6}$$

Since the discriminant of P can also be written as

$$\triangle = a^2|\alpha - \beta|^2 \geq 1,$$

we get

$$|\alpha - \beta| \geq \frac{1}{|a|} \geq \frac{1}{H(P)}. \tag{1.7}$$

Using Lemma 1.29 and (1.6) we deduce

$$\begin{aligned}|\xi - \alpha| \leq& 2\frac{|P(\xi)|}{|P'(\xi)|}\\ \leq& \frac{2}{\sqrt{1-\epsilon}}|P(\xi)|\\ \leq& \frac{8}{3}|P(\xi)|\\ \leq& \frac{2\epsilon}{3}H(P)^{-1}.\end{aligned}$$

This estimate, combined with (1.7) gives

$$\begin{aligned}|\xi-\beta| \geq&|\alpha-\beta|-|\alpha-\xi|\\ \geq&H(P)^{-1}-\frac{2\epsilon}{3}H(P)^{-1}\\ \geq&\frac{2}{3}H(P)^{-1}\\ \geq&\epsilon^{-1}|\xi-\alpha|\end{aligned}$$

and therefore

$$\begin{aligned}\frac{|P'(\xi)|}{|P(\xi)|}=&\frac{1}{|\xi-\alpha|}+\frac{1}{|\xi-\beta|}\\ =&\frac{1}{|\xi-\alpha|}\left(1+\frac{|\xi-\alpha|}{|\xi-\beta|}\right)\\ \leq&\frac{1}{|\xi-\alpha|}(1+\epsilon).\end{aligned}$$

□

Lemma 1.31. *Let $\xi \in \mathbb{C}$. If $P(T) \in \mathbb{Z}[T]$ is of degree d, then for $z \in \mathbb{C}$ with $|z-\xi| \leq 1$ we have*

$$|P(z)-P(\xi)| \leq |z-\xi|H(P)\sum_{i=1}^{d}\left((|\xi|+1)^{i}-|\xi|^{i}\right).$$

Proof. Write $P(T)=a_dT^d+a_{d-1}T^{d-1}+\cdots+a_0$. Then

$$\begin{aligned}|P(z)-P(\xi)|=&\left|\sum_{i=0}^{d}a_i(z^i-\xi^i)\right|\\ \leq&H(P)|z-\xi|\sum_{i=0}^{d}|z^{i-1}+z^{i-2}\xi+\cdots+z\xi^{i-2}+\xi^{i-1}|\\ \leq&H(P)|z-\xi|\sum_{i=0}^{d}((|\xi|+1)^{i-1}+\cdots+(|\xi|+1)|\xi|^{i-2}+|\xi|^{i-1})\\ =&H(P)|z-\xi|\sum_{i=0}^{d}\frac{(|\xi|+1)^i-|\xi|^i}{(|\xi|+1)-|\xi|}\\ =&H(P)|z-\xi|\sum_{i=1}^{d}\left((|\xi|+1)^{i}-|\xi|^{i}\right).\end{aligned}$$

□

Corollary 1.32. *Let $\xi \in \mathbb{C}$ and $P(T) \in \mathbb{Z}[T]_{\leq 2}$. If $z \in \mathbb{C}$ with $|z - \xi| \leq 1$ then*

$$|P(z) - P(\xi)| \leq (2|\xi| + 2)|z - \xi|H(P).$$

1.4 Results on determinants and resultants

Determinants and resultants can be used to decide the linear dependency of polynomials. We can also determine if two polynomials share a root by examining determinants and resultants. It is therefore essential to discuss these objects at this stage.

Definition 1.33. We define the determinant of n polynomials of degree at most $n-1$ to be the determinant of the $n \times n$ matrix of their coefficients.

Definition 1.34. We define the *sign* of a permutation σ on n elements to be

$$\operatorname{sgn}(\sigma) := \begin{cases} -1 & \text{if } \sigma \text{ is an odd permutation,} \\ 1 & \text{if } \sigma \text{ is an even permutation.} \end{cases}$$

1.4.1 Working with determinants

We define here a new object that is similar to the determinant and permanent of a matrix, and give some properties of this new object.

Notation 1.35. Let $A = (a_{ij})$ be an $n \times n$ matrix. We define

$$[[A]] := \sum_{\sigma} |a_{1\sigma(1)}||a_{2\sigma(2)}| \dots |a_{n\sigma(n)}|$$

where σ is taken over all permutations on the n symbols $\{1, 2, \dots, n\}$.

Clearly,

$$|\det(A)| = \left| \sum_{\sigma} (-1)^{\operatorname{sgn}(\sigma)} a_{1\sigma(1)} a_{2\sigma(2)} \dots a_{n\sigma(n)} \right| \leq [[A]]$$

where σ is taken over all permutations on the n symbols $\{1, 2, \dots, n\}$.

The proof of the following Proposition follows from the definitions.

Proposition 1.36. *Let $A \in \mathrm{M}_n(\mathbb{R})$. Then*

1. $[[\alpha A]] = \alpha^n [[A]]$ *for* $\alpha \in \mathbb{R}$,

2. $[[A]] = 0$ *implies* $\|A\| = 0$,

3. *If A has a row/column of zeroes, then* $[[A]] = 0$,

4. $[[\cdot]]$ *is not a norm.*

We now explain a technique for calculating determinants: let $\xi \in \mathbb{C}$ and let $P(T), Q(T) \in \mathbb{Z}[T]$ be polynomials of degree m and n respectively. Write

$$\begin{aligned} P(T) &= p_m T^m + p_{m-1} T^{m-1} + \cdots + p_0, \\ Q(T) &= q_n T^n + q_{n-1} T^{n-1} + \cdots + q_0. \end{aligned}$$

The absolute value of the resultant of P and Q is a non-negative integer defined by

$$|\operatorname{Res}(P,Q)| = \left\| \begin{matrix} p_m & p_{m-1} & \cdots & p_0 & 0 & \ldots & 0 \\ & & & \cdots & & & \\ 0 & \cdots & 0 & p_m & p_{m-1} & \cdots & p_0 \\ q_n & q_{n-1} & \cdots & q_0 & 0 & \ldots & 0 \\ & & & \cdots & & & \\ 0 & \cdots & 0 & q_n & q_{n-1} & \cdots & q_0 \end{matrix} \right\| . \tag{1.8}$$

Adding a multiple of a column to another column doesn't change the value of the determinant; we do this in a very ingenious manner. Following Brownawell [4], we consider two cases which depend on the choice of ξ: If $|\xi| < 1$, we add ξ^{m+n-j} times the j-th column to the last column for $1 \leq j \leq m+n-1$ and use the properties of

$[[\cdot]]$ to get

$$|\operatorname{Res}(P,Q)| \leq \left[\left[\begin{matrix} p_m & p_{m-1} & \cdots & p_0 & 0 & \cdots & \xi^{n-1}P(\xi) \\ & & & \cdots & & & \\ 0 & \cdots & 0 & p_m & p_{m-1} & \cdots & P(\xi) \\ q_n & q_{n-1} & \cdots & q_0 & 0 & \cdots & \xi^{m-1}Q(\xi) \\ & & & \cdots & & & \\ 0 & \cdots & 0 & q_n & q_{n-1} & \cdots & Q(\xi) \end{matrix}\right]\right]. \tag{1.9}$$

Expanding along the last column, the result is of the form

$$\begin{aligned} |\operatorname{Res}(P,Q)| &\leq \sum_{i=1}^{n} |\xi^{i-1}||P(\xi)|[[A_i]] + \sum_{j=1}^{m} |\xi^{j-1}||Q(\xi)|[[B_j]] \\ &\leq \sum_{i=1}^{n} |P(\xi)|[[A_i]] + \sum_{j=1}^{m} |Q(\xi)|[[B_j]] \end{aligned} \tag{1.10}$$

where A_i and B_j are minors of order $m+n-1$ extracted from the first $m+n-1$ columns of the matrix $\operatorname{Res}(P,Q)$. We therefore get a bound on the value of the resultant of the polynomials P and Q which takes into account their values at a fixed point $\xi \in \mathbb{C}$.

Similarly, starting at (1.8), if $|\xi| \geq 1$, we add $\xi^{-(j-1)}$ times the j-th column to the first column for $2 \leq j \leq m+n$ to get the inequalities

$$\begin{aligned} |\operatorname{Res}(P,Q)| &\leq \left[\left[\begin{matrix} \xi^{-m}P(\xi) & p_{m-1} & \cdots & p_0 & 0 & \cdots & 0 \\ & & & \cdots & & & \\ \xi^{-m-n+1}P(\xi) & \cdots & 0 & p_m & p_{m-1} & \cdots & p_0 \\ \xi^{-n}Q(\xi) & q_{n-1} & \cdots & q_0 & 0 & \cdots & 0 \\ & & & \cdots & & & \\ \xi^{-n-m+1}Q(\xi) & \cdots & 0 & q_n & q_{n-1} & \cdots & q_0 \end{matrix}\right]\right] \\ &\leq \sum_{i=1}^{n} |\xi^{-m-i+1}||P(\xi)|[[C_i]] + \sum_{j=1}^{m} |\xi^{-n-j+1}||Q(\xi)|[[D_j]] \\ &\leq \sum_{i=1}^{n} |P(\xi)|[[C_i]] + \sum_{j=1}^{m} |Q(\xi)|[[D_j]] \end{aligned}$$

for C_i and D_j minors of order $m+n-1$ extracted from the last $m+n-1$ columns of the matrix $\mathrm{Res}(P,Q)$. We arrive at the same conclusion as above (with different minors).

We can also use this idea for a determinant of n polynomials of degree at most $n-1$. In proofs to follow, this technique is used without further explanation.

1.4.2 Upper bounds for determinants and resultants

Lemma 1.37. *Let $\xi \in \mathbb{C}$ and let $P(T), Q(T) \in \mathbb{C}[T]$ be non-constant polynomials of degree m and n respectively. Then,*

$$|\mathrm{Res}(P,Q)| \le H(P)^n H(Q)^m \left(c_1 \frac{|P(\xi)|}{H(P)} + c_2 \frac{|Q(\xi)|}{H(Q)} \right)$$

for some constants $c_1 = c_1(m,n) > 0$ and $c_2 = c_2(m,n) > 0$.

Proof. We apply the formula established in the previous section. Assuming that $|\xi| < 1$, we get from equations (1.9), (1.10) and the properties of $[[\cdot]]$ that

$$\begin{aligned}
|\mathrm{Res}(P,Q)| \le & \left[\!\!\left[\begin{array}{ccccccc}
H(P) & H(P) & \dots & H(P) & 0 & \dots & \xi^{n-1}P(\xi) \\
 & & & \dots & & & \\
0 & \dots & 0 & H(P) & H(P) & \dots & P(\xi) \\
H(Q) & H(Q) & \dots & H(Q) & 0 & \dots & \xi^{m-1}Q(\xi) \\
 & & & \dots & & & \\
0 & \dots & 0 & H(Q) & H(Q) & \dots & Q(\xi)
\end{array} \right]\!\!\right] \\
\le & \sum_{i=1}^{n} |P(\xi)|[[A_i]] + \sum_{j=1}^{m} |Q(\xi)|[[B_j]] \\
\le & c_1 H(P)^{n-1} H(Q)^m |P(\xi)| + c_2 H(P)^n H(Q)^{m-1} |Q(\xi)|,
\end{aligned}$$

where c_1 counts the number of non-zero products in the determinant containing $|P(\xi)|$ as a factor, and c_2 counts the number of non-zero products in the determinant containing $|Q(\xi)|$ as a factor. We get the same result in the case $|\xi| \ge 1$. □

In fact, we can easily calculate the values for c_1 and c_2 of the previous lemma when m and n are small.

m	n	c_1	c_2
1	1	1	1
1	2	3	1
2	2	6	6
1	3	6	1
2	3	19	11
3	3	54	54

As the table shows, the coefficients c_1 and c_2 become very large, very quickly. It is often difficult to calculate them for large values of m and n. However, we can find the trivial upper bound $c_1 + c_2 \leq (m+n)!$.

Lemma 1.38. *Let $\xi \in \mathbb{C}$ and let $P(T), Q(T) \in \mathbb{Z}[T]$ be non-zero polynomials of degree m and n respectively. Let $L(T) = \gcd(P, Q)$ be of degree d. Then*

$$H(L)^{m+n-2d-1}|L(\xi)| \leq H(P)^{n-d}H(Q)^{m-d}\left(k_1\frac{|P(\xi)|}{H(P)} + k_2\frac{|Q(\xi)|}{H(Q)}\right)$$

for some computable, non-zero, positive constants k_1 and k_2.

Proof. Let

$$P_1(T) = \frac{P(T)}{L(T)}, \qquad Q_1(T) = \frac{Q(T)}{L(T)}$$

with $\deg(P_1) = m_1 = m - d$, and $\deg(Q_1) = n_1 = n - d$. From Lemma 1.25,

$$H(P_1) \leq 2^m(m+1)\frac{H(P)}{H(L)} \quad \text{and} \quad H(Q_1) \leq 2^n(n+1)\frac{H(Q)}{H(L)}.$$

Since P_1 and Q_1 have no common factor, $\operatorname{Res}(P_1, Q_1)$ is a non-zero integer. Using

Lemma 1.37 and the inequalities above,

$$\begin{aligned}
1 \leq& |\operatorname{Res}(P_1, Q_1)| \\
\leq& H(P_1)^{n_1} H(Q_1)^{m_1} \left(c_1 \frac{|P_1(\xi)|}{H(P_1)} + c_2 \frac{|Q_1(\xi)|}{H(Q_1)} \right) \\
\leq& c_1 H(P_1)^{n_1-1} H(Q_1)^{m_1} |P_1(\xi)| + c_2 H(P_1)^{n_1} H(Q_1)^{m_1-1} |Q_1(\xi)| \\
\leq& c_1 \left(2^m (m+1) \frac{H(P)}{H(L)} \right)^{n_1-1} \left(2^n (n+1) \frac{H(Q)}{H(L)} \right)^{m_1} \left| \frac{P(\xi)}{L(\xi)} \right| \\
&+ c_2 \left(2^m (m+1) \frac{H(P)}{H(L)} \right)^{n_1} \left(2^n (n+1) \frac{H(Q)}{H(L)} \right)^{m_1-1} \left| \frac{Q(\xi)}{L(\xi)} \right| .
\end{aligned}$$

Thus the lemma is proved for

$$\begin{aligned}
k_1 =& c_1 2^{m(2n-d-1)-nd} (m+1)^{n-d-1} (n+1)^{m-d}, \\
k_2 =& c_2 2^{n(2m-d-1)-md} (m+1)^{n-d} (n+1)^{m-d-1}.
\end{aligned}$$

□

Lemma 1.39. *Let* $\xi \in \mathbb{C}$ *and let* $P(T), Q(T) \in \mathbb{Z}[T]_{\leq 2}$ *with* $L(T) = \gcd(P, Q)$ *be of degree at least* 1. *Then*

$$H(L)|L(\xi)| \leq \gamma \big(H(P)|Q(\xi)| + H(Q)|P(\xi)| \big).$$

Proof. Since $L = \gcd(P, Q)$, we get that P/L, Q/L are polynomials of degree at most 1 with $\operatorname{Res}(P/L, Q/L)$ being a non-zero integer since the two polynomials have no common factor. Thus, using Lemma 1.37

$$\begin{aligned}
1 \leq& \left| \operatorname{Res}\left(\frac{P}{L}, \frac{Q}{L} \right) \right| \\
\leq& H\left(\frac{P}{L} \right) \left| \left(\frac{Q}{L} \right)(\xi) \right| + H\left(\frac{Q}{L} \right) \left| \left(\frac{P}{L} \right)(\xi) \right| \\
\leq& \gamma \frac{H(P)}{H(L)} \frac{|Q(\xi)|}{|L(\xi)|} + \gamma \frac{H(Q)}{H(L)} \frac{|P(\xi)|}{|L(\xi)|}.
\end{aligned}$$

(We used $c_1 = c_2 = 1$ as seen in the table following Lemma 1.37.) □

Lemma 1.40. *Let $\xi \in \mathbb{C}$ and let $P_i(T) \in \mathbb{C}[T]_{\leq n-1}$ for $1 \leq i \leq n$ be non-zero polynomials. Then*

$$|\det(P_1, P_2, \ldots, P_n)| \leq (n-1)!\left(\prod_{i=1}^{n} H(P_i)\right)\left(\sum_{i=1}^{n} \frac{|P_i(\xi)|}{H(P_i)}\right).$$

Proof. Write $P_i(T) = p_{i,n-1}T^{n-1} + p_{i,n-2}T^{n-2} + \cdots + p_{i,0}$ for $1 \leq i \leq n$. Then

$$\begin{aligned}
|\det(P_1, P_2, \ldots, P_n)| &= \begin{Vmatrix} p_{1,n-1} & p_{1,n-2} & \cdots & p_{1,0} \\ p_{2,n-1} & p_{2,n-2} & \cdots & p_{2,0} \\ \vdots & \vdots & \ddots & \vdots \\ p_{n,n-1} & p_{n,n-2} & \cdots & p_{n,0} \end{Vmatrix} \\
&\leq \left[\!\!\left[\begin{matrix} H(P_1) & H(P_1) & \ldots & P_1(\xi) \\ H(P_2) & H(P_2) & \ldots & P_2(\xi) \\ \vdots & \vdots & \ddots & \vdots \\ H(P_n) & H(P_n) & \ldots & P_n(\xi) \end{matrix}\right]\!\!\right] \\
&=(n-1)!\left(\prod_{i=1}^{n} H(P_i)\right)\left(\sum_{i=1}^{n} \frac{|P_i(\xi)|}{H(P_i)}\right).
\end{aligned}$$

□

We now examine the case $n = 3$ in details.

Lemma 1.41. *Let $P_1, P_2, P_3 \in \mathbb{C}[T]_{\leq 2}$ and let $\xi \in \mathbb{C}$. Then*

$$|\det(P_1, P_2, P_3)| \leq \sum_{\sigma} H(P_{\sigma(1)})|P_{\sigma(2)}(\xi)||P'_{\sigma(3)}(\xi)|$$

where σ is taken over all permutations of the three symbols $\{1, 2, 3\}$.

Proof. Write $P_i(T) = p_{i,2}T^2 + p_{i,1}T + p_{i,0}$ for $i = 1, 2, 3$. Then,

$$1 \leq \begin{Vmatrix} p_{1,2} & p_{1,1} & p_{1,0} \\ p_{2,2} & p_{2,1} & p_{2,0} \\ p_{3,2} & p_{3,1} & p_{3,0} \end{Vmatrix}$$

$$\begin{aligned}
&= \left\| \begin{matrix} p_{1,2} & 2p_{1,2}\xi + p_{1,1} & p_{1,2}\xi^2 + p_{1,1}\xi + p_{1,0} \\ p_{2,2} & 2p_{2,2}\xi + p_{2,1} & p_{2,2}\xi^2 + p_{2,1}\xi + p_{2,0} \\ p_{3,2} & 2p_{3,2}\xi + p_{3,1} & p_{3,2}\xi^2 + p_{3,1}\xi + p_{3,0} \end{matrix} \right\| \\
&\leq \left[\!\!\left[\begin{matrix} H(P_1) & P_1'(\xi) & P_1(\xi) \\ H(P_2) & P_2'(\xi) & P_2(\xi) \\ H(P_3) & P_3'(\xi) & P_3(\xi) \end{matrix} \right]\!\!\right] \\
&= \sum_{\sigma} H(P_{\sigma(1)}) |P_{\sigma(2)}(\xi)| |P'_{\sigma(3)}(\xi)|
\end{aligned}$$

where σ is taken over all permutations of the symbols $\{1, 2, 3\}$. □

We get, more generally,

Lemma 1.42. *Let $P_1, P_2, \ldots, P_n \in \mathbb{C}[T]_{\leq n-1}$ and let $\xi \in \mathbb{C}$. Then*

$$|\det(P_1, P_2, \ldots, P_n)| \leq \sum_{\sigma} H(P_{\sigma(1)}) |P_{\sigma(2)}(\xi)| |P'_{\sigma(3)}(\xi)| \ldots |P^{(n-2)}_{\sigma(n)}(\xi)|$$

where σ is taken over all permutations of the n symbols $\{1, 2, \ldots, n\}$.

Chapter 2

Special sequences of real numbers and polynomials

2.1 Construction of a polynomial sequence

Definition 2.1. We say that a function $\phi : \mathbb{Z}[T] \longrightarrow \mathbb{R}_{\geq 0}$ is a *norm* if and only if for $P \in \mathbb{Z}[T]$ and $a \in \mathbb{Z}$ we have

1. $\phi(P) = 0$ if and only if $P = 0$,

2. $\phi(aP) = |a|\phi(P)$,

3. $\phi(P+Q) \leq \phi(P) + \phi(Q)$.

Proposition 2.2. *Let $\phi : \mathbb{Z}[T]_{\leq n} \longrightarrow \mathbb{R}_{\geq 0}$ be a norm. Then there exists a strictly increasing sequence of nonzero positive integers $(X_i)_{i\geq 1}$ and a sequence of nonzero polynomials $\big(P_i(T)\big)_{i\geq 1} \subset \mathbb{Z}[T]_{\leq n}$ such that*

1. $H(P_i) = X_i \qquad (i \geq 1)$,

2. $\phi(P_{i+1}) < \phi(P_i) \qquad (i \geq 1)$, *3.* $\phi(P_i) \leq \phi(P)$ *for all* $P \in \mathbb{Z}[T]_{\leq n}$ *with* $0 < H(P) < X_{i+1}$,

4. P_i *and* P_{i+1} *are linearly independent over* $\mathbb{Q}$ *for all* i.

Proof. For each $j \in \mathbb{Z}_{>0}$ define

$$\mathcal{Q}_j := \{Q(T) \in \mathbb{Z}[T]_{\leq n} \mid Q \neq 0\,,\, H(Q) \leq j\}$$

and

$$q_j := \min_{Q \in \mathcal{Q}_j} \{\phi(Q)\} > 0.$$

From these we get two sequences,

$$\mathcal{Q}_1 \subset \mathcal{Q}_2 \subset \ldots, \qquad q_1 \geq q_2 \geq \ldots.$$

Let $X_1 = 1$ and pick $P_1 \in \mathcal{Q}_1$ such that $\phi(P_1) = q_1$. Inductively, define X_{i+1} to be the smallest integer $j \in \mathbb{Z}_{>0}$ such that $q_j < \phi(P_i)$. Pick $P_{i+1} \in \mathcal{Q}_j$ such that $\phi(P_{i+1}) = q_j$. If $P \in \mathbb{Z}[T]_{\leq n}$ with $H(P) < X_{i+1}$ for some i, then $\phi(P) \geq q_i$ by construction of the sequence and thus $H(P_{i+1}) = X_{i+1}$. Moreover, since the coefficients of P_i must be relatively prime, we get P_i and P_{i+1} linearly independent over $\mathbb{Q}$. So the two sequences constructed satisfy the four properties listed. □

Definition 2.3. We define $(P_i)_{i\geq 1} \subset \mathbb{Z}[T]_{\leq n}$ to be a *minimum polynomial sequence in degree at most* n and $\big(\phi, (X_i)_{i\geq 1}, (P_i)_{i\geq 1}\big)$ to be a *norm triplet in degree at most* n.

As a general rule, the only polynomial $P(T) \in \mathbb{Z}[T]_{\leq n}$ satisfying

$$H(P) < X_{i+1} \quad \text{and} \quad \phi(P) < \phi(P_i)$$

is the zero polynomial.

It is also clear that given a norm ϕ, the corresponding polynomial sequence is not, a priori, uniquely defined.

Example 2.4. *Here are two important examples of norms* ϕ. *Fix* $\xi \in \mathbb{R}$ *such that* $[\mathbb{Q}(\xi) : \mathbb{Q}] > d$. *For a polynomial* $P(T) \in \mathbb{Z}[T]_{\leq d}$ *let:*

1. *$\phi(P) = \phi_\xi(P) = |P(\xi)|$. Since ϕ is the absolute value of the real number $P(\xi) \neq 0$, ϕ is a norm. The sequence $(P_i)_{i\geq 1}$ is defined uniquely up to the sign of each P_i.*

2. *$\phi(Q) = \phi_\xi(Q) = \max\{|Q(\xi)|, |Q'(\xi)|, \ldots, |Q^{(d-1)}(\xi)|\}$. Since $\deg(\xi) > d$ and $\deg(Q) < d$, we get that $\phi(Q) = 0$ if and only if $Q = 0$. Moreover, for $a \in \mathbb{Z}$, $\phi(aQ) = |a|\phi(Q)$ and*

$$\begin{aligned}\phi(P+Q) =& \max\{|P(\xi)+Q(\xi)|, \ldots, |P^{(d-1)}(\xi)+Q^{(d-1)}(\xi)|\} \\ \leq& \max\{|P(\xi)|, \ldots, |P^{(d-1)}(\xi)|\} + \max\{|Q(\xi)|, \ldots, |Q^{(d-1)}(\xi)|\} \\ =& \phi(P)+\phi(Q).\end{aligned}$$

Thus ϕ is a norm and the sequence $(Q_i)_{i\geq 1}$ is defined uniquely up to sign of each Q_i for $i \gg 1$. To see this, let $R, S \in \mathbb{Z}[T]_{\leq d}$ be such that $\phi(R) = \phi(S) < 1/2$. We first note that if $\phi(R) < 1/2$ then $\deg(R) = d$. This is clear since $|R^{(\deg(d))}(\xi)| \geq 1$. So there exists $1 \leq i \leq j \leq d-1$ such that $\phi(R) = |R^{(i)}(\xi)|$ and $\phi(S) = |S^{(j)}(\xi)|$, permuting R and S if necessary. Then $R^{(i)}(\xi) = \pm S^{(j)}(\xi)$ which implies that $i = j$ and $R^{(i)} = \pm S^{(j)}$. If $i = j = 0$, we are done as we get $R = \pm S$. Otherwise, we get by integrating the polynomials that $R^{(i-1)} = \pm S^{(i-1)} + a$ with $a \in \mathbb{Z}$. Thus $|a| = |R^{(i-1)}(\xi) \pm S^{(i-1)}(\xi)| < 1$ and hence $R^{(i-1)} = \pm S^{(i-1)}$. Recursively we get $R = \pm S$ and thus the sequence $(Q_i)_{i\geq 1}$ is defined uniquely up to sign of each Q_i whenever $\phi(Q_i) < 1/2$.

2.2 General properties

It is now time to study in detail the polynomial sequence constructed in Proposition 2.2 using an arbitrary norm ϕ. The linear dependence or independence of these polynomials is carefully examined here. Henceforth, let $(\phi, (X_i)_{i\geq 1}, (P_i)_{i\geq 1})$ be a fixed norm triplet in degree at most n.

Lemma 2.5. *The set $\{P_i, P_{i+1}\}$ is a basis over $\mathbb{Z}$ for the $\mathbb{Z}$-module $\mathcal{M} = \langle P_i, P_{i+1}\rangle_{\mathbb{Q}} \cap \mathbb{Z}[T]$.*

Proof. Pick a non-zero polynomial $P \in \langle P_i, P_{i+1}\rangle_{\mathbb{Q}} \cap \mathbb{Z}[T]$ and write $P = uP_i + vP_{i+1}$ with $u, v \in \mathbb{Q}$. Let u', v' be the closest integers to u and v respectively. Then $P' = u'P_i + v'P_{i+1} \in \mathcal{M}$ and

$$P - P' = (u-u')P_i + (v-v')P_{i+1} \qquad \in \mathcal{M}$$

with $|u-u'|, |v-v'| \leq \frac{1}{2}$. We claim that this implies $u' = u$ and $v' = v$. On one hand

$$\begin{aligned} H(P-P') =& H\big((u-u')P_i + (v-v')P_{i+1}\big) \\ \leq& |u-u'|H(P_i) + |v-v'|H(P_{i+1}) \\ \leq& \frac{1}{2}\big(H(P_i) + H(P_{i+1})\big) \\ <& H(P_{i+1}). \end{aligned} \tag{2.1}$$

On the other hand,

$$\begin{aligned} \phi(P-P') =& \phi\big((u-u')P_i + (v-v')P_{i+1}\big) \\ \leq& |u-u'|\phi(P_i) + |v-v'|\phi(P_{i+1}) \\ \leq& \frac{1}{2}\big(\phi(P_i) + \phi(P_{i+1})\big) \\ <& \phi(P_i). \end{aligned} \tag{2.2}$$

By construction of the norm triplet, (2.1) and (2.2) cannot hold at the same time unless $P - P' = 0$, and therefore $u' = u$ and $v' = v$ as claimed. □

Lemma 2.6. *If the polynomials P_{i-1}, P_i and P_{i+1} are linearly dependent over $\mathbb{Q}$ then*

$$P_{i-1} \pm P_{i+1} = uP_i$$

for $u \in \mathbb{Z}$.

Proof. Using Lemma 2.5 we know that $\{P_{i-1}, P_i\}$ and $\{P_i, P_{i+1}\}$ form bases over $\mathbb{Z}$ for $\mathcal{M} = \langle P_{i-1}, P_i\rangle_{\mathbb{Q}} \cap \mathbb{Z}[T] = \langle P_i, P_{i+1}\rangle_{\mathbb{Q}} \cap \mathbb{Z}[T]$. Thus

$$P_{i-1} = uP_i + vP_{i+1} \quad \text{and} \quad P_{i+1} = u' P_{i-1} + v' P_i$$

for $u, v, u', v' \in \mathbb{Z}$. So

$$(1 - vu')P_{i-1} = (u + vv')P_i$$

which necessarily implies that $vu' = 1$ since two consecutive polynomials P_{i-1} and P_i are linearly independent. Hence $v = \pm 1$, and the lemma is proved. □

Lemma 2.7. *Let $\xi \in \mathbb{C}$ with $[\mathbb{Q}(\xi) : \mathbb{Q}] > 2$. Assume that*

1. $\lim_{i\to\infty} X_{i+1}\phi(P_i) = 0$,

2. $|P(\xi)| \leq \phi(P)$ *for all* $P \in \mathbb{Z}[T]_{\leq 2}$.

Then P_{i-1}, P_i and P_{i+1} are linearly independent for infinitely many i.

Proof. Assume, on the contrary, that P_{i-1}, P_i and P_{i+1} are linearly dependent over $\mathbb{Q}$ for all $i \geq i_0$. Then for all $i, j \geq i_0$ we have

$$\mathcal{V} = \langle P_{i-1}, P_i\rangle_{\mathbb{Q}} = \langle P_{j-1}, P_j\rangle_{\mathbb{Q}}.$$

Let $\{P, Q\} \subset \mathbb{Z}[T]_{\leq 2}$ be a basis of $\mathcal{V} \cap \mathbb{Z}[T]_{\leq 2}$. Thus for all $i \geq i_0$, $P_i = a_iP + b_iQ$ with $a_i, b_i \in \mathbb{Z}$ and $|a_i|, |b_i| \leq cX_i$ for $c = c(P, Q) > 0$. Since P_i and P_{i+1} are linearly independent by construction, we get

$$\begin{aligned} 1 \leq & \left\| \begin{matrix} a_i & b_i \\ a_{i+1} & b_{i+1} \end{matrix} \right\| \\ \leq & \frac{1}{|Q(\xi)|} \left\| \begin{matrix} a_i & a_iP(\xi) + b_iQ(\xi) \\ a_{i+1} & a_{i+1}P(\xi) + b_{i+1}Q(\xi) \end{matrix} \right\| \\ = & \frac{|a_iP_{i+1}(\xi) - a_{i+1}P_i(\xi)|}{|Q(\xi)|} \\ \leq & \frac{2c}{|Q(\xi)|} X_{i+1}\phi(P_i). \end{aligned}$$

As we let i tend to infinity, we obtain a contradiction to our initial hypothesis. □

2.3 Study of a specific norm function

We now elaborate on the second example of norm ϕ defined in Example 2.4. For $Q \in \mathbb{Z}[T]_{\leq 2}$ and $\xi \in \mathbb{C}$ with $[\mathbb{Q}(\xi) : \mathbb{Q}] > 2$, let $\phi(Q) = \max\{|Q(\xi)|, |Q'(\xi)|\}$ and fix a norm triplet $(\phi, (X_i)_{i\geq 1}, (Q_i)_{i\geq 1})$ in degree at most 2. Three main lemmas are seen below: one tells us that, under some hypothesis, Q_i does not have multiple roots, while the other two give bounds for $\phi(Q_i)$. We denote

$$Q_i(T) = q_{i,2}T^2 + q_{i,1}T + q_{i,0}.$$

Lemma 2.8. *The polynomial Q_i has degree exactly 2 for $i \geq 2$.*

Proof. Clearly, only $Q_1 = 1$ can have degree 0. So assume $\deg(Q_i) = 1$. Then $Q_i(T) = q_{i,1}T + q_{i,0}$ and

$$\phi(Q_i) = \max\{|q_{i,1}\xi + q_{i,0}|, |q_{i,1}|\} < 1 \qquad (i \geq 1).$$

Since $|q_{i,1}| \geq 1$, this is impossible and hence $\deg(Q_i) = 2$. □

Lemma 2.9. *Let $\xi \in \mathbb{C}$ with $[\mathbb{Q}(\xi) : \mathbb{Q}] > 2$. Assume that*

$$\lim_{i \longrightarrow \infty} X_i^{1/2}\phi(Q_{i-1}) = 0.$$

Then Q_i has distinct roots for all sufficiently large i.

Proof. We know from Lemma 2.8 that for $i \geq 2$ Q_i has degree 2, so assume it has only one root of multiplicity 2. Then

$$Q_i = \pm L(T)^2$$

where $L(T) = (mT + n)$ for $m, n \in \mathbb{Z}$ with $m \neq 0$. Recall that Lemma 1.27 states

$$\frac{1}{\gamma}H(L)^2 \leq H(Q_i) = X_i \leq 2H(L)^2. \tag{2.3}$$

Since $L(T) = L'(\xi)(T-\xi) + L(\xi)$ and $|L(\xi)| = |Q_i(\xi)|^{1/2} < 1 \leq |L'(\xi)| = |m|$ we have

$$\begin{aligned} H(L) =& H\big(L'(\xi)(T-\xi) + L(\xi)\big) \\ \leq& |L'(\xi)| \max\{1, |\xi|\} + |L(\xi)| \\ \leq& |L'(\xi)| \max\{2, 1+|\xi|\}, \end{aligned}$$

and using equation (2.3),

$$\begin{aligned} |L'(\xi)| \geq& \frac{H(L)}{\max\{2, 1+|\xi|\}} \\ \geq& \frac{X_i^{1/2}}{\sqrt{2}\max\{2, 1+|\xi|\}}. \end{aligned}$$

Since

$$|Q_i'(\xi)| = |2L(\xi)L'(\xi)| \leq \phi(Q_i),$$

we get the upper bound

$$\begin{aligned} |L(\xi)| \leq& \frac{\phi(Q_i)}{2|L'(\xi)|} \\ \leq& \frac{\max\{2, 1+|\xi|\}\phi(Q_i)}{\sqrt{2}X_i^{1/2}} \\ =& \frac{\kappa\phi(Q_i)}{2X_i^{1/2}} \end{aligned}$$

for $\kappa = \sqrt{2}\max\{2, 1+|\xi|\}$. Consider the resultant of L and Q_{i-1}',

$$\begin{aligned} |\operatorname{Res}(L, Q_{i-1}')| \leq& H(L)|Q_{i-1}'(\xi)| + H(Q_{i-1}')|L(\xi)| \\ \leq& \gamma^{1/2}X_i^{1/2}\phi(Q_{i-1}) + \kappa X_{i-1}\frac{\phi(Q_i)}{X_i^{1/2}} \\ \leq& \big(\gamma^{1/2} + \kappa\big)X_i^{1/2}\phi(Q_{i-1}) \end{aligned}$$

which is, for i large enough, a real number smaller than 1. Since the resultant of two integral polynomials must be an integer we have

$$|\operatorname{Res}(L, Q_{i-1}')| = 0, \tag{2.4}$$

which implies that Q'_{i-1} (of degree 1) is an integer multiple of L for i large enough.

On the other hand, the resultant of L and the polynomial $2Q_{i-1}-TQ'_{i-1}$ (of degree at most 1) is

$$\begin{aligned}\left|\mathrm{Res}(L, 2Q_{i-1}-TQ'_{i-1})\right| \leq& H(L)|2Q_{i-1}(\xi)-\xi Q'_{i-1}(\xi)| + H(2Q_{i-1}-TQ'_{i-1})|L(\xi)|\\ \leq& \gamma^{1/2}X_i^{1/2}(2+|\xi|)\phi(Q_{i-1}) + 4H(Q_{i-1})\frac{\kappa\phi(Q_i)}{2X_i^{1/2}}\\ \leq& (\gamma^{1/2}(2+|\xi|)+2\kappa)X_i^{1/2}\phi(Q_{i-1}),\end{aligned}$$

which is, again, clearly smaller than 1 for i large enough. Hence for large i

$$\left|\mathrm{Res}(L, 2Q_{i-1}-TQ'_{i-1})\right| = 0 \tag{2.5}$$

and therefore $2Q_{i-1}-TQ'_{i-1}$ is an integer multiple of L.

Since equation (2.4) implies that L divides Q'_{i-1}, and equation (2.5) implies that L divides $2Q_{i-1}-TQ'_{i-1}$, we get that L must divide Q_{i-1}. Thus, Q_{i-1} and Q'_{i-1} share a common root. Since $\deg(Q_{i-1}) = 2$, we have

$$Q_{i-1}(T) = \pm L(T)^2.$$

That is to say Q_i and Q_{i-1} are linearly dependent, which is impossible by construction of the polynomial sequence. Thus, for large i, Q_i must have two distinct roots. □

Lemma 2.10. *Under the hypotheses of Lemma 2.9, for i large enough*

$$\phi(Q_i) \geq (8+2|\xi|)^{-1}X_i^{-1}.$$

Proof. Lemma 2.9 states that Q_i does not have multiple roots for $i \geq i_0$. For such an i, the resultant of Q'_i and $2Q_i - TQ'_i$ is a non-zero integer, so

$$\begin{aligned}1 \leq& \left|\mathrm{Res}(2Q_i-TQ'_i, Q'_i)\right|\\ \leq& H(2Q_i-TQ'_i)|Q'_i(\xi)| + H(Q'_i)\left|2Q_i(\xi)-\xi Q'_i(\xi)\right|\\ \leq& H(Q_i)\left(4|Q'_i(\xi)| + 2\left|2Q_i(\xi)-\xi Q'_i(\xi)\right|\right)\\ \leq& X_i\left(4+2(2+|\xi|)\right)\phi(Q_i)\end{aligned}$$

□

Lemma 2.11. *Let $\xi \in \mathbb{C}$ with $[\mathbb{Q}(\xi) : \mathbb{Q}] > 2$. Suppose Q_{i-1}, Q_i and Q_{i+1} are linearly independent. Then*

$$1 \leq \sum_{\sigma} X_{\sigma(i-1)} \phi(Q_{\sigma(i)}) \phi(Q_{\sigma(i+1)})$$

where σ runs through the set of permutations of the three symbols $\{i-1, i, i+1\}$.

Proof. Lemma 1.41 states that

$$\begin{aligned} 1 &\leq | \det(Q_{i-1}, Q_i, Q_{i+1}) | \\ &\leq \sum_{\sigma} H(Q_{\sigma(i-1)}) |Q_{\sigma(i)}(\xi)| |Q'_{\sigma(i+1)}(\xi)| \\ &\leq \sum_{\sigma} X_{\sigma(i-1)} \phi(Q_{\sigma(i)}) \phi(Q_{\sigma(i+1)}) \end{aligned}$$

where σ runs through the set of permutations of the three symbols $\{i-1, i, i+1\}$. □

Chapter 3

Approximation to real numbers

3.1 Introduction

We now attack one of the main problems of Diophantine Approximation: how well can a real number be approximated by algebraic numbers? In particular, we look at approximations of real numbers by algebraic numbers of degree at most 2 or 3. We discuss this question by following its historical development, starting at the modern era of the Diophantine Approximation theory. As with all branches of mathematics, the theory is too broad and varied to give a complete account. Our focus is on precise theorems which motivate an optimal Gel'fond type criterion in degree 2. The standard notation $X \ll Y$ is used to mean that $X \leq cY$ for a constant $c > 0$.

3.2 Approximation to a real number by rationals

3.2.1 Dirichlet's Theorem

The modern era of the theory starts with Dirichlet [10] and his famous theorem, stated and proved more than 160 years ago.

Theorem 3.1 (Dirichlet). *Let $\alpha, Q \in \mathbb{R}$ with $Q > 1$. Then there exists $p, q \in \mathbb{Z}$ with $1 \leq q < Q$ satisfying*

$$|\alpha q - p| \leq \frac{1}{Q}.$$

Proof. Assume Q is an integer. Then the $Q + 1$ numbers

$$0\,,\,1\,,\,\{\alpha\}\,,\,\{2\alpha\}\,,\dots\,,\,\{(Q-1)\alpha\} \tag{3.1}$$

are distinct and contained in the interval $[0,1]$. Dividing the unit interval into Q subintervals

$$\left[\frac{Q-1}{Q}, 1\right], \qquad \left[\frac{u}{Q}, \frac{u+1}{Q}\right) \qquad (u = 0, 1, \dots, Q-2),$$

we find that at least two numbers enumerated in (3.1) must lie in the same interval of length $1/Q$ (clearly, the pair 0 and 1 is not). Thus, there exists $r_1, r_2, s_1, s_2 \in \mathbb{Z}$ with $0 \leq r_2 < r_1 < Q$ such that

$$\big|(r_1\alpha - s_1) - (r_2\alpha - s_2)\big| \leq \frac{1}{Q}.$$

Denoting $p = r_1 - r_2$ and $q = s_1 - s_2$ we have found integers p and q with $1 \leq q < Q$ satisfying

$$|q\alpha - p| \leq \frac{1}{Q},$$

proving the theorem whenever Q is an integer.

If Q is not an integer, we apply the above procedure to $[Q] + 1$. □

An obvious corollary is

Corollary 3.2. *Let $\alpha \in \mathbb{R}$ be an irrational number. Then there exists infinitely many rational numbers $p/q \in \mathbb{Q}$ such that*

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^2}.$$

This result led Liouville [14], in 1844, to state the first theorem of Transcendental Analysis: on approximating algebraic numbers by rational numbers.

Theorem 3.3 (Liouville). *Let $\alpha \in \mathbb{R}$ be algebraic of degree d. Then there exists a constant $c(\alpha) > 0$ such that for all $p/q \in \mathbb{Q}$ with $p/q \neq \alpha$ and $q > 0$ we have*

$$\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha)}{q^d}.$$

Liouville's Theorem can be used to prove that a given real number is transcendental by showing that it cannot be algebraic of any degree (as the next example demonstrates). In this sense, it was the first criterion to decide transcendence. The numbers to which this criterion applies are called *Liouville numbers.*

Example 3.4. *This example is attributed to Liouville: let*

$$\xi = \sum_{i=1}^{\infty} 2^{-i!}.$$

The claim is that ξ is transcendental. Define

$$p(k) = 2^{k!}\sum_{i=1}^{k} 2^{-i!}, \qquad q(k) = 2^{k!}.$$

Thus,

$$\left|\xi - \frac{p(k)}{q(k)}\right| = \sum_{i=k+1}^{\infty} 2^{-i!} < 2 \cdot 2^{-(k+1)!} = \frac{2}{q(k)^{k+1}}.$$

If we assume ξ is algebraic of degree d for some $d \in \mathbb{Z}_{>0}$, then by Liouville's Theorem there exists a constant $c(\xi) > 0$ such that

$$\left|\xi - \frac{p}{q}\right| > \frac{c(\xi)}{q^d}$$

for all rationals p/q. But for k large enough,

$$\left|\xi - \frac{p(k)}{q(k)}\right| < \frac{2}{q(k)^{k+1}} < \frac{c(\xi)}{q^d}$$

which means that by the same theorem, ξ cannot be algebraic of degree d, and hence must be transcendental.

3.3 Approximation to a real number by quadratic irrationals

3.3.1 Introduction

In 1961, Wirsing [27] proved the following statement.

Theorem 3.5 (Wirsing). *For any $\epsilon > 0$ and any real ξ which is not algebraic of degree less than or equal to k, there exists infinitely many real algebraic numbers α of degree at most k such that*

$$|\xi - \alpha| \leq H(\alpha)^{-(k+3)/2+\epsilon}.$$

Wirsing also pondered whether the optimal exponent in the above theorem is $k+1$, not $(k+3)/2$. Schmidt conjectured it true. For $n = 1$, we get Dirichlet's Theorem. The case $n = 2$ was proved by Davenport & Schmidt [8] in 1967.

Theorem 3.6 (Davenport & Schmidt). *Let $\xi \in \mathbb{R}$ with $[\mathbb{Q}(\xi) : \mathbb{Q}] > 2$. Then there exists infinitely many rational or real quadratic irrational numbers α such that*

$$|\xi - \alpha| < CH(\alpha)^{-3}$$

where

$$C := \begin{cases} C_0 & if \quad |\xi| < 1, \\ C_0\xi^2 & if \quad |\xi| > 1, \end{cases}$$

and $C_0 > \frac{160}{9}$.

We slightly modify the approach of Davenport and Schmidt to prove this result. The fact that this theorem is optimal will be proved in the following chapter.

Remark 3.7. *Suppose $0 < \xi < 1$. Let $\alpha \in \mathbb{R}$ with $[\mathbb{Q}(\xi) : \mathbb{Q}] \leq 2$ be an approximation to ξ satisfying Theorem 3.6, i.e.,*

$$|\xi - \alpha| < CH(\alpha)^{-3}.$$

Define $\xi' = 1/\xi$ and $\alpha' = 1/\alpha$. Clearly,

$$|\xi' - \alpha'| = |(\xi - \alpha)\xi'\alpha'|.$$

For a given $\epsilon > 0$ we have $|\alpha'| \leq (1+\epsilon)|\xi'|$ provided that $H(\alpha)$ is large enough. Since $H(\alpha) = H(\alpha')$ we deduce

$$|\xi' - \alpha'| < CH(\alpha)^{-3}|\xi'\alpha'| < C(1+\epsilon)|\xi'|^2 H(\alpha')^{-3}.$$

If C is a constant satisfying the theorem for $0 < \xi < 1$ then $C(1+\epsilon)\xi^2$ is a constant satisfying the theorem for $\xi > 1$. Similarly, if α is an approximation to ξ then $-\alpha$ is an approximation to $-\xi$. Hence it is enough to prove the theorem for $0 < \xi < 1$.

3.3.2 Proof of Theorem 3.6

Proof. Fix $\xi \in \mathbb{R}$ satisfying $[\mathbb{Q}(\xi) : \mathbb{Q}] > 2$ and $0 < \xi < 1$, and fix $C_0 > 160/9$. We prove this theorem by contradiction. Assume

$$|\xi - \alpha| \geq C_0 H(\alpha)^{-3}$$

for all rationals and real quadratic irrationals α of sufficiently large height.

Preliminary results

By Proposition 1.14, for all large X there exists a polynomial $P \in \mathbb{Z}[T]_{\leq 2}$ satisfying

$$H(P) \leq X \quad \text{and} \quad |P(\xi)| \leq \frac{4}{3}X^{-2}.$$

Therefore, for the norm $\phi(P) = |P(\xi)|$, the norm triplet $\big(\phi, (X_i)_{i\geq 1}, (P_i)_{i\geq 1}\big)$ in degree at most 2 satisfies

$$|P_i(\xi)| \leq \frac{4}{3}X_{i+1}^{-2} \qquad (i \gg 1). \tag{3.2}$$

If $\deg(P_i) = 1$ we can write $P_i(T) = p_{i,1}T + p_{i,0}$. Then the polynomial $TP_i(T) \in \mathbb{Z}[T]_{\leq 2}$ satisfies $H(TP_i) = X_i$ and

$$|p_{i,1}\xi + p_{i,0}| \geq |p_{i,1}\xi^2 + p_{i,0}\xi|$$

contradicting the choice of P_i. Thus, we have $\deg(P_i) = 2$ for all i. Define α_i to be the closest root of P_i to ξ. By hypothesis, for i large enough

$$|\xi - \alpha_i| \geq C_0 H(\alpha_i)^{-3}. \tag{3.3}$$

The following lemma will help us find a bound for $|P_i'(\xi)|$.

Lemma 3.8. *The discriminant of P_i is non-zero for i sufficiently large.*

Proof. Assume otherwise. Then $P_i(T) = \pm(uT - v)^2 = \pm L(T)^2$. Define $v/u = \alpha_i$. Since $0 < \xi < 1$, the fact that $|P_i(\xi)| = |u\xi - v|^2 < 1$ implies $|u| \geq |v|$ and $H(L) = H(\alpha_i) = |u|$. Then

$$\begin{aligned} |\xi - \alpha_i| =& \frac{|P_i(\xi)|^{1/2}}{|u|} \\ \leq& \sqrt{\frac{4}{3}} \frac{H(P_{i+1})^{-1}}{|u|} \\ \leq& \sqrt{\frac{4}{3}} \gamma \frac{H(L)^{-2}}{|u|} \\ =& \sqrt{\frac{4}{3}} \gamma H(\alpha_i)^{-3}. \end{aligned}$$

This contradicts (3.3) for sufficiently large i. □

Choose $0 < \epsilon < 1/3$ such that $160/9 < C_1 := (1+\epsilon)^{-1} C_0$. By (3.2) we have $|P_i(\xi)| \leq (4/3) H(P_{i+1})^{-2}$ for all $i \geq i_0$. This clearly implies that $|P_i(\xi)| \leq (\epsilon/4) H(P_i)^{-1}$ for $i \geq i_0$. Since the discriminant of P_i is non-zero for i sufficiently large, Lemma 1.30 tells us that there exists a root α_i of P_i satisfying

$$|\xi - \alpha_i| \leq (1+\epsilon) \frac{|P_i(\xi)|}{|P_i'(\xi)|} \qquad (i \gg 1).$$

Then using (3.3) we get

$$|P_i'(\xi)| < \frac{(1+\epsilon)}{C_0} H(\alpha_i)^3 |P_i(\xi)| \leq \frac{1}{C_1} X_i^3 |P_i(\xi)| \qquad (i \gg 1) \tag{3.4}$$

since $H(\alpha_i) \leq H(P_i)$ (from Lemma 1.28). Moreover, Lemma 2.7 states that we can find infinitely many i's such that P_{i-1}, P_i and P_{i+1} are linearly independent. For these i's, Lemma 1.41 gives

$$\begin{aligned}
1 \leq & \sum_{\sigma} X_{\sigma(i-1)} |P'_{\sigma(i)}(\xi)| |P_{\sigma(i+1)}(\xi)| \\
\leq & |P'_{i-1}(\xi)| \left(X_i |P_{i+1}(\xi)| + X_{i+1}|P_i(\xi)|\right) \\
& + |P'_i(\xi)| \left(X_{i-1}|P_{i+1}(\xi)| + X_{i+1}|P_{i-1}(\xi)|\right) \\
& + |P'_{i+1}(\xi)| \left(X_{i-1}|P_i(\xi)| + X_i|P_{i-1}(\xi)|\right) \\
\leq & 2X_i |P'_{i+1}(\xi)||P_{i-1}(\xi)| + 2X_{i+1}\left(|P'_i(\xi)||P_{i-1}(\xi)| + |P'_{i-1}(\xi)||P_i(\xi)|\right) \\
\leq & 2X_i |P'_{i+1}(\xi)||P_{i-1}(\xi)| + \frac{4}{C_1} X_i^3 |P_i(\xi)| X_{i+1} |P_{i-1}(\xi)| \qquad \text{by (3.4)} \\
\leq & 2X_i |P'_{i+1}(\xi)||P_{i-1}(\xi)| + \frac{64}{9C_1} \qquad \text{by (3.2)}
\end{aligned}$$

where σ runs through the set of permutations on the three symbols $\{i-1, i, i+1\}$. Thus

$$X_i |P'_{i+1}(\xi)||P_{i-1}(\xi)| > \frac{1}{2} - \frac{32}{9C_1} \tag{3.5}$$

whenever P_{i-1}, P_i and P_{i+1} are linearly independent.

Working out a contradiction

To complete the proof of Theorem 3.6, let m be large and such that P_{m-1}, P_m and P_{m+1} are linearly independent. Define $n > m$ to be the smallest integer for which P_{n-1}, P_n and P_{n+1} are also linearly independent. For all i with $m < i < n$, we have that P_{i-1}, P_i and P_{i+1} are linearly dependent, hence the vector space

$$\mathcal{V} = \langle P_m, P_{m+1}, \ldots, P_{n-1}, P_n \rangle_{\mathbb{Q}}$$

has dimension 2. Using Lemma 2.5 we know that the sets $\{P_{i-1}, P_i\}$ for $m+1 \leq i \leq n$ are bases for $\mathcal{V} \cap \mathbb{Z}[T]$. Thus we get

$$\langle P_m, P_{m+1} \rangle_{\mathbb{Z}} = \langle P_{n-1}, P_n \rangle_{\mathbb{Z}}$$

and

$$P_m = aP_{n-1} + bP_n, \qquad P_{m+1} = cP_{n-1} + dP_n$$

for $a, b, c, d \in \mathbb{Z}$ with $ad - bc = \pm 1$. Due to the multilinearity of the determinant,

$$\begin{aligned} \left|\det\left((T-\xi)^2, P_m, P_{m+1}\right)\right| =& |ad-bc|\left|\det\left((T-\xi)^2, P_{n-1}, P_n\right)\right| \\ =& \left|\det\left((T-\xi)^2, P_{n-1}, P_n\right)\right|. \end{aligned} \tag{3.6}$$

Estimating the determinant on the left hand side of equation (3.6) using relations (3.4) and (3.5) gives

$$\begin{aligned} \left|\det\left((T-\xi)^2, P_m, P_{m+1}\right)\right| =& |P'_{m+1}(\xi)P_m(\xi) - P'_m(\xi)P_{m+1}(\xi)| \\ \geq& |P'_{m+1}(\xi)||P_m(\xi)| - |P'_m(\xi)||P_{m+1}(\xi)| \\ \geq& \left(\frac{1}{2} - \frac{32}{9C_1}\right)\frac{|P_m(\xi)|}{X_m|P_{m-1}(\xi)|} - \frac{1}{C_1}X_m^3|P_m(\xi)||P_{m+1}(\xi)| \\ \geq& \frac{3}{4}\left(\frac{1}{2} - \frac{32}{9C_1}\right)X_m|P_m(\xi)| - \frac{4}{3C_1}X_m^3X_{m+2}^{-2}|P_m(\xi)| \\ \geq& \left(\frac{3}{8} - \frac{4}{C_1}\right)X_m|P_m(\xi)|. \end{aligned}$$

On the other hand, using Lemma 1.41 together with (3.2) and (3.4) we find

$$\begin{aligned} \left|\det\left((T-\xi)^2, P_{n-1}, P_n\right)\right| \leq& |P'_{n-1}(\xi)||P_n(\xi)| + |P'_n(\xi)||P_{n-1}(\xi)| \\ \leq& \frac{1}{C_1}|P_{n-1}(\xi)||P_n(\xi)|(X_{n-1}^3 + X_n^3) \\ \leq& \frac{4}{3C_1}X_n^{-2}|P_n(\xi)|(X_{n-1}^3 + X_n^3) \\ \leq& \frac{8}{3C_1}X_n|P_n(\xi)|. \end{aligned}$$

Thus, equation (3.6) now reads

$$\left(\frac{3}{8} - \frac{4}{C_1}\right)X_m|P_m(\xi)| < \frac{8}{3C_1}X_n|P_n(\xi)|$$

or, since $C_1 \geq 160/9$,

$$X_m|P_m(\xi)| < X_n|P_n(\xi)|$$

for $n > m$. But this is impossible since it gives us an infinite sequence of n for which $X_n|P_n(\xi)|$ increases, while by (3.2), $X_n|P_n(\xi)| \to 0$ as $n \to \infty$. We have a contradiction, i.e., for all $H \geq 1$, there exists a real number α such that $H(\alpha) \geq H$ and

$$|\xi - \alpha| \leq C_0 H(\alpha)^{-3}.$$

As H goes to infinity, we have found an infinitude of such α. □

3.4 Approximation to real numbers by algebraic integers

3.4.1 Introduction

To continue our study of Diophantine Approximation we change the problem of the previous section slightly. Now we want to approximate a real number by algebraic integers of degree at most 3. To be precise, we want to prove the following theorem (recalling that $\gamma = (1+\sqrt{5})/2$).

Theorem 3.9 (Davenport & Schmidt). *Suppose $\xi \in \mathbb{C}$ is such that $[\mathbb{Q}(\xi) : \mathbb{Q}] > 2$. Then there exists infinitely many algebraic integers α with* $\deg(\alpha) \leq 3$ *such that*

$$0 < |\xi - \alpha| \ll H(\alpha)^{-1-\gamma}.$$

The problem of approximating a real number ξ by algebraic integers of degree $n+1$ is related to the problem of simultaneous approximations of the n first powers of ξ by rational numbers with the same denominator. In the case $n = 2$, we need the following intermediate result.

Theorem 3.10 (Davenport & Schmidt). *Suppose $\xi \in \mathbb{C}$ is such that $[\mathbb{Q}(\xi) : \mathbb{Q}] >$ 2. Then there are arbitrary large values of $X \in \mathbb{R}$ such that, for a suitable constant*

$c = c(\xi)$, the inequalities

$$|x_0| < X, \qquad |x_0\xi - x_1| < cX^{1-\gamma}, \qquad |x_0\xi^2 - x_2| < cX^{1-\gamma}$$

have no non-zero solution $(x_0, x_1, x_2) \in \mathbb{Z}^3$.

Roy [17] showed that the exponent $\gamma - 1 = 1/\gamma = 0.618\ldots$ in this statement is optimal against the natural conjecture that it should be $1/n$ in degree n.

Remark 3.11. *It is clear that if $(x_0, x_1, x_2) \in \mathbb{Z}^3$ is a non-zero solution of the system of equations in Theorem 3.10 and X is sufficiently large then $x_0 \neq 0$.*

In fact, as will be seen below, Theorem 3.10 implies Theorem 3.9. For this reason, the dual problem is proved first. We follow the lead of Davenport and Schmidt [9] to prove the two theorems. Before going on, we need the following proposition.

Proposition 3.12. *Let $\xi \in \mathbb{C}$ be such that $[\mathbb{Q}(\xi) : \mathbb{Q}] > 2$. The following are equivalent:*

1. *There exists $c > 0$ such that, for arbitrary large X, the system*

$$|x_0| \leq X, \qquad |x_0\xi - x_1| \leq cX^{1-\gamma}, \qquad |x_0\xi^2 - x_2| \leq cX^{1-\gamma}$$

   has a solution $(x_0, x_1, x_2) \in \mathbb{Z}^3$ with $x_0 \neq 0$.

2. *There exists $c' > 0$ such that, for arbitrary large X, the conditions*

$$H(Q) \leq X, \qquad |Q(\xi)| \leq c'X^{1-\gamma}, \qquad |Q'(\xi)| \leq c'X^{1-\gamma}$$

   are satisfied by a non-zero integral polynomial $Q(T) = q_2T^2 + 2q_1T + q_0$ of degree exactly 2.

Proof. Assume $(x_0, x_1, x_2) \in \mathbb{Z}^3$ with $x_0 \neq 0$ is a non-zero solution to

$$|x_0| \leq X, \qquad |x_0\xi - x_1| \leq cX^{1-\gamma}, \qquad |x_0\xi^2 - x_2| \leq cX^{1-\gamma}.$$

Then defining $Q(T) = x_0T^2 - 2x_1T + x_2$, for X sufficiently large we get

$$\begin{aligned} H(Q) &= \max\{x_0, x_1, x_2\} \leq \max\{X, cX^{1-\gamma} + \xi X, cX^{1-\gamma} + \xi^2 X\} \leq X \\ |Q(\xi)| &= |2\xi(x_0\xi - x_1) - (x_0\xi^2 - x_2)| \leq c'X^{1-\gamma}, \\ |Q'(\xi)| &= |2x_0\xi - 2x_1| =\leq c'X^{1-\gamma} \end{aligned}$$

for $c' = \max\{(2|\xi| + 1)c, 2c\}$. Conversely, assume there exists a non-zero integral polynomial $Q(T) = x_0T^2 - 2x_1T + x_2$ with $x_0 \neq 0$ satisfying

$$H(Q) \leq X, \qquad |Q(\xi)| \leq c'X^{1-\gamma}, \qquad |Q'(\xi)| \leq c'X^{1-\gamma}.$$

Then clearly

$$|x_0| \leq X, \qquad |x_0\xi - x_1| \leq \frac{c'}{2}X^{1-\gamma}$$

and

$$|x_0\xi^2 - x_2| \leq |Q(\xi)| + 2|\xi||x_0\xi - x_1| \leq (1 + |\xi|)c'X^{1-\gamma}.$$

Thus, for $c = (1 + |\xi|)c'$ we have that the triplet $(x_0, x_1, x_2) \in \mathbb{Z}^3$ with $x_0 \neq 0$ satisfies

$$|x_0| \leq X, \qquad |x_0\xi - x_1| \leq cX^{1-\gamma}, \qquad |x_0\xi^2 - x_2| \leq cX^{1-\gamma}.$$

□

3.4.2 Proof of Theorem 3.10

Proof. We prove the theorem by contradiction. Fix $\xi \in \mathbb{C}$ with $[\mathbb{Q}(\xi) : \mathbb{Q}] > 2$. Using Proposition 3.12 we transfer the problem at hand to the equivalent problem of polynomials. Fix $c > 0$. Suppose, for all sufficiently large real number X, there exists an integral polynomial $Q \in \mathbb{Z}[T]_{\leq 2}$ with

$$H(Q) \leq X \quad \text{and} \quad \phi(Q) = \max\{|Q(\xi)|, |Q'(\xi)|\} \leq cX^{1-\gamma}. \tag{3.7}$$

Fix a norm triplet $(\phi, (X_i)_{i\geq 1}, (P_i)_{i\geq 1})$ in degree at most 2. Then (3.7) implies

$$|Q_i(\xi)| \leq cX_{i+1}^{1-\gamma}, \qquad |Q_i'(\xi)| \leq cX_{i+1}^{1-\gamma}. \tag{3.8}$$

Since

$$\lim_{i\to\infty} X_i^{1/2}\phi(Q_i) \le \lim_{i\to\infty} cX_i^{1/2}X_i^{1-\gamma} = 0$$

we can use Lemma 2.10 which tells us

$$(8+2|\xi|)^{-1}X_i^{-1} \le \phi(Q_i) \le cX_{i+1}^{1-\gamma} \tag{3.9}$$

for sufficiently large i. Consider such a large i for which Q_{i-1}, Q_i and Q_{i+1} are linearly independent. (There exists infinitely many such i by Lemma 2.7.) Then Lemma 1.41 gives us the inequality

$$1 \le \sum_\sigma H(Q_{\sigma(i-1)})|Q_{\sigma(i)}(\xi)||Q'_{\sigma(i+1)}(\xi)| \le \sum_\sigma c^2 X_{\sigma(i-1)}X_{\sigma(i)+1}^{1-\gamma}X_{\sigma(i+1)+1}^{1-\gamma} \tag{3.10}$$

for σ running through the set of permutations on the three symbols $\{i-1, i, i+1\}$. Estimating (3.10) using crude upper bounds gives $1 \le 6c^2X_{i+1}^{2-\gamma}X_i^{1-\gamma}$, which can also be written as

$$X_i^{\gamma-1} \le 6c^2X_{i+1}^{2-\gamma}. \tag{3.11}$$

Together, (3.9) and (3.11) give us

$$X_i^{(\gamma-1)^2} \le (6c^2)^{\gamma-1}X_{i+1}^{(2-\gamma)(\gamma-1)} \le (6c^2)^{\gamma-1}\big(c(8+2|\xi|)\big)^{2-\gamma}X_i^{2-\gamma} \tag{3.12}$$

for infinitely many i. Since $(1-\gamma)^2 = 2-\gamma$, (3.12) implies that

$$1 \le (6c^2)^{\gamma-1}\big(c(8+2|\xi|)\big)^{2-\gamma}$$

which is impossible for c sufficiently small. □

3.4.3 Proof of Theorem 3.9

To prove Theorem 3.9 we need the following lemma.

Lemma 3.13. *Let $\xi \in \mathbb{R}$, $\lambda \in \mathbb{R}_{>0}$ and $n \in \mathbb{Z}_{\geq 2}$. Suppose, for some $c > 0$, there exists arbitrarily large values of X such that the convex body*

$$\mathcal{C} := \begin{cases} |x_0| \leq X, \\ |x_0\xi^i - x_i| \leq cX^{-\lambda} \qquad (1 \leq i \leq n-1) \end{cases}$$

contains no non-zero point $\mathbf{x} = (x_0, \dots, x_{n-1}) \in \mathbb{Z}^n$. Then there are infinitely many algebraic integers α of degree at most n such that

$$0 < |\xi - \alpha| \ll H(\alpha)^{-1-1/\lambda}.$$

Proof. Assume, without loss of generality, that $c < 1$ and define $Y = c^{-1}X^{\lambda}$. Let $\Lambda = \mathbb{Z}^n$ be the integer-point lattice of $\mathbb{R}^n$. Let $X \geq 1$ be large enough so that the convex body $\mathcal{C}$ above contains no non-zero point $(x_0, \dots, x_{n-1}) \in \mathbb{Z}^n$. By definition, the first minimum of $\mathcal{C}$ satisfies $\lambda_1(\mathcal{C}) \geq 1$. Using Proposition 1.20, we get that the convex body $\mathcal{D}$ defined by

$$\mathcal{D} := \begin{cases} |x_{n-1}\xi^{n-1} + \cdots + x_1\xi + x_0| \leq X^{-1}, \\ |x_i| \leq Y \qquad (1 \leq i \leq n-1) \end{cases}$$

satisfies $(1/n)\mathcal{C}^* \subset \mathcal{D} \subset \mathcal{C}^*$. Using Mahler's Theorem (Theorem 1.18), $\lambda_n(\mathcal{C}^*) \leq n!$ and in particular, there exist n linearly independent integer points in the convex body $\lambda_n(\mathcal{C}^*)n\mathcal{D}$. This means that it is possible to find n linearly independent polynomials $\{P_1, P_2, \dots, P_n\} \in \mathbb{Z}[T]_{\leq n-1}$ satisfying

$$|P_i(\xi)| \leq nn!X^{-1}$$

and having coefficients of absolute value at most Y, except maybe for the constant one. Thus, these polynomials must also satisfy

$$H(P_i) \leq nn!(1 + |\xi| + \cdots + |\xi|^{n-1})Y,$$
$$|P_i'(\xi)| \leq nn!(1 + 2|\xi| + \cdots + (n-1)|\xi|^{n-2})Y.$$

Define the polynomial

$$Q(T) = (T-\xi)^n + n^2 n!(2 + 2|\xi| + \cdots + (n-1)|\xi|^{n-1})Y(T-\xi).$$

Then Q is monic of degree n and $Q(\xi) = 0$. Thus, there must exist constants $\{\theta_1, \theta_2, \ldots, \theta_n\} \subset \mathbb{R}$ such that $Q(T) = T^n + \theta_1 P_1(T) + \cdots + \theta_n P_n(T)$. Define

$$P(T) = T^n + [\theta_1]P_1(T) + \cdots + [\theta_n]P_n(T).$$

By construction

$$\begin{aligned} H(P) &\leq H(Q) + \sum_{i=1}^{n} H(P_i) \ll Y, \\ |P(\xi)| &\leq \sum_{i=1}^{n} |P_i(\xi)| \leq n^2 n! X^{-1}, \\ |P'(\xi)| &\geq |Q'(\xi)| - \sum_{i=1}^{n} |P_i'(\xi)| = n^2 n! Y. \end{aligned}$$

Let $\{\alpha_1, \ldots, \alpha_n\}$ the roots of $P(T)$. So

$$H(\alpha_i) \ll H(P) \ll Y \qquad (1 \leq i \leq n)$$

and Lemma 1.29 tells us that

$$\begin{aligned} \min_{\{i=1,\ldots,n\}} \{|\xi - \alpha_i|\} &\leq n \frac{|P(\xi)|}{|P'(\xi)|} \\ &\leq n(YX)^{-1} \\ &\ll H(\alpha_i)^{-1-1/\lambda}. \end{aligned}$$

By varying X we get infinitely many α satisfying the above relation. □

We are now ready to prove Theorem 3.9.

Proof of Theorem 3.9. Let $\xi \in \mathbb{C}$ such that $[\mathbb{Q}(\xi) : \mathbb{Q}] > 2$. Theorem 3.10 then states that there exists arbitrary large values of $X \in \mathbb{R}$ such that for a suitable constant $c > 0$ the inequalities

$$|x_0| < X, \qquad |x_0\xi - x_1| < cX^{1-\gamma}, \qquad |x_0\xi^2 - x_2| < cX^{1-\gamma}$$

have no non-zero solution $(x_0, x_1, x_2) \in \mathbb{Z}^3$. Then using Lemma 3.13, we know that there exists infinitely many algebraic integers α of degree at most 3 satisfying

$$0 < |\xi - \alpha| \ll H(\alpha)^{-\gamma^{-1}},$$

hence proving Theorem 3.9 □

3.5 A Gel'fond type criterion in degree 2

3.5.1 Introduction

In this section, we develop another criterion to decide if a given complex number ξ is algebraic of degree at most two. This time, we do not compare ξ to algebraic numbers, but rather study the value of polynomials of degree at most 2 at the point ξ. The work below is part of a joint paper with Roy [2]. The theorem we wish to prove is

Theorem 3.14. *Let $\xi \in \mathbb{C}$. Assume that for any sufficiently large $X \in \mathbb{Z}_{>0}$ there exists a nonzero polynomial $P(T) \in \mathbb{Z}[T]_{\leq 2}$ such that*

$$H(P) \leq X \quad \textit{and} \quad |P(\xi)| \leq \frac{1}{4} X^{-\gamma^2}.$$

Then $[\mathbb{Q}(\xi) : \mathbb{Q}] \leq 2$.

3.5.2 Proof of Theorem 3.14

Proof. Assume $[\mathbb{Q}(\xi) : \mathbb{Q}] > 2$. Fix $c > 0$ and assume that, for any sufficiently large number X, there exists a non-zero polynomial $P \in \mathbb{Z}[T]_{\leq 2}$ satisfying

$$H(P) \leq X \quad \text{and} \quad |P(\xi)| \leq cX^{-\gamma^2}. \tag{3.13}$$

Define the norm $\phi(P) = |P(\xi)|$ for $P \in \mathbb{Z}[T]$ and fix a norm triplet $\big(\phi, (X_i)_{i\geq 1}, (P_i)_{i\geq 1}\big)$ in degree at most 2. Thus, (3.13) necessarily means that

$$|P_i(\xi)| \leq cX_{i+1}^{-\gamma^2} < cX_i^{-\gamma^2} \qquad (i \gg 1).$$

Let $c_1 > c$. Since Lemma 2.7 states that P_{i-1}, P_i and P_{i+1} are linearly independent over $\mathbb{Q}$ for infinitely many i, for such large i Lemma 1.40 now states

$$\begin{aligned}
1 \leq& 2X_{i-1}X_iX_{i+1}\left(\frac{|P_{i-1}(\xi)|}{X_{i-1}} + \frac{|P_i(\xi)|}{X_i} + \frac{|P_{i+1}(\xi)|}{X_{i+1}}\right)\\
\leq& 4X_{i-1}X_{i+1}|P_i(\xi)| + 2X_iX_{i+1}|P_{i-1}(\xi)|\\
\leq& 4cX_{i-1}X_{i+1}^{-\gamma} + 2cX_i^{-\gamma}X_{i+1}\\
\leq& 4cX_{i+1}^{-1/\gamma} + 2cX_i^{-\gamma}X_{i+1}
\end{aligned}$$

meaning that

$$\frac{1-o(1)}{X_{i+1}} \leq 2cX_i^{-\gamma}.$$

Thus, for large i we get the estimate

$$X_i^{\gamma} \leq 2c_1X_{i+1}. \tag{3.14}$$

We need another inequality relating X_i and X_{i+1}. Assume P_i and P_{i+1} have a common root $z \in \mathbb{C}$. This root necessarily must be in $\mathbb{Q}$ since $P \in \mathbb{Z}[T]_{\leq 2}$ and we denote it by m/n. Then

$$P_i(T) = L(T)Q(T), \qquad P_{i+1}(T) = L(T)R(T)$$

where $L(T) = \gcd(P_i, P_{i+1}) = (nT - m)$ and $n \leq H(L) \leq H(P_i) = X_i$ by Lemma 1.28. But Lemma 1.39 then tells us that

$$|n\xi - m| \leq \frac{c\gamma}{H(L)}\left(X_iX_{i+1}^{-\gamma^2} + X_{i+1}X_{i+2}^{-\gamma^2}\right) \leq \frac{2c\gamma X_{i+1}^{-\gamma}}{H(L)}$$

which is smaller than 1 for i sufficiently large. In particular, we have $|\xi - m/n| < 1$. We can now use Corollary 1.32 to estimate the integer $n^2P_{i-1}(m/n)$:

$$\begin{aligned}\left|n^2P_{i-1}\left(\frac{m}{n}\right)\right| \leq & nH(L)\left(|P_{i-1}(\xi)| + \left|P_{i-1}(\frac{m}{n}) - P_{i-1}(\xi)\right|\right) \\ \leq & nH(L)\left(cX_i^{-\gamma^2} + (2|\xi|+2)\left|\frac{m}{n} - \xi\right| H(P_{i-1})\right) \\ \leq & cX_i^{1-\gamma^2} + nH(L)(2|\xi|+2)\frac{2\gamma cX_{i+1}^{-\gamma}}{nH(L)}H(P_{i-1}) \\ \leq & cX_i^{-\gamma} + 2\gamma c(2|\xi|+2)X_{i+1}^{-\gamma}X_{i-1} \\ \leq & \big(c + 2\gamma c(2|\xi|+2)\big)X_i^{1-\gamma}\end{aligned}$$

which is again smaller than 1 for i large enough. Thus, m/n must be a root of P_{i-1}. That is to say P_{i-1}, P_i and P_{i+1} are linearly dependent, contradicting the hypothesis on the choice of i. Thus, two consecutive polynomials of sufficiently large index have no common root in $\mathbb{Q}$. For large i the resultant of P_i and P_{i+1} is therefore a non-zero integer, and using Lemma 1.37 we have

$$\begin{aligned} 1 &\leq |\operatorname{Res}(P_i, P_{i+1})| \\ &\leq 6X_iX_{i+1}\big(cX_iX_{i+2}^{-\gamma^2} + cX_{i+1}^{-\gamma}\big) \\ &\leq 6cX_iX_{i+1}^{1-\gamma}(1+o(1)).\end{aligned}$$

We now have a second estimate

$$1 \leq 6c_1X_iX_{i+1}^{-1/\gamma} \tag{3.15}$$

for i large enough.

To conclude, we combine (3.14) and (3.15) to get

$$1 \leq 6c_1X_iX_{i+1}^{-1/\gamma} \leq 6c_1(2c_1)^{1/\gamma}$$

and therefore $c_1 \geq (6\cdot 2^{1/\gamma})^{-1/\gamma}$. In particular, this means that if $c = \frac{1}{4} < (6\cdot 2^{1/\gamma})^{-1/\gamma}$ then $[\mathbb{Q}(\xi) : \mathbb{Q}] \leq 2$. □

Chapter 4

Optimality of the exponents

4.1 Introduction

This chapter is devoted to another important question of Diophantine Approximation: how sharp are our estimates? This is a legitimate question since mathematicians always search for more precise results. Can we get better criteria? The answer is no for Theorem 3.6 and Theorem 3.14 with respect to the approximation exponents. The optimality of these criteria is shown in this chapter.

4.2 Approximation to a real number by quadratic irrationals

We start our study by showing that the exponent of approximation in Theorem 3.6 is the best possible exponent. The following theorem does so.

Theorem 4.1. *Let* $\epsilon > 0$. *Then there exists a real transcendental number* ξ *such that, for all algebraic numbers* α *with* $\deg(\alpha) \leq 2$, *we have*

$$|\xi - \alpha| \geq H(\alpha)^{-3-\epsilon}.$$

Proof. Let

$$\mathcal{P}_X = \{P \in \mathbb{Z}[T]_{\leq 2} | H(P) = X \text{ and } P \text{ is irreducible}\}.$$

Since the number of polynomials of height X is the difference in the number of polynomials of height at most X and the number of polynomials of height at most $X - 1$ we get,

$$| \mathcal{P}_X |= (2X+1)^3 - (2X-1)^3 = 24X^2 + 2.$$

Let $B(\alpha, r)$ be the open ball of radius $r > 0$ around $\alpha \in \mathbb{C}$ and let μ be the Lebesgue measure on $\mathbb{R}$. We will calculate

$$\mu\left(\bigcup_{X=1}^{\infty} \bigcup_{P \in \mathcal{P}_X} \bigcup_{P(\alpha)=0} (B(\alpha, X^{-3-\epsilon}) \cap \mathbb{R})\right),$$

which is the measure of the set of real numbers within radius $X^{-3-\epsilon}$ about an algebraic number of degree at most 2 and height at most X. We recall that for countably many sets $A_1, A_2, \cdots \subset \mathbb{R}$ we have $\mu(A_1 \cup A_2 \cup \dots) \leq \sum_{i=1}^{\infty} \mu(A_i)$. Then

$$\begin{aligned}
&\mu\left(\bigcup_{X=1}^{\infty} \bigcup_{P \in \mathcal{P}_X} \bigcup_{P(\alpha)=0} (B(\alpha, X^{-3-\epsilon}) \cap \mathbb{R})\right) \\
&\leq \sum_{X=1}^{\infty} \mu\left(\bigcup_{P \in \mathcal{P}_X} \bigcup_{P(\alpha)=0} (B(\alpha, X^{-3-\epsilon}) \cap \mathbb{R})\right) \\
&\leq \sum_{X=1}^{\infty} 2(24X^2+2)\left(2X^{-3-\epsilon}\right) \\
&\ll \sum_{X=1}^{\infty} X^{-1-\epsilon} \\
&< \infty.
\end{aligned}$$

Thus, there exists $\xi \in \mathbb{R} \setminus \overline{\mathbb{Q}}$ which is more than $X^{-3-\epsilon}$ away from all algebraic numbers α. This proves the theorem. □

4.3 A Gel'fond type criterion in degree 2

We now show the optimality of the approximation exponent in Theorem 3.14. This is done by constructing a real number ξ which is transcendental and satisfies the main hypothesis of Theorem 3.14 provided that the constant 1/4 is replaced by a slightly larger number (in this case 1.27.) Thus, the theorem is an optimal criterion to decide whether a number is algebraic of degree at most 2, up to the value of the constant.

Theorem 4.2. *There exists a real transcendental number ξ such that for all sufficiently large real number $X > 0$ there exists a non-zero polynomial $P \in \mathbb{Z}[T]_{\leq 2}$ satisfying*

$$H(P) \leq X \quad \textit{and} \quad |P(\xi)| \leq 1.27X^{-\gamma^2}.$$

4.3.1 Introduction to continued fractions

For a more detailed exposition of continued fractions see [21, Chapter 1].

Let $\xi \in \mathbb{R} \setminus \mathbb{Q}$. Then ξ can be written as $\xi = i_0 + r_0$ where $i_0 = [\xi]$ is the integer part of ξ and $r_0 = \{\xi\}$ is its fractional part. Since $1/r_0 > 1$, applying the same procedure gives

$$\xi = i_0 + \frac{1}{i_1 + r_1},$$

where $i_1 = [1/r_0]$ and $r_1 = \{1/r_0\}$. Following this pattern, we get formally

$$\xi = i_0 + \cfrac{1}{i_1 + \cfrac{1}{i_2 + \dots}}. \tag{4.1}$$

Expression (4.1) is called the *continued fraction expansion of* ξ and is denoted by

$$\xi = [i_0, i_1, i_2, \dots].$$

Definition 4.3. We define the *j-th convergent of* ξ to be

$$\frac{p_j}{q_j} = [i_0, i_1, \dots, i_j] = i_0 + \cfrac{1}{i_1 + \cfrac{1}{\dots + \cfrac{1}{i_j}}}.$$

Convergents hold very important information as the next lemma shows. For a proof, see [21, Lemma 4A, p.11] and [21, Lemma 4D, p.14].

Lemma 4.4. *Let $\xi \in \mathbb{R} \setminus \mathbb{Q}$ and let p_i/q_i be the i-th convergent of ξ. Then the sequences $(p_i)_{i\geq 1}$ and $(q_i)_{i\geq 1}$ are strictly increasing and for $n \geq 0$*

$$\left|\xi - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2}.$$

Moreover,

$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \dots < \xi < \dots < \frac{p_3}{q_3} < \frac{p_1}{q_1}.$$

In particular, Lemma 4.4 shows that

$$\lim_{i\to\infty} \frac{p_i}{q_i} = \xi.$$

Lemma 4.5. *Let $\xi \in \mathbb{R}\setminus\mathbb{Q}$ with $0 < \xi < 1$ and let $\xi = [0, a_1, a_2, \dots]$ be its continued fraction expansion. Denote the j-th convergent of ξ by p_j/q_j. Then*

$$\begin{pmatrix} q_j & q_{j-1} \\ p_j & p_{j-1} \end{pmatrix} = \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_2 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_j & 1 \\ 1 & 0 \end{pmatrix}.$$

Proof. This follows by induction based on the recurrence relations

$$p_i = a_i p_{i-1} + p_{i-2} \quad \text{and} \quad q_i = a_i q_{i-1} + q_{i-2}$$

for $i \geq 2$. □

For the proof of the next lemma, see [21, Lemma 3B, p.9].

Lemma 4.6. *Let $\xi \in \mathbb{R} \setminus \mathbb{Q}$ with $0 < \xi < 1$. Let $\xi = [0, a_1, a_2, \dots]$ be its continued fraction expansion and let p_k/q_k be the k-th convergent of ξ. Then*

$$\xi = \frac{p_k t + p_{k-1}}{q_k t + q_{k-1}}$$

for $t = [a_{k+1}, a_{k+2}, \dots]$.

4.3.2 A particular type of continued fractions

The next sections are based on and are a continuation for Roy [17], [18] and [19]. Let $E = \{a, b\}$ with $a \neq b$ and let E^* be the monoid of the words on E with word concatenation as product. We define the Fibonacci sequence in E^* as the sequence $(w_i)_{i \geq 0}$ of words defined by

$$w_0 = b, \qquad w_1 = a, \qquad w_i = w_{i-1} w_{i-2} \quad (i \geq 2).$$

Since w_{i-1} is the prefix of w_i, the sequence $(w_i)_{i \geq 0}$ converges to an infinite word

$$w = w_1 w_2 \cdots = abaaba \dots$$

called the *Fibonacci word on the alphabet* $\{a, b\}$. Using this word, we define the Fibonacci number on two positive distinct integers $\{a, b\}$ as

$$\xi_{a,b} = [0, w] = [0, a, b, a, a, b, a, \dots].$$

The real number $\xi_{a,b}$ constructed in this manner is a type of Sturmian continued fraction, which were proved to be transcendental by Allouche, Davison, Queffélec and Zamboni [1]. The following property of the Fibonacci word is due to J. Berstel.

Lemma 4.7. *For $i \geq 1$, the word m_i formed by taking the word w_{i+2} and deleting the last two letters is a palindrome. Moreover, if we define*

$$s_i = \begin{cases} ab & i \text{ even} \\ ba & i \text{ odd} \end{cases}$$

then

$$m_0 = \varnothing, \qquad m_1 = a, \qquad m_2 = aba, \qquad m_i = m_{i-1}s_{i-1}m_{i-2} \quad (i \geq 3).$$

Proof. By recursion on i, it is clear that $w_i = w_{i-1}w_{i-2}$ finishes with s_i for $i \geq 2$. It is also clear that m_i is a palindrome for $i = 1, 2, 3$. Now assume m_j is a palindrome for $j = 1, \ldots, i-1$ where $i \geq 4$. By definition,

$$m_i = m_{i-1}s_{i-1}m_{i-2} = m_{i-2}s_{i-2}m_{i-3}s_{i-1}m_{i-2}$$

which is a palindrome since s_{i-1} and s_{i-2} are opposites. □

4.3.3 Study of the Fibonacci continued fraction

We now study the properties of the number $\xi_{a,b}$ constructed above. For the remainder of this section, fix $a, b \in \mathbb{Z}_{>0}$, let $\xi = \xi_{a,b}$ and put $\Theta = 1 + ab + (a+b)\xi + \xi^2$. Defining

$$A = \begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} b & 1 \\ 1 & 0 \end{pmatrix},$$

there exists a unique homomorphism of monoids $\Phi : E^* \longrightarrow \mathrm{GL}_2(\mathbb{Z})$ such that

$$\Phi(a) = A, \qquad \Phi(b) = B.$$

We use this to simplify the proofs.

Lemma 4.8. *There exists a sequence of points* $(\mathbf{x}_i)_{i\geq 1} = \big((x_{i,0}, x_{i,1}, x_{i,2})\big)_{i\geq 1} \subset \mathbb{Z}^3$ *such that*

1. $x_{i,2}/x_{i,1}$ *and* $x_{i,1}/x_{i,0}$ *are consecutive convergents of* ξ.

2. $0 \leq x_{i,2} \leq x_{i,1} \leq x_{i,0} \quad (i \geq 1)$,

3. $(X_i)_{i\geq 1} = (x_{i,0})_{i\geq 1}$ *is an increasing sequence of positive integers,*

4. $\det(\mathbf{x}_i) = x_{i,0}x_{i,2} - x_{i,1}^2 = \pm 1 \quad (i \geq 1)$,

Proof. Let $m_i = [a, b, a, \ldots, c]$, where $c = a$ or b, be as in Lemma 4.7. Define

$$\begin{pmatrix} x_{i,0} & x_{i,1} \\ x_{i,1} & x_{i,2} \end{pmatrix} = \Phi(m_i) = ABA \ldots C.$$

Then Lemma 4.5 tells us $x_{i,2}/x_{i,1}$ and $x_{i,1}/x_{i,0}$ are consecutive convergents of ξ. From Lemma 4.4, we know that the sequences of numerators and denominators of convergents are increasing and thus we get $0 \leq x_{i,2} \leq x_{i,1} \leq x_{i,0}$. Moreover, since $x_{i,0}$ is the numerator of a convergent, Lemma 4.4 implies that $(x_{i,0})_{i\geq 1}$ is an increasing sequence.

To conclude, $\det(A) = \det(B) = -1$ and $\det(\mathbf{x}_i) = \det(ABA \ldots C) = \pm 1$. □

Theorem 4.9. *Fix $\epsilon > 0$. Let $\big((x_{i,0}, x_{i,1}, x_{i,2})\big)_{i\geq 1} \subset \mathbb{Z}^3$ and $(X_i)_{i\geq 1}$ be the sequences defined in Lemma 4.8. Then for $i \geq i_0(\epsilon)$*

1. $\max_{j=1,2}\{|x_{i,0}\xi^j - x_{i,j}|\} < (\xi + \frac{1}{\xi} + \epsilon)X_i^{-1}$,

2. $\Theta - \epsilon < \frac{X_i}{X_{i-1}X_{i-2}} < \Theta + \epsilon$,

3. $(\Theta - \epsilon)^{1/\gamma}X_{i-1}^{\gamma} < X_i < (\Theta + \epsilon)^{1/\gamma}X_{i-1}^{\gamma}$,

4. $|\det(\mathbf{x}_i, \mathbf{x}_{i+1}, \mathbf{x}_{i+2})| = |b - a|$.

Proof. 1.) By construction of the sequence $\big((x_{i,0}, x_{i,1}, x_{i,2})\big)_{i\geq 1}$ we have that $x_{i,2}/x_{i,1}$ and $x_{i,1}/x_{i,0}$ are consecutive convergents of ξ. Thus, using Lemma 4.4,

$$|x_{i,0}\xi - x_{i,1}| \leq \frac{1}{x_{i,0}}, \qquad |x_{i,1}\xi - x_{i,2}| \leq \frac{1}{x_{i,1}}.$$

Doing arithmetic on the previous two equations gives, for sufficiently large i, that

$$\max_{j=1,2}\{|x_{i,0}\xi^j - x_{i,j}|\} \leq \max\left\{\frac{1}{x_{i,0}}, \frac{\xi}{x_{i,0}} + \frac{1}{x_{i,1}}\right\} \leq (\xi + \frac{1}{\xi} + \epsilon)X_i^{-1}.$$

2.) Under the correspondance (for $i \geq 3$)

$$M_i = \Phi(m_i) = \Phi(m_{i-1}s_{i-1}m_{i-2}) = M_{i-1}S_{i-1}M_{i-2}$$

we get

$$X_i = x_{i,0} = (x_{i-1,0}, x_{i-1,1}) S_{i-1} \begin{pmatrix} x_{i-2,0} \\ x_{i-2,1} \end{pmatrix}$$

and thus

$$\frac{X_i}{X_{i-1}X_{i-2}} = 1 + ab + a\frac{x_{i-2,1}}{x_{i-2,0}} + b\frac{x_{i-1,1}}{x_{i-1,0}} + \frac{x_{i-1,1}}{x_{i-1,0}}\frac{x_{i-2,1}}{x_{i-2,0}}$$

for i even and where a and b are permuted for i odd. As

$$\lim_{i\to\infty} \frac{x_{i-2,1}}{x_{i-2,0}} = \lim_{i\to\infty} \frac{x_{i-1,1}}{x_{i-1,0}} = \xi$$

we have

$$\Theta = \lim_{i\to\infty} \frac{X_i}{X_{i-1}X_{i-2}}.$$

Choose $0 < \eta < \epsilon$ such that

$$\frac{\Theta + \eta}{(\Theta - \eta)^{1/\gamma}} < \left(\Theta + \frac{\epsilon}{2}\right)^{1/\gamma^2}, \qquad \left(\Theta - \frac{\epsilon}{2}\right)^{1/\gamma^2} < \frac{\Theta - \eta}{(\Theta + \eta)^{1/\gamma}}.$$

Clearly, for i large enough, say $i \geq i_1$, we have

$$\Theta - \eta < \frac{X_i}{X_{i-1}X_{i-2}} < \Theta + \eta.$$

3.) Define

$$q_i := \frac{X_i}{X_{i-1}^{\gamma}} \qquad (i \geq 2).$$

Then

$$q_i = \frac{X_i}{X_{i-1}X_{i-2}} q_{i-1}^{-1/\gamma} \qquad (i \geq 3)$$

so that using the result found in 2), for $i \geq i_1$, we have $(\Theta - \eta) q_{i-1}^{-1/\gamma} < q_i < (\Theta + \eta) q_{i-1}^{-1/\gamma}$ which, for $i \geq i_1 + 1$, implies

$$\frac{(\Theta - \eta)}{(\Theta + \eta)^{1/\gamma}} q_{i-2}^{1/\gamma^2} < q_i < \frac{(\Theta + \eta)}{(\Theta - \eta)^{1/\gamma}} q_{i-2}^{1/\gamma^2}.$$

By the choice of η,

$$\left(\Theta - \frac{\epsilon}{2}\right)^{1/\gamma^2} q_{i-2}^{1/\gamma^2} < q_i < \left(\Theta + \frac{\epsilon}{2}\right)^{1/\gamma^2} q_{i-2}^{1/\gamma^2}.$$

But for all $i \geq i_1$ we can write $i = i_2 + 2j$ where

$$i_2 := \begin{cases} i_1 & \text{if } i - i_1 \equiv 0 \mod 2, \\ i_1 + 1 & \text{if } i - i_1 \equiv 1 \mod 2, \end{cases}$$

and we get, by recursion on $i \geq i_1$, the formula

$$(\Theta - \frac{\epsilon}{2})^{\frac{1}{\gamma^2}+\frac{1}{\gamma^4}+\cdots+\frac{1}{\gamma^{2j}}} q_{i_2}^{1/\gamma^{2j}} < q_{i_2+2j} < (\Theta + \frac{\epsilon}{2})^{\frac{1}{\gamma^2}+\frac{1}{\gamma^4}+\cdots+\frac{1}{\gamma^{2j}}} q_{i_2}^{1/\gamma^{2j}}.$$

Since

$$\lim_{j\to\infty} q_{i_i}^{1/\gamma^{2j}} = \lim_{j\to\infty} q_{i_i+1}^{1/\gamma^{2j}} = 1 \quad \text{and} \quad \sum_{i=1}^{\infty}(1/\gamma^2)^n = 1/\gamma,$$

we deduce

$$(\Theta - \epsilon)^{1/\gamma} < q_i < (\Theta + \epsilon)^{1/\gamma}$$

for all sufficiently large i.

4.) Since m_i is a palindrome, we have for $i \geq 3$, under the homomorphism Φ, that

$$\begin{aligned} M_i = M_{i-1}S_{i-1}M_{i-2} &= M_{i-2}S_{i-2}M_{i-1} \\ &= M_{i-2}S_{i-2}M_{i-2}S_{i-2}M_{i-3} \\ &= (M_{i-2}S_{i-2})^2 M_{i-3}. \end{aligned} \tag{4.2}$$

The Cayley-Hamilton Theorem states for $A \in \mathrm{M}_2(\mathbb{C})$ that

$$A^2 = \mathrm{tr}(A)A - \det(A)I$$

and thus, (4.2) gives the relation

$$\begin{aligned} M_i &= \mathrm{tr}(M_{i-2}S_{i-2})M_{i-2}S_{i-2}M_{i-3} - \det(M_{i-2}S_{i-2})M_{i-3} \\ &= \mathrm{tr}(M_{i-2}S_{i-2})M_{i-1} \pm M_{i-3}. \end{aligned}$$

In particular,

$$\mathbf{x}_i = c_i \mathbf{x}_{i-1} \pm \mathbf{x}_{i-3} \tag{4.3}$$

for $c_i \in \mathbb{Z}$. Using (4.3) and the multilinearity of the determinant, we see that $\det(\mathbf{x}_{i-2}, \mathbf{x}_{i-1}, \mathbf{x}_i) = \pm \det(\mathbf{x}_{i-3}, \mathbf{x}_{i-2}, \mathbf{x}_{i-1})$. Using this recurrence relation we get

$$\det(\mathbf{x}_{i-2}, \mathbf{x}_{i-1}, \mathbf{x}_i) = \pm \det(\mathbf{x}_0, \mathbf{x}_1, \mathbf{x}_2).$$

Clearly,

$$M_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad M_1 = \begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix}, \qquad M_2 = \begin{pmatrix} ba^2 + 2a & ab + 1 \\ ab + 1 & b \end{pmatrix}$$

and thus

$$|\det(\mathbf{x}_i, \mathbf{x}_{i+1}, \mathbf{x}_{i+2})| = \left\| \begin{matrix} 1 & 0 & 1 \\ a & 1 & 0 \\ ba^2 + 2a & ab + 1 & b \end{matrix} \right\| = |b - a|.$$

□

Proposition 4.10. *Let the sequences* $\left((x_{i,0}, x_{i,1}, x_{i,2})\right)_{i \geq 1} \subset \mathbb{Z}^3$ *and* $(X_i)_{i \geq 1}$ *be as in Lemma 4.8. For* $k \geq 1$, *define*

$$Q_k(T) = \begin{vmatrix} 1 & T & T^2 \\ x_{k,0} & x_{k,1} & x_{k,2} \\ x_{k+1,0} & x_{k+1,1} & x_{k+1,2} \end{vmatrix}.$$

Then

1. $|Q_k(\xi)| = |b - a| X_{k+2}^{-1} + O\left(\frac{X_{k-1}}{X_{k+2}^2}\right)$,
2. $H(Q_k) = c_k \frac{X_{k+1}}{X_k} + O\left(\frac{X_k}{X_{k+1}}\right)$,

where

$$c_k = \begin{cases} c(a) = \max\left\{\left|\frac{a+\xi}{\Theta}\right|, \left|1 - \frac{2\xi(a+\xi)}{\Theta}\right|, |\xi|\left|1 - \frac{\xi(a+\xi)}{\Theta}\right|\right\} & \text{if } k \text{ is odd}, \\ c(b) = \max\left\{\left|\frac{b+\xi}{\Theta}\right|, \left|1 - \frac{2\xi(b+\xi)}{\Theta}\right|, |\xi|\left|1 - \frac{\xi(b+\xi)}{\Theta}\right|\right\} & \text{if } k \text{ is even}. \end{cases}$$

Proof. By Lemma 4.7 we know

$$m_{k+2} = \begin{cases} m_{k+1}bam_k = m_k abm_{k-1} & \text{if } k \text{ is even,} \\ m_{k+1}abm_k = m_k bam_{k-1} & \text{if } k \text{ is odd,} \end{cases}$$

since m_{k+2} is a palindrome. Without loss of generality, assume k is even. Then

$$\xi = [0, a, b, a, a, b, a, \ldots] = [0, m_{k+2}, \ldots] = [0, m_k, t]$$

where $t = [a, b, m_{k+1}, \ldots]$. Using Lemma 4.4,

$$\begin{aligned} t =& a + \frac{1}{b + [0, m_{k+1}, \ldots]} \\ =& a + \frac{1}{b + \xi + O(X_{k+1}^{-2})}. \end{aligned}$$

It is now possible to use Lemma 4.6 and get

$$\begin{aligned} \xi =& \frac{x_{k,1}t + x_{k,2}}{x_{k,0}t + x_{k,1}} \\ =& \frac{x_{k,1}\left(a + \frac{1}{b + \xi + O(X_{k+1}^{-2})}\right) + x_{k,2}}{x_{k,0}\left(a + \frac{1}{b + \xi + O(X_{k+1}^{-2})}\right) + x_{k,1}} \end{aligned}$$

such that

$$\begin{aligned} x_{k,0}\xi - x_{k,1} =& \frac{x_{k,0}x_{k,2} - x_{k,1}^2}{x_{k,0}\left(a + \frac{1}{b + \xi + O(X_{k+1}^{-2})}\right) + x_{k,1}} \\ =& \frac{\det(\mathbf{x}_k)}{X_k\left(a + \frac{1}{b + \xi} + \xi + O(X_k^{-2})\right)} \\ =& \frac{b + \xi}{\Theta X_k}\left(1 + O(X_k^{-2})\right)\det(\mathbf{x}_k) \\ =& \frac{b + \xi}{\Theta X_k}\det(\mathbf{x}_k) + O(X_k^{-3}). \end{aligned} \tag{4.4}$$

Clearly, if k is odd, we have

$$x_{k,0}\xi - x_{k,1} = \frac{a + \xi}{\Theta X_k}\det(\mathbf{x}_k) + O(X_k^{-3})$$

which corresponds to (4.4) under the change $a \leftrightarrow b$. Since

$$x_{k,0}\big(x_{k,2} - 2x_{k,1}\xi + x_{k,0}\xi^2\big) = \det(\mathbf{x}_k) + (x_{k,1} - x_{k,0}\xi)^2 = \det(\mathbf{x}_k) + O(X_k^{-2}),$$

we have

$$x_{k,2} - 2x_{k,1}\xi + x_{k,0}\xi^2 = \frac{\det(\mathbf{x}_k)}{X_k} + O(X_k^{-3}).$$

The height of $Q_k(T)$ is

$$H(Q_k) = \max\left\{\left\|\begin{matrix} x_{k,0} & x_{k,1} \\ x_{k+1,0} & x_{k+1,1}\end{matrix}\right\|, \left\|\begin{matrix} x_{k,0} & x_{k,2} \\ x_{k+1,0} & x_{k+1,2}\end{matrix}\right\|, \left\|\begin{matrix} x_{k,1} & x_{k,2} \\ x_{k+1,1} & x_{k+1,2}\end{matrix}\right\|\right\}.$$

Since $\det(\mathbf{x}_k) = \pm 1$ and $|x_{k+1,1}| = |\xi| X_{k+1} + O(X_{k+1}^{-1})$ we estimate the above determinants and get

$$\begin{aligned}\left\|\begin{matrix} x_{k,0} & x_{k,1} \\ x_{k+1,0} & x_{k+1,1}\end{matrix}\right\| &= \left\|\begin{matrix} x_{k,0} & x_{k,1} - x_{k,0}\xi \\ x_{k+1,0} & x_{k+1,1} - x_{k+1,0}\xi\end{matrix}\right\| \\ &= \big|x_{k,0}(x_{k+1,1} - x_{k+1,0}\xi) - x_{k+1,0}(x_{k,1} - x_{k,0}\xi)\big| \\ &= \big|x_{k+1,0}(x_{k,1} - x_{k,0}\xi)\big| + O\left(\frac{X_k}{X_{k+1}}\right) \\ &= \begin{cases} \frac{X_{k+1}}{X_k}\left|\frac{b+\xi}{\Theta}\right| + O\left(\frac{X_k}{X_{k+1}}\right) & \text{if } k \text{ is even,} \\ \frac{X_{k+1}}{X_k}\left|\frac{a+\xi}{\Theta}\right| + O\left(\frac{X_k}{X_{k+1}}\right) & \text{if } k \text{ is odd,}\end{cases}\end{aligned}$$

$$\begin{aligned}\left\|\begin{matrix} x_{k,0} & x_{k,2} \\ x_{k+1,0} & x_{k+1,2}\end{matrix}\right\| &= \left\|\begin{matrix} x_{k,0} & x_{k,2} - x_{k,0}\xi^2 \\ x_{k+1,0} & x_{k+1,2} - x_{k+1,0}\xi^2\end{matrix}\right\| \\ &= \big|x_{k,0}(x_{k+1,2} - x_{k+1,0}\xi^2) - x_{k+1,0}(x_{k,2} - x_{k,0}\xi^2)\big| \\ &= \big|x_{k+1,0}(x_{k,2} - x_{k,0}\xi^2)\big| + O\left(\frac{X_k}{X_{k+1}}\right) \\ &= \big|x_{k+1,0}\big((x_{k,0}\xi^2 - 2x_{k,1}\xi + x_{k,2}) - 2\xi(x_{k,0}\xi - x_{k,1})\big)\big| + O\left(\frac{X_k}{X_{k+1}}\right) \\ &= \begin{cases} \frac{X_{k+1}}{X_k}\left|1 - \frac{2\xi(b+\xi)}{\Theta}\right| + O\left(\frac{X_k}{X_{k+1}}\right) & \text{if } k \text{ is even,} \\ \frac{X_{k+1}}{X_k}\left|1 - \frac{2\xi(a+\xi)}{\Theta}\right| + O\left(\frac{X_k}{X_{k+1}}\right) & \text{if } k \text{ is odd,}\end{cases}\end{aligned}$$

$$
\begin{aligned}
\left\| \begin{matrix} x_{k,1} & x_{k,2} \\ x_{k+1,1} & x_{k+1,2} \end{matrix} \right\| = & \left\| \begin{matrix} x_{k,1} & x_{k,2} - x_{k,1}\xi \\ x_{k+1,1} & x_{k+1,2} - x_{k+1,1}\xi \end{matrix} \right\| \\
= & \big| x_{k,1}(x_{k+1,2} - x_{k+1,1}\xi) - x_{k+1,1}(x_{k,2} - x_{k,1}\xi) \big| \\
= & \big| x_{k+1,1}(x_{k,2} - x_{k,1}\xi) \big| + O\left(\frac{X_k}{X_{k+1}}\right) \\
= & \big| x_{k+1,1}\big((\xi(x_{k,0}\xi - x_{k,1}) - (x_{k,0}\xi^2 - 2\xi x_{k,1} + x_{k,2})\big) \big| + O\left(\frac{X_k}{X_{k+1}}\right) \\
= & \begin{cases} \frac{X_{k+1}}{X_k}|\xi|\left|\frac{\xi(b+\xi)}{\Theta} - 1\right| + O\left(\frac{X_k}{X_{k+1}}\right) & \text{if } k \text{ is even,} \\ \frac{X_{k+1}}{X_k}|\xi|\left|\frac{\xi(a+\xi)}{\Theta} - 1\right| + O\left(\frac{X_k}{X_{k+1}}\right) & \text{if } k \text{ is odd.} \end{cases}
\end{aligned}
$$

Thus

$$H(Q_k) = c_k \frac{X_{k+1}}{X_k} + O\left(\frac{X_k}{X_{k+1}}\right)$$

where c_k is as in the statement of the proposition.

Write

$$x_{k+2,0}\big(1, \xi, \xi^2\big) = \mathbf{x}_{k+2} + \mathbf{z}$$

where

$$\mathbf{z} = \big(0, x_{k+2,0}\xi - x_{k+2,1}, x_{k+2,0}\xi^2 - x_{k+2,2}\big).$$

Using the multilinearity of the determinant, we have

$$\big| x_{k+2,0} Q_k(\xi) \big| = \big| \det(\mathbf{x}_{k+2}, \mathbf{x}_k, \mathbf{x}_{k+1}) + \det(\mathbf{z}, \mathbf{x}_k, \mathbf{x}_{k+1}) \big|.$$

But using the estimates of Theorem 4.9,

$$
\begin{aligned}
\det(\mathbf{z}, \mathbf{x}_k, \mathbf{x}_{k+1}) \le & \left| \begin{matrix} 0 & x_{k+2,0}\xi - x_{k+2,1} & x_{k+2,0}\xi^2 - x_{k+2,2} \\ x_{k,0} & x_{k,0}\xi - x_{k,1} & x_{k,0}\xi^2 - x_{k,2} \\ x_{k+1,0} & x_{k+1,0}\xi - x_{k+1,1} & x_{k+1,0}\xi^2 - x_{k+1,2} \end{matrix} \right| \\
\ll & X_{k+2}^{-1}\big(X_{k+1}X_k^{-1} + X_k X_{k+1}^{-1}\big) \\
\ll & \frac{X_{k+1}}{X_k X_{k+2}} \\
\ll & \frac{X_{k-1}}{X_{k+2}}.
\end{aligned}
$$

Again using Theorem 4.9, we find

$$\begin{aligned}|Q_k(\xi)| =&\frac{1}{|x_{k+2,0}|}\left(|\det(\mathbf{x}_{k+2},\mathbf{x}_k,\mathbf{x}_{k+1})|+O\left(\frac{X_{k-1}}{X_{k+2}}\right)\right)\\ =&\frac{|b-a|}{X_{k+2}}+O\left(\frac{X_{k-1}}{X_{k+2}^2}\right).\end{aligned}$$

□

Using the same notation as in Proposition 4.10, we can prove the following corollary which brings us one step closer to our goal.

Corollary 4.11. *Fix κ with $\kappa > |b-a|\Theta\max\{c(a)^{\gamma^2}, c(b)^{\gamma^2}\}$. Then, for any sufficiently large positive real number X, there exists an index k such that the polynomial $Q_k(T)$ satisfies*

$$H(Q_k)\le X, \qquad |Q_k(\xi)|\le\kappa X^{-\gamma^2}.$$

Proof. For X sufficiently large, there exists a k such that

$$H(Q_k)<X<H(Q_{k+1}).$$

For this choice of k, we get the inequality

$$X<c_{k+1}\frac{X_{k+2}}{X_{k+1}}\big(1+o(1)\big) \tag{4.5}$$

and clearly, for $X\longrightarrow\infty$, we must have $k\longrightarrow\infty$. Since Theorem 4.9 states that

$$\frac{X_i}{X_{i-1}X_{i-2}}=\Theta\big(1+o(1)\big)$$

we get

$$\Theta X_{i-2}=\frac{X_i}{X_{i-1}}\big(1+o(1)\big).$$

Hence, equation (4.5) is equivalent to

$$\frac{X}{c_{k+1}\Theta}<X_k\big(1+o(1)\big).$$

Using the estimates of Theorem 4.9 and Proposition 4.10, we have

$$\begin{aligned}|Q_k(\xi)| =&|b-a|X_{k+2}^{-1}(1+o(1))\\ \le&|b-a|\Theta^{-1/\gamma}X_{k+1}^{-\gamma}(1+o(1))\\ \le&|b-a|\Theta^{-\gamma}X_k^{-\gamma^2}(1+o(1))\\ \le&|b-a|\Theta^{-\gamma}\left(\frac{X}{c_{k+1}\Theta}\right)^{-\gamma^2}(1+o(1))\\ =&|b-a|c_{k+1}^{\gamma^2}\Theta X^{-\gamma^2}(1+o(1)).\end{aligned}$$

Thus, for κ satisfying $\kappa > |b-a|\Theta\max\{c(a)^{\gamma^2}, c(b)^{\gamma^2}\}$ we have

$$|Q_k(\xi)| \le \kappa X^{-\gamma^2}$$

provided that X is sufficiently large. □

Proposition 4.12. *Let $\xi = \xi_{1,2}$ and let everything be defined as in Corollary 4.11. Then*

$$\Theta\max\{c(1)^{\gamma^2}, c(2)^{\gamma^2}\} \le 1.27.$$

Proof. Since $a = 1$, $b = 2$, we use the fact that the 18th and 19th convergents of ξ act as upper and lower bounds for the value of ξ (see Lemma 4.4) and get that

$$0.7204846674 \le \xi \le 0.7204846677.$$

Then

$$\Theta = 3 + 3\xi + \xi^2 \le 5.680552159$$

and

$$c(1) \le 0.5635696006 \quad \text{and} \quad c(2) \le 0.4789120128.$$

Clearly,

$$\Theta\max\{c(1)^{\gamma^2}, c(2)^{\gamma^2}\} \le 1.265793309.$$

□

4.3.4 Proof of Theorem 4.1

Proof. Let $\xi = \xi_{1,2}$. As stated earlier, ξ has been proved to be transcendental in [1]. Let $Q_k(T) \in \mathbb{Z}[T]$ be defined as in Proposition 4.10. Then each Q_k has degree at most 2 and for X large enough, Corollary 4.11 and Proposition 4.12 together show that there exists an index k such that

$$H(Q_k) \leq X, \qquad |Q_k(\xi)| \leq 1.27X^{-\gamma^2}.$$

□

Conclusion

In this thesis, we studied optimal approximation exponents for problems in Diophantine Approximation. We revisited several results of Davenport & Schmidt and proved a new and optimal Gel'fond type criterion to decide if a given complex number is rational or quadratic over $\mathbb{Q}$. This leaves open many questions about optimal exponents. In particular:

1. Is the conjecture of Wirsing-Schmidt true for $n \geq 3$?

2. What is the optimal approximation exponent for the simultaneous approximation of the real numbers $\xi, \xi^2, \ldots, \xi^n$ by rational numbers with the same denominator for $n \geq 3$?

3. What is the optimal approximation exponent of a real number by algebraic integers of degree at most n for $n \geq 4$?

4. What is the optimal exponent for a Gel'fond type criterion in degree $n \geq 3$?

The real numbers $\xi_{a,b}$, having a Fibonacci continued fraction expansion, are known to achieve the optimal approximation exponent in degree $n = 2$ of the second and fourth problems listed above (proved here and by Roy [17]). It would be interesting to see if this connection exists in arbitrary degree n.

There is still much work to do to solve these questions. At present, only the cases of low degree are solved, and no mechanism known to solve the problems in general.

Appendix A

More versions of Gel'fond's criterion

A.1 Introduction

We have seen in Chapter 3 a new version of what is usually referred to as Gel'fond's criterion. This criterion uses the value of integral polynomials at a given real or complex number to decide for the algebraicity of this number. We present below two more versions of this result as well as the original criterion. This is in no way a comprehensive survey of the history of the above mentionned criterion.

A.2 Original Gel'fond's criterion

We first state the original criterion due to Gel'fond [11, Chapter 3, §4, Lemma VII].

Theorem A.1. *Let $\xi \in \mathbb{R}$ be non-zero and $a_0 > 1$. Let $\sigma, \theta : \mathbb{R} \longrightarrow \mathbb{R}_{>0}$ be monotonic increasing functions such that $\sigma(x) > x$ and $\theta(x) > 0$. Moreover, for $x > x_0 > 0$ we ask that $\lim_{x\to\infty} \sigma(x) = \lim_{x\to\infty} \theta(x) = \infty$ and $a_0\sigma(x) \geq \sigma(x+1)$. If for all integers*

$N > N_0 > 0$ *there exists a non-zero integral polynomial* P *satisfying*

$$|P(\alpha)| < e^{-\sigma^2(N)\theta(N)}, \qquad \max\{\deg(P), \log H(P)\} \leq \frac{1}{3}\sigma(N)$$

then α *is an algebraic number.*

A.3 Roy and Waldschmidt's version

This next version follows D. Roy and M. Waldschmidt [20]. In their paper, the authors prove the result over any field K. Here, we study the theorem over the field $\mathbb{Q}$ only.

We first need another version of Gel'fond's Lemma (c.f. Theorem 1.25). For a proof, see [12, Chapter 3].

Lemma A.2. *Let* $P_1, \dots, P_k \in \mathbb{Z}[T]$ *be non-zero polynomials and let* $P = P_1 \cdots P_k$ *be of degree* n. *Then*

$$e^{-n}H(P_1)\dots H(P_k) < H(P) < e^n H(P_1)\dots H(P_k).$$

Theorem A.3. *Let* $\xi \in \mathbb{R}$, $n \in \mathbb{Z}_{>0}$ *and suppose that for* X *large enough there exists a non-zero polynomial* $P = P_X \in \mathbb{Z}[T]_{\leq n}$ *with*

$$H(P) \leq X \quad \textit{and} \quad \frac{|P(\xi)|}{H(P)} \leq cH(P)^{-n}X^{-\deg(P)}$$

where $c^{-1} = e^{4n^2}(n+1)(2n)!$. *Then* ξ *is algebraic of degree at most* n *and the polynomial* P *vanishes at* ξ *for sufficiently large* X.

Proof. Fix $\xi \in \mathbb{R}$ and $n \in \mathbb{Z}_{>0}$. Without loss of generality, we may assume that all the polynomials we deal with are primitive (i.e. their coefficients are relatively prime.) We prove this by contradiction. Assume that for some large value of X, $P = P_X \in \mathbb{Z}[T]_{\leq n}$ satisfies

$$H(P) \leq X, \qquad \frac{|P(\xi)|}{H(P)} \leq cH(P)^{-n}X^{-\deg(P)}$$

and $P(\xi) \neq 0$.

Claim: For each integer $m = 1, \dots, n$ we can construct a primitive polynomial $Q(T) \in \mathbb{Z}[T]_{\leq m}$ of arbitrary large height which satisfies

$$0 < \frac{|Q(\xi)|}{H(Q)} < cH(Q)^{-n-\deg(Q)}. \tag{A.1}$$

We will demonstrate the claim by induction. For $m = n$, the polynomials P_X for which $P_X(\xi) \neq 0$ satisfy (A.1). Moreover, as

$$\lim_{X\to\infty} \frac{|P_X(\xi)|}{H(P_X)} \leq \lim_{X\to\infty} cH(P)^{-n}X^{-\deg(P)} = 0,$$

we get

$$\lim_{X\to\infty} H(P_X) = \infty$$

and the claim is thus satisfied for $m = n$. Now assume that the claim is satisfied for some integer m with $2 \leq m \leq n$. So choose $Q(T) \in \mathbb{Z}[T]_{\leq m}$ satisfying (A.1). Without lost of generality, assume $H(Q)$ is large enough so that putting $X = e^{-n}H(Q)$ the polynomial $P = P_X$ above is defined. Let $G(T) = \gcd(P(T), Q(T)) \in \mathbb{Z}[T]$ be of degree d. As Q is primitive, we get that G is also primitive. Since $H(P) \leq e^{-n}H(Q)$, Lemma A.2 implies that $G \neq \pm Q$ and thus $0 \leq d < \deg(Q) \leq m$. Then

$$H(P) \leq X, \qquad H(Q) = e^n X, \qquad \frac{H(G)}{H(P)} \leq e^n, \qquad \frac{H(G)}{H(Q)} \leq e^n.$$

Denote $\deg(P) = d_p$ and $\deg(Q) = d_q$. Using Lemma 1.38, and simplifying at each step with the above inequalities, we get

$$\begin{aligned}
\frac{|G(\xi)|}{H(G)} \leq & \left(\frac{H(P)}{H(G)}\right)^{d_q-d} \left(\frac{H(Q)}{H(G)}\right)^{d_p-d} \left(k_1\frac{|P(\xi)|}{H(P)} + k_2\frac{|Q(\xi)|}{H(Q)}\right)\\
<c & \left(\frac{H(P)}{H(G)}\right)^{d_q-d} \left(\frac{H(Q)}{H(G)}\right)^{d_p-d} \left(k_1 H(P)^{-n}X^{-d_p} + k_2 H(Q)^{-n-d_q}\right)\\
=c & H(G)^{-n}X^{-d}\Bigg[k_1 \left(\frac{H(G)}{H(P)}\right)^{n+d-d_q} \left(\frac{H(Q)}{XH(G)}\right)^{d_p-d}\\
& + k_2 \left(\frac{H(G)}{H(Q)}\right)^{n+d+d_q-d_p} \left(\frac{H(P)}{XH(G)}\right)^{d_q-d} X^{d_q}H(G)^{-d_q}\Bigg]
\end{aligned}$$

$$\begin{aligned}
\leq & cH(G)^{-n}X^{-d}\Bigg[k_1\left(\frac{H(G)}{H(P)}\right)^{n+d-d_q}\left(\frac{H(Q)}{XH(G)}\right)^{d_p-d} \\
& \qquad + k_2\left(\frac{H(G)}{H(Q)}\right)^{n+d-d_p}\left(\frac{H(P)}{XH(G)}\right)^{d_q-d} e^{-nd_q}\Bigg] \\
\leq & cH(G)^{-n}X^{-d}\Bigg[k_1\left(e^n\right)^{n+d-d_q}\left(\frac{e^n}{H(G)}\right)^{d_p-d} + k_2\left(e^n\right)^{n+d-d_p}\left(\frac{1}{H(G)}\right)^{d_q-d} e^{-nd_q}\Bigg] \\
= & cH(G)^{-n}X^{-d}\left[k_1 e^{n(n+d_p-d_q)}H(G)^{d-d_p} + k_2 e^{n(n+d-d_p-d_q)}H(G)^{d-d_q}\right] \\
\leq & ce^{2n^2}H(G)^{-n}X^{-d}\left(k_1 H(G)^{d-d_p} + k_2 H(G)^{d-d_q}\right).
\end{aligned}$$

Since the constants c_1, c_2 of Lemma 1.37 satisfy $c_1, c_2 \leq (2n)!$ and since $2^j(j+1) \leq e^{j+1}$ for $j \geq 0$, we get that the constants k_1, k_2 of Lemma 1.38 satisfy $ck_1e^{2n^2}, ck_2e^{2n^2} \leq 1$. Then, we can rewrite the last inequality as

$$\frac{|G(\xi)|}{H(G)} \leq H(G)^{-n}X^{-d}\max\{H(G)^{d-d_p}, H(G)^{d-d_q}\}. \qquad (A.2)$$

Since $Q(\xi) \neq 0$ and G divides Q, we necessarily have $G(\xi) \neq 0$. If $d = \deg(G) = 0$, equation (A.2) gives

$$1 = \frac{|G(\xi)|}{H(G)} \leq H(G)^{-n}\max\{H(G)^{-d_p}, H(G)^{-d_q}\} < 1$$

which is impossible. Thus, we have $d \geq 1$. Moreover, (A.2) shows that $|G(\xi)|/H(G)$ can be made arbitrary small by making X large enough, i.e., by choosing Q of height large enough. In particular, we can pick Q such that $c^{-1}e^{n^2} \leq H(G)$. Recall that

$$1 \leq H(G) \leq e^nH(P) \leq e^nX.$$

In the case $d < d_p$ we rewrite equation (A.2) as

$$\frac{|G(\xi)|}{H(G)} < H(G)^{-n-1}X^{-d} \leq ce^{-n^2}H(G)^{-n}X^{-d}$$

and hence

$$\frac{|G(\xi)|}{H(G)} \leq cH(G)^{-n-\deg(G)}.$$

If $d = d_p$ then $G = \pm P$ and so, by hypothesis,

$$\frac{|G(\xi)|}{H(G)} = \frac{|P(\xi)|}{H(P)} < cH(P)^{-n}X^{-d_p} < cH(P)^{-n-d_p} = cH(G)^{-n-\deg(G)}.$$

Thus, there exists polynomials G of degree at most $m-1$ and arbitrary large height for which (A.1) is satisfied. This proves our claim.

In particular, for $m = 1$, we can find a primitive polynomial $Q \in \mathbb{Z}[T]_{\leq 1}$ of degree 1 satisfying (A.1). Choose Q of height large enough so that putting $X = e^{-n}H(Q)$ the polynomial $P = P_X$ is defined. As noted above, if we let $G = \gcd(P, Q)$, this construction implies by Lemma A.2 that $G \neq \pm Q$ and thus, Q does not divide P. Since P and Q are integral polynomials, we use Lemma 1.37 and the estimates $c_1, c_2 \leq (2n)!$ to get

$$\begin{aligned}
|\operatorname{Res}(P,Q)| \leq & H(P)^{\deg(Q)}H(Q)^{\deg(P)}\left(c_1\frac{|P(\xi)|}{H(P)} + c_2\frac{|Q(\xi)|}{H(Q)}\right)\\
\leq & H(P)H(Q)^{\deg(P)}\left(c_1cH(P)^{-n}X^{-\deg(P)} + c_2cH(Q)^{-n-1}\right)\\
\leq & c\max\{c_1,c_2\}\left(e^{n\deg(P)+n^2-n}H(Q)^{1-\deg(P)} + 1\right)\\
\leq & \frac{1}{e^{2n^2}(n+1)}\left(H(Q)^{1-\deg(P)} + 1\right)\\
< & 1,
\end{aligned}$$

and thus $|\operatorname{Res}(P,Q)| = 0$. Hence P and Q share a root. This is impossible since Q has degree 1, is primitive and does not divide P. This construction of polynomials based on the hypothesis that $P_X(\xi) \neq 0$ leads us to a contradiction. □

A.4 Brownawell's version

We conclude with the following version of Brownawell. For a proof, see [4]

Theorem A.4. *Let $c, d \in \mathbb{Z}_{\geq 1}$ with $cd > 1$. Suppose that $(\gamma_n)_{n\geq 1} \subset \mathbb{R}$ and $(\delta_n)_{n\geq 1} \subset \mathbb{R}$ are monotonic nondecreasing sequences such that*

$$\lim_{n\to\infty} \delta_n\gamma_n = \infty$$

and

$$\gamma_{n+1} \leq c\gamma_n \quad (n \geq 1), \qquad \delta_{n+1} \leq d\delta_n \quad (n \geq 1).$$

Let $\alpha \in \mathbb{C}$. *If there exists a sequence of polynomials* $(P_n)_{n\geq 1} \subset \mathbb{Z}[T]_{\leq \delta_n}$ *with* $P_n \neq 0, 1$, *height* $H(P_n) \leq e^{\gamma_n}$ *and*

$$\log |P_n(\alpha)| \leq -\delta_n\big((c+d+1)\gamma_n + (2d+1)\delta_n\big) \qquad (n \geq 1),$$

then α *is algebraic and*

$$P_n(\alpha) = 0 \qquad (n \geq 1).$$

Bibliography

[1] Allouche, J.-P., Davison, J.L., Queffélec, M., Zamboni, L.Q., Transcendence of Sturmian or morphic continued fractions, *J. Number Theory* **91** (2001), 39-66.

[2] Arbour, B., Roy, D., A Gel'fond type criterion in degree two, *Acta Arith.* (to appear), 6 pages, arXiv:math.NT/0212209.

[3] Baker, A., *Transcendental Number Theory*, Cambridge University Press, Great Britain, 1979.

[4] Brownawell, W.D., Sequences of diophantine approximations, *J. Number Theory* **6** (1974), 11-21.

[5] Bugeaud, Y., *Approximation by Algebraic Numbers*, Cambridge Tracts in Mathematics (to appear).

[6] Bugeaud, Y., Teulié, O., Approximation d'un nombre réel par des nombres algébriques de degré donné, *Acta Arith.* **43** (2000), 77-86.

[7] Cassels, J.W.S., *An Introduction to The Geometry of Numbers*, Springer-Verlag, Berlin, 1959.

[8] Davenport, H., Schmidt, W.M., Approximation to real numbers by quadratic irrationals, *Acta Arith.* **8** (1967), 169-176.

[9] Davenport, H., Schmidt, W.M., Approximation to real numbers by algebraic integers, *Acta Arith.* **15** (1969), 393-416.

[10] Dirichlet, L.G.P., Verallgemeinerung eines Satzes aus der Lehre von den Kettenbrüchen nebst einigen Anwendungen auf die Theorie der Zahlen, *S. B. Preuss. Akad. Wiss.*, 93-95, 1842.

[11] Gel'fond, A.O., *Transcendental & Algebraic Numbers*, Dover, New York, 1960.

[12] Lang, S., *Fundamentals of Diophantine Geometry*, Springer-Verlag, New York, 1983.

[13] Lekkerkerker, C.G., *Geometry of Numbers*, John Wiley & Sons Inc., New York, 1969.

[14] Liouville, J., Sur des classes très étendues de quantités dont la valeur n'est ni algébrique, ni même réductible à des irrationnelles algébriques, *J. Math. Pures Appl.* (1) **16** (1851), 133-142.

[15] Mahler, K., *Lectures on Transcendental Numbers*, Lecture Notes in Mathematics **546**, Springer-Verlag, Berlin, 1976.

[16] Roth, K.F., Rational approximations to algebraic numbers, *Mathematika* **2** (1955), 1-20.

[17] Roy, D., Approximation to real numbers by cubic algebraic integers I, *Proc. London Math. Soc.* (to appear), 22 pages, arXiv:math.NT/0210181.

[18] Roy, D., Approximation to real numbers by cubic algebraic integers II, *Annals of Math.* (to appear), 7 pages, arXiv:math.NT/0210182.

[19] Roy, D., Approximation Simultanée d'un nombre et son carré, *C.R. Acad. Sci. Paris* Ser. I **336** (2003), 1-6.

[20] Roy, D., Waldschmidt, M., Diophantine approximation by conjugate algebraic integers, *Compositio Math.* (to appear), 31 pages, arXiv:math.NT/0207102.

[21] Schmidt, W.M., *Diophantine Approximation*, Lecture Notes in Mathematics **785**, Springer-Verlag, Berlin, 1980.

[22] Schmidt, W.M., *Diophantine Approximations and Diophantine Equations*, Lecture Notes in Mathematics **1467**, Springer-Verlag, Berlin, 1991.

[23] Sprindžuk, V.G., *Mahler's Problem in Metric Number Theory*, Transl. Math Monographs 25, Amer. Math Soc., Providence, R.I., 1969.

[24] van Lint, J.H., Wilson, R.M., *A Course in Combinatorics*, Cambridge University Press, Great Britain, 1992.

[25] Waldschmidt, M., *Diophantine Approximation on Linear Algebraic Groups; Transcendence Properties of the Exponential Function in Several Variables*, Series of Comprehensive Studies in Mathematics **326**, Springer-Verlag, Germany, 1991.

[26] Waldschmidt, M., *Nombres Transcendants*, Lecture Notes in Mathematics **402**, Springer-Verlag, Berlin, 1974.

[27] Wirsing, E., Approximation mit algebraischen Zahlen beschränkten Grades, *J. reine angew Math.* **206** (1960), 67-77