Close p-adic Roots of Integer Polynomials

Bethany Dixon

PhD

University of York
Mathematics

January 2025

Abstract

In this thesis I will study the question of how close roots of a fixed degree integer polynomial can be in terms of its height. This question has been studied extensively in the case of real and complex roots but there is much less known in the case of p-adic roots and this is what will be studied in this work. More specifically we will investigate the largest real number K such that for any $\kappa < K$ it is possible to find infinitely many integer polynomials of fixed degree and bounded height such that

$$|\alpha_1 - \alpha_2|_p \leq H(P)^{-\kappa}$$

holds for some roots $\alpha_1 \neq \alpha_2 \in \overline{\mathbb{Q}_p}$ of P. This question for the case of real and complex roots was first discussed by Mahler in 1964 as he proved that $K \leq n + 1$ for polynomials of degree n.

I will also study the quantitative version of this problem by counting the number of polynomials with close p-adic roots. We will also explore the related problem of bounding the discriminant of polynomials as we consider the separation of all roots of a polynomial. To this end we will establish a counting result for the number of polynomials of fixed degree and bounded height with p-adically small discriminant.

The method that I use relies on the quantitative non-divergence of Kleinbock and Tomanov and its use in the investigation of the distribution of close p-adic roots to find the infimum K. This work follows and develops similar methods for the real and complex case by Beresnevich, Bernik and Götze.

Contents

List of Figures

Acknowledgments

I would like to express my deepest gratitude to my supervisors, Victor Beresnevich and Sanju Velani, for their invaluable support, both academically and helping me navigate the challenges along the way.

I'd also like to thank my partner Sam for always believing in me, especially during moments when I struggled to believe in myself.

My heartfelt thanks go out to all the people at York who offered their help and support, I wouldn't have been able to do this without the help of the PhD network. In particular, I am especially grateful to my housemates and friends, Simen, Cordelia, Andrew, Rutvij, Ding and Ambroise. Your friendship and encouragement played a crucial role in helping me gain confidence in myself. I also want to thank Jenny and Cordelia for introducing me to the art of crochet by teaching me the value of relaxation through craft and to Simen for all the puzzle games we played together.

Finally, I would like to thank my family for their unwavering support over the years and for inspiring me to pursue my goals with determination and confidence.

Author's declaration

I declare that the work presented in this thesis, except where otherwise stated, is based on my own research carried out at the University of York and has not been submitted previously for any degree at this or any other university. Sources are acknowledged by explicit references.

Chapter 5 is taken from [6] which is joint work with Victor Beresnevich and will be submitted for publication imminently.

— 1 —

Introduction

If you take any two algebraic numbers not equal to each other of bounded heights and degrees then they cannot be arbitrary close to each other. This can easily be seen to be true since the number of algebraic numbers in question is finite. Indeed if you have two rationals $\frac{a}{b}$ and $\frac{c}{d}$ not equal to each other with $|b|, |d| \leq H$ for some $H \in \mathbb{R}$ then

$$\left|\frac{a}{b} - \frac{c}{d}\right| \geq \frac{1}{bd} \geq \frac{1}{H^2}.$$

These rationals are roots of some polynomials, namely

$$P(X) = (bX - a)(dX - c).$$

In general, if the algebraic numbers are conjugate over the field of the rational numbers then they will be roots of the same irreducible polynomial with integer coefficients, otherwise they are roots of two different irreducible polynomials P_1 and P_2. Of course, they can also be viewed as roots of the same (reducible) polynomial $P = P_1P_2$. An example of this is the polynomial above which is clearly reducible over $\mathbb{Q}$.

In the 1960's, Mahler [39] quantified the above trivial observation regarding the separation of algebraic numbers, by establishing a very general lower bound on the distance between two algebraic number of bounded height and degree. Various upper bounds have also been obtained. We will give a survey of these in Chapter 3. However, much less is know in the p-adic case.

The main purpose of this work is to answer the question of how close, as a function of the naive height, can p-adic roots of an irreducible polynomial of degree n be, where the naive height for a given integer polynomial $P = a_nx^n + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$,

is defined as

$$H(P) := \max_{0 \le i \le n} |a_i|.$$

For the field of p-adic numbers, $\mathbb{Q}_p$, and $\mathcal{P}_{irr}(n)$ the infinite subclass of irreducible polynomials in $\mathbb{Z}[x]$ with $\deg P = n$ and roots in $\mathbb{Q}_p$. Define $\boldsymbol{\kappa_{\mathbf{irr}}(n, p)}$ to be the infimum of all κ such that for all polynomials $P \in \mathcal{P}_{irr}(n)$ of sufficiently large height

$$|\alpha_1 - \alpha_2| > H(P)^{-\kappa}$$

holds for any pair of roots $\alpha_1 \neq \alpha_2 \in \mathbb{Q}_p$ of P. That is to say that $\kappa_{\text{irr}}(n, p)$ is the largest real number such that for any $\kappa < \kappa_{\text{irr}}(n, p)$ it is possible to find infinitely many $P \in \mathcal{P}_{irr}(n)$ such that

$$|\alpha_1 - \alpha_2| \le H(P)^{-\kappa}$$

holds for some roots $\alpha_1 \neq \alpha_2 \in \mathbb{Q}_p$ of P.

The above question can then be answered as we find a lower bound on $\kappa_{\text{irr}}(n, p)$ by the following theorem.

Theorem A. *For any $n \ge 2$ and any prime p, we have that*

$$\kappa_{\text{irr}}(n, p) \ge \frac{n+1}{3}.$$

The natural progression of this is to then consider the discriminant of a polynomial, which naturally encodes and quantifies the joint separation between all the roots of a given polynomial. Indeed, by definition the discriminant of a polynomial P of degree n with roots $\alpha_1, \ldots, \alpha_n$ and the leading coefficient a_n is

$$D(P) := a_n^{2n-2} \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2.$$

Therefore the secondary aim of this work is to establish counting results for the number of polynomials of a fixed degree and bounded height with p-adically small discriminant. The size of the discriminant will be bounded by a function of the height and degree.

This will be done by defining the set of polynomials of interest

$$\mathcal{D}_{n,p,\gamma}(Q, \nu) := \left\{ P \in \mathcal{P}_n(Q) : \begin{array}{c} 0 < |D(P)|_p \le \gamma Q^{-2\nu} \text{and} \\ P \text{ is irreducible over } \mathbb{Q} \end{array} \right\}$$

and finding a lower bound of $\#\mathcal{D}_{n,p,\gamma}(Q, \nu)$. This is done as the following theorem.

Theorem B. *Let $n \geq 2$ be an integer, p be a prime. Then there exist constants $Q_0 = Q_0(n,p) > 1$, $\gamma = \gamma(n,p) > 0$ and $C' = C'(n,p) > 0$ such that for all $Q \geq Q_0$ and any*

$$0 \leq \nu \leq n-1$$

we have that

$$\#\mathcal{D}_{n,p,\gamma}(Q,\nu) \geq C' Q^{n+1-\frac{n+2}{n}\nu}.$$

1.1 STRUCTURE OF THESIS

As already mentioned above, the problems addressed in the thesis have been investigated extensively in the real and complex case however relatively little is known for the p-adic case. The past work on the problems, as well as key new results obtained in this thesis, will be surveyed in Chapter 3.

In Chapter 2, we will give a brief introduction to p-adic numbers and other relevant core definitions and results that will be used throughout. In Chapter 4, we will discuss the methods of Kleinbock and Tomanov on the topic of quantitative non-divergence. Their method will be instrumental in the proofs of the new results of the thesis. Finally Chapter 5 is dedicated to obtaining full proofs of the new results.

— 2 —

Preliminaries

2.1 HISTORY AND MOTIVATION TO p-ADIC NUMBERS

The p-adic numbers were first introduced by Kurt Hensel in 1897 in a paper entitled "Über eine neue Begründung der Theorie der algebraischen Zahlen" ("On a New Foundation for the Theory of Algebraic Numbers") [29]. He was heavily influenced by Kummer's techniques involving prime powers and congruence's. Hensel's notation and formalism for p-adic numbers were not as refined as modern standards. This played a part in the initial scepticism around a number system that differed so radically from the familiar real and complex number systems. Another reason for the scepticism was his false proof that e is transcendental. Further details of this can be found in [46].

We begin by summarising Hensel's ideas. Consider that the rings $\mathbb{Z}$ and $\mathbb{C}[x]$ are similar in the respect that they both have a unique factorisation of elements. That is, any integer can be expressed uniquely as the product of primes (possibly having to be multiplied by -1, which is a unit — that is an invertible element — in $\mathbb{Z}$.) and any polynomial in $\mathbb{C}[x]$ can be expressed as the following unique product

$$P(x) = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

where $\alpha_1, ..., \alpha_n \in \mathbb{C}$ are the roots of P and $a \neq 0$ is thus a unit in $\mathbb{C}$. Therefore it can be said that the primes are analogous to the polynomials $(x - \alpha) \in \mathbb{C}[x]$. Hensel's idea stretches further than this as he considered the Taylor expansion of an element of $\mathbb{C}[x]$ and how this could be brought to $\mathbb{Z}$. That is to say that a polynomial

in $\mathbb{C}[x]$ can be expressed as

$$P(x) = \sum_{i=0}^{n} a_i (X - \alpha)^i$$

with the coefficients $a_i \in \mathbb{C}$ and naturally for any positive integer m and prime p it is possible to write

$$m = \bar{a}_0 p^0 + \bar{a}_1 p + \cdots + \bar{a}_n p^n = \sum_{i=0}^{n} \bar{a}_i p^i,$$

where $0 \leq \bar{a}_i < p$ for all $0 \leq i \leq n$.

The Taylor expansion allows us to see the local behaviour of a function around an element, while p-adic expansions examines the local behavior of numbers with respect to divisibility by powers of p.

The benefit of writing a number m as above is that it is possible to lift roots of a polynomial equation. That is to say, if it is possible to find a root modulo p^k then it is possible to find roots module $p^{k+1}, p^{k+2}, \ldots$. This concept is generalised to what is now known as *Hensel's Lemma* which will be discussed later in Section 2.2.3. For now, this idea can be thought of as analogous to Newton's method for finding roots of a real function.

Hensel was initially more interested in congruence equations. He wanted to find a sequence of numbers $A_0, A_1, ...$ such that

$$\omega = A_0 + A_1 x + A_2 x^2 + \cdots \qquad \mod p^m$$

for each $m \in \mathbb{N}$.

From around 1904, he began to consider questions involving convergence of the series $\sum_{i=0}^{n} a_i p^i$ and how these objects form a field $K(p)$ (This is what we call $\mathbb{Q}_p$ in modern notation). These new ideas were then explored and later in 1908 he published his book "Theorie der algebraischen Zahlen" ("The Theory of Algebraic Numbers")[30] and this clarification of ideas and notation aided in the growing interest into the subject. An analysis of this book in English was given by Steven Kieffer in their thesis "Computability in Principle and in Practice in Algebraic Number Theory: Hensel to Zassenhaus" [32] as Chapter 2, Section 4.

An example of this growing interest is the work of Helmut Hasse who studied under Hensel in the 1920s. This work lead to the Hasse-Minkowski Theorem. A more in depth version of this history can be found in [46].

The p-adics provide an alternate version of solving problem which can (sometimes) be easier to work with than the real numbers. Examples of using p-adics include the following questions.

- When is $n^3 + 1$ highly divisible by 3?
- How to find roots of polynomials in modular arithmetic (Hensel's Lemma)?
- How to prove it's not possible to dissect a square into an odd number of triangles of equal area (Monsky's Theorem)?
- Why does $\sum_{i=0}^{\infty} 4 \cdot 5^i = -1$ makes sense?

While all these are interesting problems the one this thesis is mainly concerned about involves looking at when p-adic conjugate roots of polynomials are close and the proportion of time that this occurs.

2.1.1 Motivation and Visualisation

First it is important to consider a motivation for p-adics. Starting with a system of rational numbers, consider the following series

$$4 \sum_{k \geq 0} \frac{(-1)^k}{2k+1}.$$

This is a sequence of rational numbers which converges to a number which is not rational (namely π). There are many similar examples, hence our system of rational numbers must have gaps. Ideally these gaps should be filled in to create a complete number system. The more obvious answer is to do this by extending the rational numbers to the real numbers but that is not the only option.

Instead it is possible to extend the rationals in a different way by considering what is meant when two numbers are 'close' to each other. First note that every rational number $x \in \mathbb{Q}$ can be rewritten as

$$x = \sum_{i=-n}^{\infty} a_i p^i$$

where $n \in \mathbb{N} \cup \{0\}$, p is prime, and the a_i's are a sequence of natural numbers such that $0 \leq a_i \leq p-1$. This is defined as a *p-adic number*. In this way each x can be thought of as a power series in base p similarly to how usually a decimal number is a power series in base 10. The sequence can be written in the following way:-

$$\cdots a_i \cdots a_2 a_1 a_0 . a_{-1} \cdots a_{-n}$$

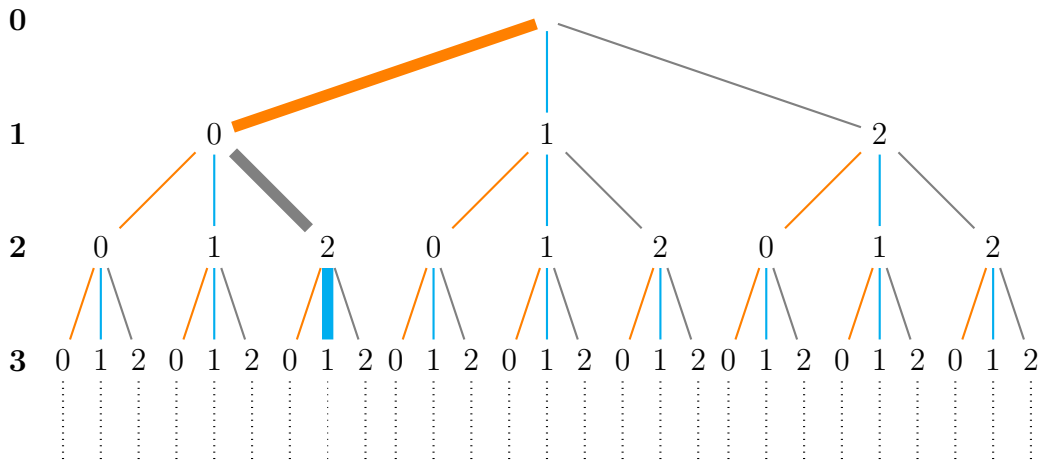


Figure 2.1: A 3-adic tree with levels labeled and the representation of ...120 highlighted

Notice that numbers here runs continuously to the left, whereas when in the realm of real numbers $\mathbb{R}$ they run continuously to the right (a number gets more precise as it has more decimal places). As an example of this, take $p = 5$ and a rational $x = \frac{241}{25}$ so it can be rewritten as follows:

$$x = 1 \cdot 5^{-2} + 3 \cdot 5^{-1} + 4 \cdot 5^{0} + 1 \cdot 5^{1},$$

and therefore as a p-adic, x can be written as 14.31.

Two p-adics are described as close to each other if the first difference in their sequences is a high power of p. The simplest way to imagine this in the p-adic numbers is by a tree structure as seen in Figure 2.1, two p-adic's are close to each other if the point at which they had a node in common is on a high level.

For example in Figure 2.1 ...120 is closer to ...220 than ...110. This is because ...120 and ...220 are one branch away from each other (they last had a node in common at level 2) where as ...120 and ...110 are two branches away (they last had a node in common at level 1).

Another way to think of p-adic numbers is as nested balls. This can be seen in Figures 2.2 and 2.3. In this context two p-adics are close to each other when the number of nested ball we must move through to get to one that they share is small.

In Figure 2.1 the choice of digit 0,1 or 2 was selected by taking the left, middle or right branch respectively, now in Figure 2.2 the choice of digit 0,1 or 2 will selected by taking the top, bottom left or bottom right circle respectively. It can be seen

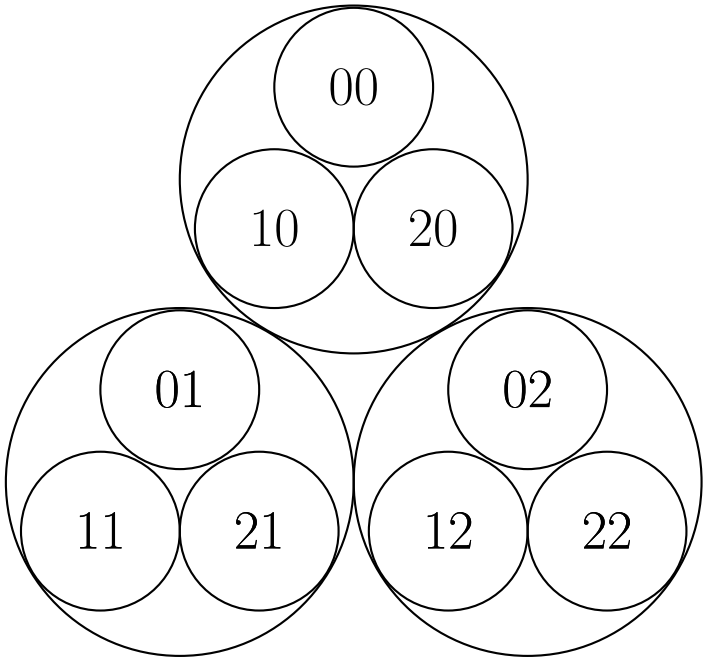


Figure 2.2: A 3-adic circle diagram showing positioning of numbers

that the larger circles dictates the digit on the right and the smaller circles indicate the digit to the left. This pattern continues and if the diagram is drawn to have more layers, the next digit will be added to the left. This additional layer is shown in Figure 2.3.

Again it can be seen by looking at Figure 2.3 that ...120 (in orange) is closer to ...220 (in cyan) than ...110 (in gray) as the orange and cyan balls are 1 layer apart whereas the orange and gray balls are two layers apart.

Both diagrams in Figure 2.1 and Figure 2.3 show the same basic information however, the different visualisations have different uses. The tree diagram shows the expansion of coefficients and their positions in the sequence in a simpler way whereas the circle diagram emphasizes the symmetric, modular and nested nature of the p-adic numbers. In this way when imagining the p-adic numbers it is important to consider both methods.

In both diagrams only numbers to the left of the decimal point have been considered, i.e. those of the form

$$x = \sum_{i=n}^{\infty} a_i p^i$$

where $n \in \mathbb{N} \cup \{0\}$ and $0 \leq a_i \leq p-1$. These p-adic numbers are called *p-adic integers*. Both diagrams can be expanded though to show the more general p-adic

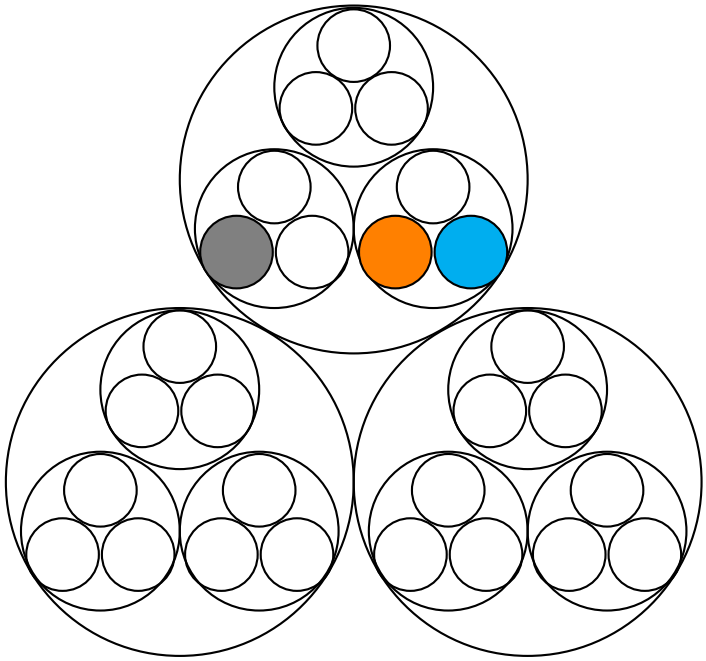


Figure 2.3: A 3-adic circle diagram with ...120 coloured in orange, ...220 in cyan and ...110 in gray

number by adding a layer further upwards. This would be adding a layer 0 or -1 in the tree diagram or larger circles around everything in the circular diagram.

2.2 STANDARD RESULTS FOR p-ADICS

In this Section the facts discussed previously will be formalised.

Let K be a field. A *valuation* on K is a map $|\cdot| : K \to \mathbb{R}$ satisfying for all $x, y \in K$

A1. $|x| \geq 0$ and $|x| = 0$ if and only if $x = 0$,

A2. $|x + y| \leq |x| + |y|$ (triangle inequality),

A3. $|xy| = |x||y|$.

A valuation on K is called *non-Archimedean* or *ultrametric* if it satisfies the stronger triangle inequality

$$|x + y| \leq \max(|x|, |y|)$$

for all $x, y \in K$, otherwise it is called *Archimedean*. The usual norm $|\cdot|_\infty$ on $\mathbb{R}$ is an example of a valuation that is Archimedean while the valuation on the p-adic

numbers satisfies the stronger triangle inequality and is thus non-Archimedean. We will see this property of the p-adic valuation in more detail later in this section.

Now that we have the tools to formally introduce the p-adic valuation.

Suppose that $x \in \mathbb{Q}$, then it can be written in the following way:

$$x = p^{\alpha}\frac{a}{b}$$

where $\alpha, a, b \in \mathbb{Z}$, $b \neq 0$, $p \nmid a$ and $p \nmid b$. From this the *p-adic valuation* (or *order*) can be defined as a function $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$,

$$v_p(x) := \begin{cases} \alpha, & \text{if } x = p^{\alpha}\frac{a}{b} \\ \infty, & \text{if } x = 0 \end{cases}$$

with α, a, b defined as above. The p-adic valuation has the following properties for $u, v \in \mathbb{Q} \setminus \{0\}$:

V1. $v_p(uv) = v_p(u) + v_p(v)$,

V2. $v_p(u + v) \geq \min\{v_p(u), v_p(v)\}$,

V3. if $v_p(u) \neq v_p(v)$, then $v_p(u + v) = \min\{v_p(u), v_p(v)\}$,

V4. $v_p(x) = \infty \Leftrightarrow x = 0$.

From here the *p-adic absolute value* or *p-adic norm* of $a \in \mathbb{Q}$ is defined as

$$|a|_p = \begin{cases} p^{-v_p(a)} & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases}$$

and has the following properties

P1. $|ab|_p = |a|_p \cdot |b|_p$,

P2. $|a + b|_p \leq \max\{|a|_p, |b|_p\} \leq |a|_p + |b|_p$,

P3. $|x|_p = 0 \Leftrightarrow x = 0$.

The set of p-adic numbers is defined as the completion of $\mathbb{Q}$ with respect to the p-adic absolute value and is denoted by $\mathbb{Q}_p$. Note that the elements of $\mathbb{Q}_p$ also satisfy properties P1-P3 stated above. It can also be seen from the property 2 that the p-adic norm satisfies the strong triangle inequality and hence is ultrametric. A key property of the space being ultrametric is given by the following lemma. Before this we will introduce the following notation. Throughout, *open ball* centred at $x_0 \in \mathbb{Q}_p$ with radius $r > 0$ will be denoted as

$$B(x_0, r) = \{x \in \mathbb{Q}_p : |x - x_0|_p < r\},$$

and a *closed ball*, that is the one that uses $\leq$ instead of $<$, will be denoted with square brackets (i.e. $B[x_0, r]$). Later we shall see that open balls are in fact closed balls.

Lemma 2.2.1. *Suppose that $x, y \in \mathbb{Q}_p$ and $r > 0$ then*

$$y \in B[x, r] \Leftrightarrow B[y, r] = B[x, r].$$

The proof of this can be found as Proposition 2.3.6 of [28]. This lemma gives an idea of the structure of p-adics. Every point inside of a given ball is also the centre of the ball which is very different from the Euclidean case. It implies that all points within a ball are equally close to each other which can be seen in the hierarchical structure of the nested balls. This clustering impacts the way that functions and series behave within the space. An example of this can be seen when looking at the series

$$S = \sum_{n=0}^{\infty} 5^n.$$

In Euclidean space this grows rapidly and without bound, however, in the p-adic metric the series does have a limit $(-1/4)$ and is therefore bounded.

From the definition of the p-adic norm it follows that for x to be a p-adic integer then $|x|_p \leq 1$ and this can be seen as an alternative definition. Another observation is that p-adic numbers which are divisible by a higher power of p will have a smaller p-adic norm. The field of p-adic numbers can be defined as the set

$$\mathbb{Q}_p = \left\{ \frac{a}{b} : b \neq 0, a, b \in \mathbb{Z}_p \right\}$$

with the operations $+$ and $\cdot$ as they are defined in the quotient field.

Now we will establish a direct connection between the p-adic norm and congruences modulo powers of p.

Lemma 2.2.2. *For any $y \in \mathbb{Q}$ the following identity holds*

$$|y|_p \leq p^{-b} \Leftrightarrow y \equiv 0 \mod p^b.$$

Proof. Suppose first that $|y|_p \leq p^{-b}$, this means that $|y|_p = p^{-m}$ for some $m \in \mathbb{Z}$ and $p^{-m} \leq p^{-b}$. Then as $b \leq m$ it must be that y is a multiple of p^b and hence $y \equiv 0 \mod p^b$. If instead it is supposed that $y \equiv 0 \mod p^b$ then $y = p^b \cdot k$ for some $k \in \mathbb{Z}$. Therefore, it follows that $|y|_p = |p^b|_p |k|_p = p^{-b} \cdot |k|_p$ and as $k \in \mathbb{Z}$ we have that $|k|_p \leq 1$ so therefore $|y|_p \leq p^{-b}$. □

This statement aids in showing a direct relationship between the divisibility of a p-adic y by the powers of p and how the concept of size is closely tied to divisibility. Indeed by letting $b = 0$, it also clarifies the idea that $|y|_p \leq 1$ implies that $y \in \mathbb{Z}_p$.

2.2.1 TOPOLOGY IN $\mathbb{Q}_p$

The field of p-adic numbers $\mathbb{Q}_p$ with the standard ultrametric topology is a locally compact topological group. The p-adic norm induces a distance function

$$d(x, y) = |x - y|_p$$

on $\mathbb{Q}_p$ and this can be used to define the topology on $\mathbb{Q}_p$. The open sets that form the basis of the topology are the open balls $B(x, r)$. A key feature of the topology is the following lemma.

Lemma 2.2.3. *In $\mathbb{Q}_p$ a ball is open if and only if it is closed.*

The proof of this can be found in [28, Proposition 2.3.6]. Thus, every ball in the p-adic topology is clopen, that is both open and closed.

This result shows that $\mathbb{Q}_p$ is a totally disconnected space, which significantly influences the analysis and structure within the p-adic setting. An example of this can be seen by looking again at the convergence of a p-adic sequence. A sequence $\{a_n\}$ converges to a point $a \in \mathbb{Q}_p$ if there exists a ball around a that eventually contains all the terms of the sequence for large enough n. Since these balls are clopen, any sequence within a ball stays within it with no gradual approach to an external boundary. This greatly simplifies a convergence criteria because once the terms of the sequence enter a clopen ball around the limit, they remain in that ball permanently. This means that there is no need to consider boundary points or asymptotic approaches as in real analysis. Another consequence of this is the following lemma.

Lemma 2.2.4. *The field $\mathbb{Q}_p$ is locally compact.*

The proof of this can be found in [28, Corollary 3.3.8].

Let $S = \{p_1, p_2, ..., p_{l-1}, \infty\}$. Define now the subset S_f of S to be $\{p_1, p_2, ..., p_{l-1}\}$ and define the *ring of S-adic integers* of $\mathbb{Q}$ to be

$$\begin{aligned} \mathbb{Z}_S &:= \mathbb{Z}\left[\frac{1}{p_1}, \cdots, \frac{1}{p_{l-1}}\right] \\ &= \{x \in \mathbb{Q} : x \in \mathbb{Z}_p \text{ for all primes } p \notin S_f\}. \end{aligned} \tag{2.1}$$

This can be described as the set of all fractions where the denominator is composed of the multiplication of elements from $S_f \cup \{1\}$.

We now discuss the measure on the p-adic space. Define $\mathcal{A}(\mathbb{Q}_p)$ to be the σ-algebra (the family of open subsets of $\mathbb{Q}_p$). Then $\mu : \mathcal{A}(Q_p) \to [0, \infty]$ is defined to be a Haar measure with the following properties:

1. $\mu \neq 0$,
2. for a compact subset $K \subset \mathcal{A}(\mathbb{Q}_p)$ we have $\mu(K) < \infty$,
3. for $a \in \mathbb{Q}_p$ and $K \in \mathcal{A}(\mathbb{Q}_p)$, $\mu(a + K) = \mu(K)$.

As $\mathbb{Q}_p$ is locally compact there exists a unique Haar measure μ such that the p-adic integer have measure 1, $\mu(\mathbb{Z}_p) = 1$.

Finally the compact sets of $\mathbb{Q}_p$ will be discussed. In $\mathbb{Q}_p$, as in $\mathbb{R}$, a set is compact iff it is closed and bounded. The reason why this is the case for the two fields is different however. In $\mathbb{R}$, the Bolzano–Weierstrass theorem states that closed and bounded sets are sequentially compact. Additionally due to the topology of $\mathbb{R}$ the terms compact and sequentially compact are equivalent, so we have that compact sets are those sets that are closed and bounded. In contrast to show the same result holds in $\mathbb{Q}_p$ we will use the fact that in a complete and totally bounded space, a set is compact. $\mathbb{Q}_p$ has an ultrametric topology and so by the strong triangle inequality a set being bounded automatically implies that it is totally bounded. Combining this with the completeness of $\mathbb{Q}_p$ gives that the closed and bounded set of $\mathbb{Q}_p$ are compact. For example, closed balls in $\mathbb{Q}_p$ are compact and so the set of p-adic integers $\mathbb{Z}_p$ is compact.

2.2.2 THE SPACE $\mathbb{Q}_S^m$

For some set $S = \{p_1, p_2, ..., p_{l-1}, \infty\}$ of primes (and infinity), for $l \in \mathbb{N}$, define $\mathbb{Q}_S^m$ to be the direct product of $\mathbb{Q}_v^m$ for $v \in S$,

$$\mathbb{Q}_S^m = \mathbb{Q}_{p_1}^m \otimes \mathbb{Q}_{p_2}^m \otimes \cdots \otimes \mathbb{Q}_{p_l-1}^m \otimes \mathbb{Q}_\infty^m.$$

Elements $\mathbf{x} \in \mathbb{Q}_S^m$ will be denoted as $\mathbf{x} = (\mathbf{x}^{(v)})$, $v \in S$, where $\mathbf{x}^{(v)} = (x_1^{(v)}, ..., x_m^{(v)}) \in \mathbb{Q}_v^m$. The absolute value will be denoted as $|\cdot|_v$ for all $v \in S$ where $|\cdot|_\infty$ is the usual absolute value in $\mathbb{R}$.

Now we will discuss the p-adic norm of a vector. Let $m \in \mathbb{N}$ and $\mathbb{Q}_p^m$ denote a vector space over $\mathbb{Q}_p$ which consists of all points $\mathbf{x} = (x_1, x_2, ..., x_m)$, where

$x_1, x_2, ..., x_m$ are in $\mathbb{Q}_p$. Define the *p-adic norm* on $\mathbb{Q}_p^m$ by

$$||\mathbf{x}||_p = \max_{1 \leq j \leq m} |x_j|_p, \qquad \text{for } \mathbf{x} \in \mathbb{Q}_p^m. \tag{2.2}$$

For example, suppose that $p = 7$ and let

$$\mathbf{a} = \begin{pmatrix} 7^{-5} \cdot 1 \\ 7^{12} \cdot 3 \\ 7^3 \cdot 6 \end{pmatrix}$$

Then $||\mathbf{a}||_p = \max\{7^5, 7^{-12}, 7^{-3}\} = 7^5$.

2.2.3 Hensel's Lemma

This lemma has many versions and has been adapted many times. The most common version finds simple roots and reads as follows.

Theorem 2.2.5. *Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ be a polynomial whose coefficients are in $\mathbb{Z}_p$. Suppose that there exists $\alpha_1 \in \mathbb{Z}_p$ such that*

$$\begin{aligned} f(\alpha_1) &\equiv 0 \qquad \textit{mod } p, \\ f'(\alpha_1) &\not\equiv 0 \qquad \textit{mod } p. \end{aligned}$$

Then there exists a unique $\alpha \in \mathbb{Z}_p$ such that

$$f(\alpha) = 0 \quad \textit{and} \quad \alpha \equiv \alpha_1 \textit{ mod } p.$$

A proof of this lemma can be found in [37, Theorem 3]. A variant which considers the use of modulo $p\mathbb{Z}_p$ rather that p can be found in [28] as Theorem 3.4.1. A version which is closer to the one that shall be used in this thesis can be found in [21], this uses the condition that $|f(a)|_p < |f'(a)|_p^2$ and so can find roots that are not simple.

The following Theorem is taken from [22] where two proofs can be found in sections 5 and 6

Theorem 2.2.6 (Hensel's Lemma)**.** *Let $f(x) \in \mathbb{Z}_p[x]$ and $a \in \mathbb{Z}_p$ for a fixed p. Suppose that $|f(a)|_p < |f'(a)|_p^2$. Then there exists a unique $z \in \mathbb{Z}_p$ such that the following three conditions hold:*

1. $f(z) = 0$,
2. $|z - a|_p = \left|\frac{f(a)}{f'(a)}\right|_p < |f'(a)|_p$,

3. $|f'(z)|_p = |f'(a)|_p$.

It can be seen that the idea of this theorem is very similar to that of the Newton–Raphson method for finding roots of equations. Whereas the latter is used for finding approximations to roots, the former is used to find exact solutions. Another difference between the two is that the Newton–Raphson method does not always converge to a root but Hensel's Lemma guarantees a root if the conditions required are met. Indeed later in Section 5.5 Hensel's Lemma will be used to find a p-adic root of a polynomial equation.

2.3 DEFINITIONS

This Section will state the main definitions and notations that will be used throughout the thesis.

A *partially ordered* set is a set combined with a binary relation that is reflexive, antisymmetric and transitive. A metric space X is said to be *Besicovitch* if there exists a constant N_X such that for any bounded subset A of X and any family of non-empty open balls $\mathcal{B} \in X$ such that for every $x \in A$ it follows that x is the centre of some ball of $\mathcal{B}$, there exists a finite subfamily $\{B_i\}$ of balls from $\mathcal{B}$ with the property that

$$1_A \leq \sum_i 1_{B_i} \leq N_X,$$

where 1_A and 1_{B_i} are indicator functions. An example of a Besicovitch metric space is the p-adics where $N_X = 1$ because of the nested property of balls.

A locally finite Borel measure μ on X is called *uniformly Federer* if for all $c > 1$,

$$D_\mu(c) := \sup_{x \in \operatorname{supp}\mu, r>0} \frac{\mu(B(x,cr))}{\mu(B(x,r))} < \infty \tag{2.3}$$

for all $x \in \operatorname{supp}(\mu)$. This definition can be found in [35].

An example of a measure μ being uniformly Federer is Lebesgue measure on $\mathbb{R}$. This can be seen for a ball $B(x,r)$, it follows that $\mu(B(x,cr)) = cr$, hence

$$\sup_{r>0} \frac{\mu(B(x,cr))}{\mu(B(x,r))} = \frac{2cr}{2r} = c.$$

Therefore for every $c > 1$ it is that $D_\mu(c) < \infty$.

Another example we will look at is Haar measure on $\mathbb{Q}_p$. Due to the discrete nature of the measure, it is that the measure of the p-adic ball is the largest power of p such that the radius is bigger than it. So for the balls $B(x,r)$ and $B(x,cr)$ it is that

$$p^{-n-1} < r \leq p^{-n}, \tag{2.4}$$
$$p^{-m-1} < cr \leq p^{-m}. \tag{2.5}$$

Therefore the ratio can be seen to be

$$\sup_{r>0} \frac{\mu(B(x,cr))}{\mu(B(x,r))} \leq p^{-m+n}.$$

Multiplying the equation (2.4) by c it can be combined with equation (2.5) to get the bound $p^{-m-1} < cp^{-n}$ and hence $p^{-m+n} < cp$ so that for every $c > 1$, $D_\mu(c) < cp < \infty$.

In the case that $c = 3$, we write D_μ rather than $D_\mu(c)$ in equation (2.3). Additionally it is that μ is Federer if for μ-almost everywhere and $x \in X$ there exists a neighbourhood U of x, such that $\mu|_U$ is uniformly Federer.

2.3.1 Exterior Product

The *exterior product* (or *wedge product*) of two vectors $\mathbf{a}$ and $\mathbf{b}$ in a vector space will be denoted as $\mathbf{a} \wedge \mathbf{b}$. It is a mathematical bilinear operation that, geometrically, represents the oriented area of the parallelogram spanned by the vectors $\mathbf{a}$ and $\mathbf{b}$. The result is a bivector that encodes both the area and orientation of the parallelogram spanned by $\mathbf{a}$ and $\mathbf{b}$. A key property of the exterior product is that it is antisymmetric, so that

$$\mathbf{a} \wedge \mathbf{b} = -\mathbf{b} \wedge \mathbf{a}.$$

In particular if the two vectors $\mathbf{a}$ and $\mathbf{b}$ are parallel then their exterior product is zero. This property is useful in establishing the linear independence of vectors.

For a matrix V composed of the k vectors $\mathbf{v}_1, ..., \mathbf{v}_k \in \mathbb{R}^n$, the exterior product $\mathbf{v}_1 \wedge \cdots \wedge \mathbf{v}_k$ is known to be associated with the determinant of V. This is because the exterior product captures the orientated volume of the parallelotope formed by the vectors, this information can equally be displayed as the determinant. When $k = n$, the determinant is the exact volume of the parallelotope in $\mathbb{R}^n$ and when $k < n$, the determinant measures the k-dimensional volume of the parallelotope embedded in the higher n-dimensional space.

Denote the standard basis of $\mathbb{R}^n$ to be the vectors $e_1 = (1, 0, ..., 0), ..., e_n = (0, 0, ..., 1)$. Then for $1 \leq p \leq n$ and integers $1 \leq i_1 < i_2 < \cdots < i_p \leq n$ the elements

$$e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_p}$$

form a basis of $\mathbb{R}^n_p$ of dimension $l = \binom{n}{p}$. This is known to be the standard basis of the wedge product.

An application of this can be seen as the Laplace identity as described by Schmidt in his book Diophantine Approximation [43] which says that for $\mathbf{x}_1, ..., \mathbf{x}_p, \mathbf{y}_1, ..., \mathbf{y}_p$ the following holds true:-

$$(\mathbf{x}_1 \wedge \cdots \wedge \mathbf{x}_p) \cdot (\mathbf{y}_1 \wedge \cdots \wedge \mathbf{y}_p) = \begin{vmatrix} \mathbf{x}_1\mathbf{y}_1 & \mathbf{x}_1\mathbf{y}_2 & \dots & \mathbf{x}_1\mathbf{y}_p \\ \mathbf{x}_2\mathbf{y}_1 & \mathbf{x}_2\mathbf{y}_2 & \dots & \mathbf{x}_2\mathbf{y}_p \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{x}_p\mathbf{y}_1 & \mathbf{x}_p\mathbf{y}_2 & \dots & \mathbf{x}_p\mathbf{y}_p \end{vmatrix}. \tag{2.6}$$

This equation can be seen to be true as both sides gives the volume of the body. The left hand side of (2.6) represents the dot product of the two oriented volumes formed by the vectors $\mathbf{x}_1, ..., \mathbf{x}_p$ and $\mathbf{y}_1, ..., \mathbf{y}_p$. That is to say the volume of the body described by the determinant of the multiplication of the matrix where the rows are each $\mathbf{x}_i$ and the matrix where each column is each $\mathbf{y}_j$, i.e. -

$$\begin{pmatrix} \cdots & \mathbf{x}_1 & \cdots \\ \cdots & \mathbf{x}_2 & \cdots \\ & \vdots & \\ \cdots & \mathbf{x}_p & \cdots \end{pmatrix} \begin{pmatrix} \vdots & \vdots & & \vdots \\ \mathbf{y}_1 & \mathbf{y}_2 & \cdots & \mathbf{y}_p \\ \vdots & \vdots & & \vdots \end{pmatrix},$$

which is exactly the right hand side of (2.6). This method will be used later in Section 5.3.2 to expand out a determinant of a Wronskian matrix.

2.3.2 Minkowski Theorems

A set $H \subset \mathbb{R}^n$ is a *convex set* if for any $x, y \in H$ we can draw a line between them that is completely contained in H and a *convex body* is a complete convex set with non-empty interior. A convex body H is *symmetric about the origin* if for any $a \in H$ we have $-a \in H$. The convex body H is said to be *strictly convex* if for x and y in the closure of H, (denoted $\bar{H}$) with $x \neq y$, all points

$$\theta x + (1 - \theta)y$$

with $0 < \theta < 1$ are all inner points of H.

Now there is enough information to state the Minkowski Theorems which establish connections between convex bodies and lattice points.

Theorem 2.3.1 (Minkowski's First Theorem)**.** *A bounded convex body K which is symmetric about the origin in $\mathbb{R}^n$ with volume $\mathrm{vol}(K) > 2^n$ contains at least one point u (not equal to the origin) with integral coordinates.*

This essentially says that if a convex body has enough volume then it is guaranteed to contain a non-zero lattice point. This theorem will be used later to show that a system of equations has a non-zero solution.

Minkowski's Second Theorem introduces the concept of successive minima, which helps to understand how a convex body interacts with the underlying lattice. For a bounded convex body K, over a lattice Γ, which is symmetric about the origin, let λ be a positive number and consider the body λK, that is the body obtained by scaling K uniformly in all directions by a factor of λ. If λ is sufficiently small then λK does not contain any point except the origin. Given $i \in \mathbb{R}$ by increasing the size of λ, λK contains i independent lattice points. From this, define λ_i to be the the greatest lower bound of λ such that λK contains i independent lattice points. In other words:

$$\lambda_i = \inf\{\lambda : \lambda > 0, \dim(\lambda K \cap \Gamma) \geq i\}$$

for $i = 1, ..., n$. The numbers λ_i are called the *successive minima* of K and necessarily it must be that,

$$0 < \lambda_1 \leq \cdots \leq \lambda_n.$$

Theorem 2.3.2 (Minkowski's Second Theorem)**.** *Let Γ be a lattice in $\mathbb{R}^n$ and $B \subset \mathbb{R}^n$ be a bounded convex body which is symmetric about the origin with successive minima $\lambda_1, ..., \lambda_n$ over Γ. Then*

$$\frac{2^n}{n!}\,\mathrm{vol}(\mathbb{R}^n/\Gamma) \leq \lambda_1\lambda_2\cdots\lambda_n\,\mathrm{vol}(B) \leq 2^n\,\mathrm{vol}(\mathbb{R}^n/\Gamma).$$

This gives a bound on the product of the successive minima of a convex body which will be used later when scaling a convex body to ensure a non-zero point is still present.

— 3 —

Distribution of Algebraic Numbers

As already mentioned in the introduction, the problems that will be addressed in this thesis were first studied extensively in the Archimedean case. In this Section we give an overview of previous results as well as state the new results obtained in this thesis.

The notation used in the papers on the topic varies, so first, we will introduce notation that will be used in this thesis for clarity and consistency. Given an integer polynomial $P = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, define the height of P as

$$H(P) := \max_{0 \le i \le n} |a_i|. \tag{3.1}$$

For a given field L, define $\overline{L}$ to be the algebraic closure of L. Let $\mathcal{C}_n$ be an infinite subclass of polynomials in $\mathbb{Z}[x]$ with $\deg P = n$. Then for L satisfying $K \subset L \subset \overline{K}$, where K is either $\mathbb{Q}_p$ or $\mathbb{R}$, define $\boldsymbol{\kappa(L, \mathcal{C}_n)}$ to be the infimum of all κ such that for all polynomials $P \in \mathcal{C}_n$ of sufficiently large height

$$|\alpha_1 - \alpha_2| > H(P)^{-\kappa}$$

holds for any pair of roots $\alpha_1 \neq \alpha_2 \in L$ of P. That is to say that $\kappa(L, \mathcal{C}_n)$ is the largest real number such that for any $\kappa < \kappa(L, \mathcal{C}_n)$ it is possible to find infinitely many $P \in \mathcal{C}_n$ such that

$$|\alpha_1 - \alpha_2| \le H(P)^{-\kappa}$$

holds for some roots $\alpha_1 \neq \alpha_2 \in L$ of P.

The goal of Chapter 5 is to obtain lower bounds for

$$\kappa_{\mathrm{irr}}(n, p) := \kappa(\overline{\mathbb{Q}_p}, \mathcal{P}_{\mathrm{irr}}(n)),$$

where $\mathcal{P}_{\text{irr}}(n)$ (*resp.* $\mathcal{P}^*_{\text{irr}}(n)$) is the set of all irreducible (*resp.* monic irreducible) integer polynomials of degree n.

As stated above this problem has been intensively studied in the Archimedean case, in which the most studied exponents are $\kappa_{\text{irr}}(n) := \kappa(\mathbb{C}, \mathcal{P}_{\text{irr}}(n))$ and $\kappa^*_{\text{irr}}(n) := \kappa(\mathbb{C}, \mathcal{P}^*_{\text{irr}}(n))$, as well as their analogues for all and all reducible integer polynomials:

$$\kappa_{\text{all}}(n) := \kappa(\mathbb{C}, \mathcal{P}(n)), \qquad \kappa^*_{\text{all}}(n) := \kappa(\mathbb{C}, \mathcal{P}^*(n))$$

$$\kappa_{\text{red}}(n) := \kappa(\mathbb{C}, \mathcal{P}_{\text{red}}(n)), \qquad \kappa^*_{\text{red}}(n) := \kappa(\mathbb{C}, \mathcal{P}^*_{\text{red}}(n))$$

where $\mathcal{P}(n)$, $\mathcal{P}^*(n)$, $\mathcal{P}_{\text{red}}(n)$, $\mathcal{P}^*_{\text{red}}(n)$ are the sets of all, all monic, all reducible and all monic reducible integer polynomials of degree n respectively.

3.1 REAL AND COMPLEX CLOSE ROOTS

The earliest study of this problem was in 1964 by Mahler [39]. Rather than using the height of a polynomial he used the so called Mahler measure, denoted $M(P)$ which is defined for a polynomial P as above with roots $\alpha_1, ..., \alpha_n$ as

$$M(P) = |a_n| \prod_{i=1}^{n} \max(1, |\alpha_i|).$$

It can be shown however that Mahler measure is comparable to height as

$$\binom{n}{\lfloor \frac{n}{2} \rfloor}^{-1} H(P) \leq M(P) \leq H(P)\sqrt{n+1}.$$

Using this he proved that $\kappa_{\text{irr}}(n) \leq n - 1$. To obtain this result he used methods concerning discriminants. He actually proved his result for a wider set of polynomials that do not have a repeated root.

Forty years later in 2004, Evertse [26] proved that $\kappa_{\text{all}}(3) = 2$. Similarly in this paper, Evertse used Mahler measure for the estimate rather than height. The proof of this heavily leans on the following lemma

Lemma 3.1.1. *Let α be a real, irrational algebraic number and let $\beta_1, ..., \beta_n$ be different complex numbers different from α. Then for every $\delta > 0$ and every Q which is sufficiently large in terms of δ, there is a matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL(2, \mathbb{Z})$ such that*

$$\begin{aligned} Q^{-1-\delta} \leq |\alpha a + b|, |\alpha c + d| \leq Q^{-1+\delta}, \\ Q^{1-\delta} \leq |\beta_i a + b|, |\beta_i c + d| \leq Q^{1+\delta} \quad (i = 1, ..., n). \end{aligned}$$

An alternative proof of $\kappa_{\text{all}}(3) = 2$ is by Schönhage can also be found in [44] where he used arguments involving the discriminant (similarly to the method of Mahler).

Then in 2010, Beresnevich, Bernik and Götze [5] used methods relying on quantitative non-divergence estimates (this method will be discussed in greater detail later in chapter 4) to show that

$$\min\{\kappa_{\text{irr}}(n), \kappa^*_{\text{irr}}(n+1)\} \geq (n+1)/3.$$

Furthermore, it was also proved true for the field being restricted to just the real numbers, - i.e.

$$\min\{\kappa(\mathbb{R}, \mathcal{P}_{\text{irr}}(n)), \kappa(\mathbb{R}, \mathcal{P}^*_{\text{irr}}(n+1))\} \geq (n+1)/3.$$

In 2011, Bugeaud and Mignotte [19] in which they proved many results regarding general and irreducible polynomials. Among them, they proved the statement that $\kappa_{\text{all}}(3) = \kappa_{\text{irr}}(3) = 2$ using ideas similar to that of Schönhage. They did go a step further in the proof of this as their proof incorporated the idea of product of root distances. That is for k and n being integers such that $2 \leq k \leq n$, let $K_{\text{irr}}[n,k]$ (*resp.* $K^*_{\text{irr}}[n,k]$) be the infimum of all κ such that

$$\prod_{1 \leq i < j \leq k} |\alpha_i - \alpha_j| \geq H(P)^{-\kappa},$$

where $\alpha_1, ..., \alpha_n$ are roots of the polynomial P. They showed that $K_{\text{irr}}[n, n-1] = n-1$ for $n \geq 3$. Additionally they showed for $n \geq 4$ and any integer $k \geq 2$ such that k divides n it is that $K_{\text{irr}}[n,k] \leq \frac{n(k-1)}{k}$. These statements can be found as Theorem 3 of [19] and while interesting the study of $K_{\text{irr}}[n,k]$ and $K^*_{\text{irr}}[n,k]$ will not be discussed further.

Additionally in this paper [19] they found results for $\kappa_{\text{irr}}(2), \kappa_{\text{all}}(2), \kappa^*_{\text{irr}}(2)$ and $\kappa^*_{\text{all}}(2)$ by considering the distance

$$\text{sep}(P) := \min\{|\alpha_i - \alpha_j| : 1 \leq i < j \leq n\}$$

so that the question of root seperation can be restated as

$$\text{sep}(P) \geq H(P)^{-(n-1)}.$$

In this way by considering a square free quadratic polynomial $P(x) = ax^2 + bx + c$ with $a > 0$ and discriminant Δ the exact formula

$$\text{sep}(P) = \frac{\sqrt{|\Delta|}}{a}$$

can be seen. They then choose more specific values of a, b and c to get exact values of Δ so as to show that

$$\kappa_{\text{irr}}(2) = \kappa_{\text{all}}(2) = 1;$$
$$\kappa^*_{\text{irr}}(2) = \kappa^*_{\text{all}}(2) = 0.$$

Note that the root separation in question is always considered between distinct roots. This avoids the trivial case of repeated roots and ensures that all bounds on $\kappa_{irr}, \kappa_{all}, \kappa^*_{irr}$ and κ^*_{all} are non-trivial. The approach that Bugeaud and Mignotte take is to take an integer polynomial that originally has one root repeated k times, and then modify it slightly to produce a new polynomial with k distinct roots that are nearly the same.

In the same paper [19] as Theorem 2, they stated and proved that

- for any even integer $n \geq 4$, $\kappa_{\text{all}}(n) \geq \kappa_{\text{irr}}(n) \geq \frac{n}{2}$;
- for any odd integer $n \geq 5$, $\kappa_{\text{all}}(n) \geq \frac{n+1}{2}$ and $\kappa_{\text{irr}}(n) \geq \frac{n+2}{4}$.

Then as Theorem 4 they stated that $\kappa^*_{\text{irr}}(3) = \kappa^*_{\text{all}}(3) \geq 3/2$ with equality if Hall's conjecture is true. Where Hall's conjecture is that if for any $\varepsilon > 0$, there exists a constant $c(\varepsilon) > 0$ such that if x and y are positive integers satisfying $x^3 \neq y^2$, then $|x^3 - y^2| > c(\varepsilon)x^{1/2-\varepsilon}$. Finally as Theorem 5, they stated that

- for any even integer $n \geq 4$, $\kappa^*_{\text{all}}(n) \geq n/2$ and $\kappa^*_{\text{irr}}(n) \geq \frac{n-1}{2}$;
- for any odd integer $n \geq 5$, $\kappa^*_{\text{all}}(n) \geq \frac{n-1}{2}$ and $\kappa^*_{\text{irr}}(n) \geq \frac{n+2}{4}$.

Later in the same year, Bugeaud and Dujella [17] obtained the following:

- for any integer $n \geq 4$, $\kappa_{\text{irr}}(n) \geq n/2 + \frac{n-2}{4(n-1)}$;
- for any odd integer $n \geq 7$, $\kappa^*_{\text{irr}}(n) \geq n/2 + \frac{n-2}{4(n-1)} - 1$.

To prove these, Bugeaud and Dujella construct a one-parametric family of irreducible integer polynomials denoted as $P_{n,a}(x)$.

In a subsequent paper in 2014 Bugeaud and Dujella [18] proved that

- for any even positive integer $n \geq 6$, $\kappa^*_{\text{all}}(n) \geq \frac{2n-3}{3}$;
- for any odd positive integer $n \geq 7$, $\kappa^*_{\text{all}}(n) \geq \frac{2n-5}{3}$;
- for any positive integer $n \geq 4$, $\kappa^*_{\text{irr}}(n) \geq \frac{n}{2} - \frac{1}{4}$.

Again in these proofs they construct parametric families of integer polynomials

In 2017, Dujella and Pejković [25] found new bounds for reducible monic polynomials of specific degrees:

- $3 \geq \kappa^*_{\text{red}}(5) \geq \frac{7}{3}$;
- $5 \geq \kappa^*_{\text{red}}(7) \geq \frac{17}{5}$;
- $7 \geq \kappa^*_{\text{red}}(9) \geq \frac{31}{7}$.

by again construct parametric families of integer polynomials.

In 2020, for arbitrary degree Dubickas [24] found that

$$\frac{n}{2} \leq \kappa_{\text{red}}(n) \leq \frac{3n-2}{4}.$$

This estimate comes from looking at a separable integer polynomial P of degree $n \geq 3$ and its derivative P'. By letting $m \leq n-1$ be the largest positive integer such that P' has an irreducible factor over $\mathbb{Q}$ of degree m it can be seen that

$$\kappa_{\text{red}} \leq \frac{n+m-1}{2}.$$

Then by considering trinomial P (or its reciprocal) of the form $a_0 + a_{n-l}x^{n-l} + a_n x^n$ where $1 \leq l \leq \lfloor n/2 \rfloor$ it must be that $m \leq l$ and so

$$\kappa_{\text{red}} \leq \frac{n+l-1}{2}.$$

and by the conditions on l the bound can be obtained.

3.1.1 Wirsing's problem

A similar problem to the one considered in this thesis is that of Wirsing's problem. Before stating this we will introduce the classifications of Mahler and Koksma. The former will be discussed later in Section 3.2 but will be introduced here for completeness and for comparison to the latter classification.

Mahler's classification divides the set of real numbers ξ by how accurate a non-zero polynomial evaluated at ξ approaches 0. Define $\omega_n(\xi)$ to be the supremum of real numbers ω such that there exists infinity many integer polynomials $P(X)$ of degree less than or equal to n that satisfy

$$0 < |P(\xi)| \leq H(P)^{-\omega}.$$

Also define

$$\omega(\xi) = \limsup_{n \to +\infty} \frac{\omega_n(\xi)}{n}.$$

The classification of a real number ξ is as such:

- ξ is an A-number if $\omega(\xi) = 0$,
- ξ is an S-number if $0 < \omega(\xi) < \infty$,
- ξ is an T-number if $\omega(\xi) = \infty$ and $\omega_n(\xi) < \infty$ for all $n \geq 1$,
- ξ is an U-number if $\omega_n(\xi) = \infty$ for all n greater than some $N \in \mathbb{N}$.

These classes can be broken down further but will not be discussed here. Further details can be found in [16].

Koksma's Classification considers the approximation of ξ by algebraic numbers. Define $\omega_n^*(\xi)$ to be the supremum of real numbers ω such that there exists infinity many real algebraic numbers α of degree less than or equal to n that satisfy

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

where $H(\alpha)$ is the the height of the irreducible polynomial of which α is a root of.

Now there is enough information to state Wirsing's problem which is as follows:

Given any integer $n \geq 1$ and transcendental real ξ, do we have $\omega_n^*(\xi) \geq n$?

This problem can be found in Wirsing's 1961 paper [47] in which he established the bound that $\omega_n^*(\xi) \geq \frac{n+1}{2}$ for any transcendental real ξ. By Dirichlet's Theorem the problem is true for $n = 1$ and it was also shown to be true for $n = 2$ by Davenport and Schmidt [23]. Recent work around this include that done by Badziahin and Schleischitz [2] in 2019 who found that $\omega_n^*(\xi) \geq \frac{n}{\sqrt{3}}$ for $n \geq 4$. Then in 2024, Poëls [42] improved this to $\omega_n^*(\xi) \geq an$ where $a = \frac{1}{2-\log 2}$ for $n \geq 2$.

3.2 p-ADIC CLOSE ROOTS

There are far fewer results surrounding p-adic root separation so instead we will look at a more general introduction to the area where similar problems have been discussed.

In 1978, Morrison [40] proved results about the approximation of a p-adic $\xi \in \mathbb{Q}_p$ by algebraic numbers. That is he considered the p-adic version of Wirsing's problem discussed above. Specifically he had two results

- Let $\xi \in \mathbb{Q}_p$. If ξ is not algebraic of degree less than or equal to n, then there are infinitely many solutions $\alpha \in \mathbb{Q}_p$, to

$$|\xi - \alpha|_p \ll H(\alpha)^{-(n+3)/2}$$

where α is algebraic of degree at most n.

- Let $\xi \in \mathbb{Q}_p$. If ξ is not a rational or quadratic irrational there are infinitely many solutions $\alpha \in \mathbb{Q}_p$ to

$$|\xi - \alpha|_p \ll H(\alpha)^{-(1+\sqrt{3})}$$

with α rational or quadratic irrational.

Here the notation $f \ll g$ is used to mean $f \leq Cg$ where C is a constant depending only on ξ, n and p.

In 2004, Bugeaud discussed Mahler's and Koksma's functions in [16] (Section 9.3 (pages 194-199)) and how this classification could be extended to be used for p-adics. Similar to the work of Morrison, Bugeaud considered the approximation of a p-adic $\xi \in \mathbb{Q}_p$ by algebraic numbers, but he restricted his attention to those numbers within $\mathbb{Q}_p$.

This work was continued in 2015 when Bugeaud and Pejković [20] found explicit examples of p-adic numbers for which the values of Mahler's and Koksma's functions differ by any prescribed value from the interval $[0, 1]$ for polynomials with degree at most 2. Here they used families of close conjugate p-adic numbers to construct numbers with different Mahler and Koksma exponents.

In 2016, Pejković [41] found in the irreducible cubic case with $p \neq 2$, that $\kappa_{\text{irr}}(3, p) \geq 25/14$.

3.3 POLYNOMIALS WITH SMALL DISCRIMINANTS

The other problem which will be studied in this thesis will be on the estimate of the number of polynomials of bounded height and degree such that they have a small discriminant. That is to estimate the number of polynomials satisfying

$$0 < |D(P)| \leq \gamma H(P)^{2n-2-2\nu},$$

where

$$D(P) := a_n^{2n-2} \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2, \tag{3.2}$$

where a_n is the leading coefficient of P and $\alpha_1, \ldots, \alpha_n$ are its roots. Since $D(P) = 0$ if and only if $P(x)$ has repeated roots, the condition $0 < |D(P)|$ implies that $P(x)$ has distinct roots. Additionally, since we require the polynomials to have integer

coefficients, the discriminant must also be an integer. Therefore, we can restate the problem as estimating the number of polynomials satisfying

$$1 \leq |D(P)| \leq \gamma H(P)^{2n-2-2\nu}.$$

The analogous p-adic problem is to count polynomial of bounded height and degree such that

$$0 < |D(P)|_p \leq H(P)^{-2\nu} \tag{3.3}$$

for some $\nu > 0$.

Define the set of polynomials

$$\mathcal{P}_n(Q) := \{P \in \mathbb{Z}[x] : \deg P = n \text{ and } H(P) \leq Q\}.$$

To estimate the number of polynomials in $\mathcal{P}_n(Q)$ that have small discriminant, define the following set that combines the Archimedean and p-adic cases

$$\mathcal{D}_{n,\gamma_1,\gamma_2}(Q,\nu_1,\nu_2) := \left\{ P \in \mathcal{P}_n(Q) : \begin{array}{l} 1 \leq |D(P)| \leq \gamma_1 Q^{2n-2-2\nu_1} \\ \text{and } \ |D(P)|_p \leq \gamma_2 Q^{-2\nu_2} \end{array} \right\}.$$

In the case that $\gamma_i = 1$ for $i = 1$ or $i = 2$, the subscript will be dropped, for example $\mathcal{D}_n(Q,\nu_1,\nu_2) := \mathcal{D}_{n,1,1}(Q,\nu_1,\nu_2)$.

3.3.1 EUCLIDEAN CASE

To begin known results relating to the real/complex case will be stated, in this case it is that $\nu_2 = 0$. The first estimate of this type of result was in 2008 by Bernik, Götze and Kukso [9]. Their Theorem 1 shows that

$$\#\mathcal{D}_n(Q,\nu_1,0) \gg_n Q^{n+1-2\nu_1}$$

where $\nu_1 \in [0, \frac{1}{2}]$. This was later extended to $\nu_1 \in [0,(n-2)/3]$ in [3] Later then in 2014, Götze, Kaliada and Kusko [31] proved that for $n = 3$

$$\#\mathcal{D}_n(Q,\nu_1,0) \asymp_n Q^{4-\frac{5}{3}\nu_1}$$

where $0 \leq \nu_1 < \frac{3}{5}$. This range was extended to $0 \leq \nu_1 \leq 2$ by Badziahin [1] in 2024.

Then in 2016, Beresnevich, Bernik and Götze [4] extended the known lower bound to obtain

$$\#\mathcal{D}_{n,\gamma_1}(Q,\nu_1,0) \gg_n Q^{n+1-\frac{n+2}{n}\nu_1},$$

where $0 \leq \nu_1 \leq n-1$. This together with Badziahin's [1] result essentially resolves the problem for $n = 3$ in the Archimedean case. In 2019, Koleda [38] proved that for polynomials with no complex roots it we have that

$$\#\mathcal{D}_{n,\gamma_1}(Q, \nu_1, 0) \asymp_n Q^{n+1-\frac{n+2}{n}\nu_1},$$

where $0 \leq \nu_1 \leq \frac{n}{n+2}$.

3.3.1.1 Ordered Roots

Next we will discuss special cases where the roots are ordered in specific ways. In 2015, Bernik, Budarina and O'Donnell [8] considered the case the roots of a polynomial were ordered so that

$$|\alpha_1 - \alpha_2| \leq |\alpha_1 - \alpha_3| \leq \cdots \leq |\alpha_1 - \alpha_n|.$$

They stated that if $|\alpha_1 - \alpha_3| = Q^{-t}$ where $0 \leq t \leq \frac{\nu_1}{3}$ then

$$\#\mathcal{D}_3(Q, \nu_1, 0) \gg_n Q^{4-2\nu_1+t}.$$

In 2017, Bernik, Budarina and Götze [11] looked at the set of polynomials $P \in \mathcal{P}_3(Q)$ such that the roots $\alpha_1, \alpha_2, \alpha_3$ are ordered in the following way

$$\begin{aligned} |\alpha_1 - \alpha_2| &\leq |\alpha_1 - \alpha_3|, \\ |\alpha_1 - \alpha_2| &= Q^{-\rho_2}, \\ |\alpha_1 - \alpha_3| &= Q^{-\rho_3}, \end{aligned}$$

with $0 \leq \rho_3 \leq \rho_2$. By letting $\mathcal{D}_3'(Q, \nu_1, 0)$ denote the set of such polynomials that satisfy

$$\frac{\nu_1}{3} \leq \rho_2 \leq 4 - \frac{5\nu_1}{3},$$

they found that

$$\#\mathcal{D}_3'(Q, \nu_1, 0) \ll_n Q^{4-\frac{5\nu_1}{3}+\varepsilon},$$

for $0 \leq \nu_1 \leq 2$.

In 2020, Bernik, Budarina and O'Donnell [15] considered the polynomials of degree 4. In this case the roots of the polynomial are ordered as

$$\begin{aligned} &|\alpha_1 - \alpha_2| \leq |\alpha_1 - \alpha_3| \leq |\alpha_1 - \alpha_4|, \\ &|\alpha_1 - \alpha_2| \ll |\alpha_3 - \alpha_4| \ll |\alpha_2 - \alpha_3| \ll |\alpha_1 - \alpha_3|, \end{aligned}$$

and they found that

$$\#\mathcal{D}_4'(Q,\nu_1,0) < Q^{5-\frac{3\nu_1}{2}+\varepsilon},$$

for $0 \le \nu_1 \le 1$.

Another special result to consider is that of Budarina in 2019 [14] who considered a subset of polynomials from $\mathcal{D}_n(Q,\nu_1,0)$ such that the roots of these polynomials $\alpha_1,...,\alpha_n \in \mathbb{C}$ are ordered such that for a real number $\rho \ge 0$ they satisfy

$$\begin{gathered}|\alpha_1-\alpha_2| \le |\alpha_1-\alpha_3| \le \cdots \le |\alpha_1-\alpha_n|,\\ |\alpha_1-\alpha_j| \ll 1, \quad \text{for } 3 \le j \le n,\\ |\alpha_1-\alpha_2| = Q^{-\rho}.\end{gathered}$$

This set of polynomials can be described as the set of irreducible polynomials $P \in \mathcal{D}_n(Q,\nu_1,0)$ that have only one root α_2 close to α_1. This set of polynomials will be denoted as $\mathcal{D}_n^*(Q,\nu_1,0)$ and it was found by Budarina that

$$\begin{aligned}&\#\mathcal{D}_n^*(Q,\nu_1,0) \gg_n Q^{n+1-2\nu_1},\\ &\#\mathcal{D}_n^*(Q,\nu_1,0) \ll_n Q^{n+1-2\nu_1} \quad \text{for } \rho \ge \frac{n-1+2\nu_1}{3}+\varepsilon,\end{aligned}$$

if $0 \le \nu_1 \le \frac{n+2}{4} - \varepsilon$.

3.3.1.2 Asymptotic results

Asymptotic estimates for

$$\mathcal{N}_n(Q,X) := \#\{P \in \mathcal{P}_n(Q) : |D(P)| \le X\}$$

have been studied for degrees $n = 2$ and $n = 3$.

In 2013, Götze, Kaliada and Korolev [27] proved that

$$N_2(Q,X) = \kappa_2 QX + O(X^{3/2}\ln Q + (Q\ln Q)^{3/2}),$$

where $\kappa_2 = 4(\ln 2 + 1)$. It is easy to see that for the main term in this estimate to be larger than the error term it is required that $Q^{1/2}(\log Q)^{3/2} \ll X \ll (Q/\log Q)^2$. Then in 2014, Götze, Kaliada and Kusko [31] showed that

$$N_3(Q,X) = \kappa_3 Q^{2/3}X^{5/6} + O(X\ln Q + Q^3)$$

where $\kappa_3 = 26.95\ldots$. It is easy to see that for the main term in this estimate to be larger than the error term it is required that $Q^{14/5} \ll X \ll Q^4/(\log Q)^6$.

3.3.2 p-adic and Combined Cases

In 2008, Bernik, Götze and Kukso [12] additionally published an analogous p-adic version of their result [9]. They showed that

$$\mathcal{D}_{n,\gamma_2}(Q,0,\nu_2) \gg_n Q^{n+1-2\nu_2}$$

for $0 \leq \nu_2 \leq \frac{1}{2}$.

Finally we consider the case where polynomials have a small discriminant in terms of both the Euclidean and p-adic metrics at the same time. In 2012, Budarina, Dickinson and Yuan [48] considered a combined version of the result in which ν_1 and ν_2 were the same so that

$$\mathcal{D}_{n,\gamma_2}(Q,\nu_3,\nu_3) \gg_n Q^{n+1-4\nu_2}$$

for $0 \leq \nu_3 \leq \frac{1}{3}$. Then in 2018 Bernik, Budarina and O'Donnell [7] also studied this combined case and found that

$$\#\mathcal{D}_3(Q,\nu_1,\nu_2) < Q^{4-\frac{5}{3}(\nu_1+\nu_2)+\varepsilon}$$

holds if $\frac{3\varepsilon}{20} \leq \nu_1+\nu_2 \leq \frac{6}{5}$. More recently in 2023, Bernik, Vasilyev, Kalosha and Panteleeva [10] obtained a bound for arbitrary degrees when $0 < \nu_1+\nu_2 < 2$:

$$\mathcal{D}_n(Q,\nu_1,\nu_2) \ll_n Q^{n+1-(\nu_1+\nu_2)+\varepsilon}$$

for arbitrarily small $\varepsilon > 0$.

3.4 NEW RESULTS

As stated above the main results of this thesis are concerned with the problem of obtaining a lower bound for

$$\kappa_{\mathrm{irr}}(n,p) := \kappa(\overline{\mathbb{Q}_p}, \mathcal{P}_{\mathrm{irr}}(n)).$$

More specifically we will prove that

Theorem A. *For any $n \geq 2$ and any prime p, we have that*

$$\kappa_{\mathrm{irr}}(n,p) \geq \frac{n+1}{3}.$$

The new result for the lower bound of the number of polynomials with a small p-adic discriminant is as follows.

Theorem B. *Let $n \geq 2$ be an integer, p be a prime. Then there exist constants $Q_0 = Q_0(n,p) > 1$, $\gamma_2 = \gamma(n,p) > 0$ and $C' = C'(n,p) > 0$ such that for all $Q \geq Q_0$ and any*

$$0 \leq \nu_2 \leq n-1 \tag{3.4}$$

we have that

$$\#\mathcal{D}_{n,\gamma_2}(Q,0,\nu_2) \geq C' Q^{n+1-\frac{n+2}{n}\nu_2}\,. \tag{3.5}$$

— 4 —

Quantitative Non-Divergence

The term 'Quantitative Non-Divergence' is used to describe the process in which by imposing certain quantitative conditions, the likelihood of trajectories diverging into regions where they might otherwise exhibit extreme behaviour are limited. The general idea of this technique is to show that the measure of the set of points where a function takes small values (e.g. covolume or shortest vector length) can be explicitly bounded from above. These small values are the points at which the system is approaching instability, such as a lattice collapsing in certain directions. Quantitative non-divergence results ensure that the set of points where this instability occurs is small and they additionally provide estimates on how large this set can be. This technique was developed by Kleinbock and Margulis in 1998 [36]. These ideas were then built upon by Kleinbock and Tomanov in their paper 'Flows on S-arithmetic homogeneous spaces and applications to metric Diophantine approximation' [35] as they established quantitative non-divergence estimates for continuous transformations on homogeneous spaces. In this Chapter, e will overview a technique as presented by Kleinbock and Tomanov which will be used later in Chapter 5.

Firstly we shall state the notation used within the paper. Let S be a finite set of normalised valuations of $\mathbb{Q}$ that contains the Archimedean one (i.e ∞ which corresponds to $\mathbb{Q}_\infty = \mathbb{R}$), $\mathbb{Z}_S$ is the ring of S-adic integers of $\mathbb{Q}$ as defined by equation 2.1 and $\mathbb{Q}_S = \prod_{v\in S} \mathbb{Q}_v$ where $\mathbb{Q}_v$ is the completion of $\mathbb{Q}$ over a valuation v. From here, the groups within this context can be defined as follows:

$$GL(m, \mathbb{Q}_S) := \prod_{v\in S} GL(m, \mathbb{Q}_v),$$
$$GL^1(m, \mathbb{Q}_S) := \{(g^{(v)})_{v\in S} \in GL(m, \mathbb{Q}_S) : \prod_{v\in S} |\det(g^{(v)})|_v = 1\}.$$

Here, $GL(m, \mathbb{Q}_S)$ is the Cartesian product of the general linear groups $GL(m, \mathbb{Q}_v)$ for each $v \in S$, and the group $GL^1(m, \mathbb{Q}_S)$ is a subset of $GL(m, \mathbb{Q}_S)$ consisting of tuples where the product of the determinants, taken with respect to each $v \in S$, is equal to 1. Similarly, define $GL(m, \mathbb{Z}_S)$ to be the group of $m \times m$ matrices that take entries from $\mathbb{Z}_S$ and are invertible. There is a natural diagonally embedding of $GL(m, \mathbb{Z}_S)$ into $GL(m, \mathbb{Q}_S)$ in which each matrix $g \in GL(m, \mathbb{Z}_S)$ is mapped to the tuple $(g, g, ..., g) \in \prod_{v \in S} GL(m, \mathbb{Q}_v)$. For such a matrix to be invertible in $GL(m, \mathbb{Z}_S)$ it is needed that the determinant is a unit of $\mathbb{Z}_S$ as these are the only invertible elements of the ring. That is under the diagonal embedding each determinant satisfies that $\det(g)$ is a unit of $\mathbb{Z}_v$ for all $v \in S$ and moreover when taking the product of these determinants we get that

$$\prod_{v \in S} |\det(g^{(v)})|_v = 1,$$

and so $GL(m, \mathbb{Z}_S)$ is a subset of $GL^1(m, \mathbb{Q}_S)$. Using these definitions it is possible to define the homogeneous space

$$\begin{aligned} \Omega^1_{S,m} &:= GL^1(m, \mathbb{Q}_S)/GL(m, \mathbb{Z}_S), \\ &= \{g\mathbb{Z}_S^m : g \in GL^1(m, \mathbb{Q}_S)\}. \end{aligned}$$

This can be interpreted as the space of all lattices in $\mathbb{Q}_S^m$ that have covolume 1, where each lattice is a free $\mathbb{Z}_S$-module of rank m.

Now we shall define the content functions

$$c(x) := \prod_{v \in S} |x^{(v)}|_v \quad \text{for } x = (x^{(v)})_{v \in S} \in \mathbb{Q}_S, \tag{4.1}$$

$$c(\mathbf{x}) := \prod_{v \in S} ||\mathbf{x}^{(v)}||_v \quad \text{for } \mathbf{x} = (\mathbf{x}^{(v)})_{v \in S} \in \mathbb{Q}_S^m, \tag{4.2}$$

where $||\mathbf{x}^{(v)}||_v$ is defined by (2.2).

4.1 (C, α)-GOOD FUNCTIONS

Suppose that X is a metric space. Let B be a subset of X and $(F, |\cdot|)$ be a valued field. A function $f : B \to F$ is said to be *good* if the set of points $x \in B$ where f has small values has small measure. More formally, given an $\varepsilon > 0$, points x which take small measure over a function f will be denoted as

$$B^{f,\varepsilon} = \{x \in B : |f(x)| < \varepsilon\}. \tag{4.3}$$

Additionally, define $||f||_B := \sup_{x\in B}|f(x)|$. Further for a locally finite measure μ on X such that $\mu(B) > 0$ define $||f||_{\mu,B} := ||f||_{B\cap \operatorname{supp}\mu}$. In the case that f is continuous and B is open it can be seen that

$$||f||_{\mu,B} = \sup\{c : \mu(\{x \in B : |f(x)| > c\}) > 0\}. \tag{4.4}$$

This norm measures the largest significant size of $|f|$ on B in the sense that it excludes the extreme values that may occur on certain subsets of B which have negligible measure. In this way the norm is not effected by spikes or singular values of f that may occur on sets of measure zero.

Definition 4.1.1. Let X be a metric space with a Borel measure μ and $(F, |\cdot|)$ be a valued field. Suppose $U \subset X$ and $C, \alpha > 0$ are constants, then a Borel measurable function $f : U \to F$ is (C, α)-*good* on U with respect to μ if for any open ball $B \subset U$ centred in the support of μ

$$\mu\left(B^{f,\varepsilon}\right) \leq C\left(\frac{\varepsilon}{||f||_{\mu,B}}\right)^{\alpha}\mu(B) \tag{4.5}$$

for all $\varepsilon > 0$.

From this definition, the following lemma can be seen.

Lemma 4.1.2 (Lemma 3.1 of [35])**.** *For a metric space X, a measure μ on X and a subset U of X let $C, \alpha > 0$ and $f : U \to F$ be a function. Then*

1. *f is (C, α)-good on U with respect to μ iff $|f|$ is (C, α)-good on U with respect to μ;*
2. *If f is (C, α)-good then $c \cdot f$ is (C, α)-good for all $c \in F$;*
3. *If f_i for $i \in I$ are (C, α)-good on U with respect to μ and $f = \sup_{i\in I}|f_i|$ is Borel measurable then f is (C, α)-good on U with respect to μ;*
4. *If f is (C, α)-good on U with respect to μ and $c_1 \leq \frac{|f(x)|}{|h(x)|} \leq c_2$ for all $x \in U$ then h is $(C(\frac{c_2}{c_1})^{\alpha}, \alpha)$-good on U with respect to μ.*

This lemma is given without proof in [35] so one shall be provided here for completeness. Versions of this lemma can also be found in [13], [33] and [34].

Proof. 1. By definition it can be seen that $\left|\left|f\right|\right|_{\mu,B} = \left|\left||f|\right|\right|_{\mu,B}$ and $B^{f,\varepsilon} = B^{|f|,\varepsilon}$. Hence the statement follows.

2. Consider first the trivial case where $c = 0$. In this case $c \cdot f(x) = 0$ for all $x \in B$ which implies that $B^{0 \cdot f, \varepsilon} = B$ and $||0 \cdot f||_{\mu,B} = 0$. Hence the statement holds true trivially. Now consider $c \neq 0$. It can be seen that $||c \cdot f||_{\mu,B} = |c| \cdot ||f||_{\mu,B}$ and similarly

$$\begin{aligned} B^{cf,\varepsilon} &= \{x \in B : |cf(x)| < \varepsilon\}, \\ &= \left\{x \in B : |f(x)| < \frac{\varepsilon}{|c|}\right\}, \\ &= B^{f, \frac{\varepsilon}{|c|}}. \end{aligned}$$

Using the fact that f is (C, α)-good, we observe that

$$\begin{aligned} \mu\left(B^{f, \frac{\varepsilon}{|c|}}\right) &\leq C\left(\frac{\frac{\varepsilon}{|c|}}{||f||_{\mu,B}}\right)^{\alpha} \mu(B), \\ &= C\left(\frac{\varepsilon}{|c| \cdot ||f||_{\mu,B}}\right)^{\alpha} \mu(B), \\ &= C\left(\frac{\varepsilon}{||c \cdot f||_{\mu,B}}\right)^{\alpha} \mu(B). \end{aligned}$$

Then as $B^{cf,\varepsilon} = B^{f, \frac{\varepsilon}{|c|}}$, it must be that $c \cdot f$ is also (C, α)-good for all $c \in F$.

3. By definition $|f_i(x)| \leq |f(x)|$ for all $i \in I$, then as

$$B^{f,\varepsilon} = \{x \in B : |f_i(x)| \leq |f(x)| < \varepsilon\},$$

it can be seen that $B^{f,\varepsilon} \subseteq B^{f_i,\varepsilon}$. Hence $\mu(B^{f,\varepsilon}) \leq \mu(B^{f_i,\varepsilon})$. Similarly it can be seen that $||f||_{\mu,B} = \sup_{i \in I} ||f_i||_{\mu,B}$. Using the definition of each f_i being (C, α)-good it can be then verified that

$$\mu\left(B^{f,\varepsilon}\right) \leq \mu\left(B^{f_i,\varepsilon}\right) \leq C\left(\frac{\varepsilon}{||f_i||_{\mu,B}}\right)^{\alpha} \mu(B) \leq C\left(\frac{\varepsilon}{||f||_{\mu,B}}\right)^{\alpha} \mu(B).$$

4. From the given condition, it must be that $c_1||h||_{\mu,B} \leq ||f||_{\mu,B}$. Similar to above if $|h(x)| < \varepsilon$ then it must be that $|f(x)| < c_2\varepsilon$ and so $B^{h,\varepsilon} \subseteq B^{f,c_2\varepsilon}$ which in turn implies that $\mu(B^{h,\varepsilon}) \leq \mu(B^{f,c_2\varepsilon})$. Putting these together with the fact that f is (C, α)-good;

$$\mu\left(B^{h,\varepsilon}\right) \leq \mu\left(B^{f,c_2\varepsilon}\right) \leq C\left(\frac{c_2\varepsilon}{||f||_{\mu,B}}\right)^{\alpha} \mu(B) \leq C\left(\frac{c_2\varepsilon}{c_1||h||_{\mu,B}}\right)^{\alpha} \mu(B).$$

This then implies that h is $(C(c_2/c_1)^{\alpha}, \alpha)$-good on U with respect to μ.

□

4.1.1 Polynomials are Good Functions

It can be seen that polynomials are in fact good functions. The first result that shall be considered is from [35].

Lemma 4.1.3 (Lemma 3.4 of [35]). *Let F be either $\mathbb{R}$ or a locally compact ultrametric valued field. Then for any $d, k \in \mathbb{N}$, any polynomial $f \in F[x_1, x_2, ..., x_d]$ of degree not greater than k is a $(C, 1/dk)$-good on F^d with respect to Haar measure λ, where C is a constant depending only on d and k.*

This lemma considers the case for more than one variable and while the paper does not provide a proof it does outline how it would be obtained using two other papers. The proof is split into two parts with the first considering a single variable (i.e. $d = 1$) and the second considering multiple variables (i.e. $d > 1$).

The result for when $d = 1$ can be seen by using Lagrange's interpolation formula, a proof of which can be seen in Proposition 3.2 of [33] where it can be seen that $\alpha = \frac{1}{k}$ and $C = \frac{1}{2k}(k+1)^{1/k}$. The proof in the case $d > 1$ can be found in [45] as Lemma 4.1. The case we will consider is that of when $d = 1$.

The following lemma can be used when dealing with functions on products of metric spaces.

Lemma 4.1.4 (Lemma 3.2 of [35]). *Let metric spaces X and Y with measures μ, ν given. Suppose that f is a continuous function on $U \times V$, where $U \subset X$ and $V \subset Y$ are open subsets, and suppose C, D, α, β are positive constants such that*

1. *for all $y \in V \cap \operatorname{supp} \nu$, the function $x \mapsto f(x, y)$ is (C, α)-good on U with respect to μ,*
2. *for all $x \in U \cap \operatorname{supp} \mu$, the function $y \mapsto f(x, y)$ is (D, β)-good on V with respect to ν.*

Then f is (E, γ)-good on $U \times V$ with respect to $\mu \times \nu$, where

$$\gamma = \frac{\alpha\beta}{\alpha + \beta} \quad \text{and} \quad E = (\alpha + \beta)\left(\left(\frac{C}{\beta}\right)^{\beta}\left(\frac{D}{\alpha}\right)^{\alpha}\right)^{\frac{1}{\alpha+\beta}} \tag{4.6}$$

Remark. This result has been stated for completeness. It will not be necessary to use this later in Section 5.3.2 as the function that is considered later only takes one p-adic value x from $\mathbb{Q}_p$. The element that we end up taking from $\mathbb{Q}_\infty$ is not involved in the estimate so as stated above we have that $d = 1$. The more general case though, that perhaps take multiple values from $\mathbb{Q}_S$, would make use of this lemma.

4.2 SUBMODULES

The final ingredient to introduce before the quantitive non-divergence estimates is that of submodules. These will be used in the first specialisation of the quantitative non-divergence Theorem (stated in Section 4.3) as elements of a poset that shall be introduced at the end of this Section. To start, recall these standard definitions from Algebra and Number Theory.

Definition 4.2.1. Let R be a ring with identity 1_R. A *(left) R-module* M is an additive abelian group together with scalar multiplication $R \times M \to M$, such that for $m, m' \in M$ and $r, r' \in R$ the following holds:

1. $r(m + m') = rm + rm'$,
2. $(rr')m = r(r'm)$,
3. $1_R m = m$.

A non-empty subset N of M is a *submodule* if N is closed under addition and scalar multiplication. A R-module is called *simple* if it is non-zero and has no non-zero proper subgroups. A R-module M is *free*, if there exists a R-basis for M, meaning that there is a set of elements $\{m_1, ..., m_k\}$ in M such that every element $m \in M$ can be uniquely expressed as a finite linear combination of the basis elements with coefficients from R. The size of this basis is uniquely determined and referred to as the rank of M and is denoted $\mathrm{rk}(M)$.

An example of this can be seen by taking $R = \mathbb{Z}$ and $M = \mathbb{Z}_p$. This is not a free submodule however as it is not possible to find a basis with finitely many elements. The $\mathbb{Z}$-module $M = \mathbb{Z}^n$ is free however and this can be seen as the elements $e_1, e_2, ..., e_n$ where e_i is the tuple with 1 in the i-th position and 0 elsewhere.

Definition 4.2.2. Suppose that Λ is a R-submodule of M and Δ is a submodule of Λ. Suppose that δ is any submodule of Λ such that $\mathrm{rk}(\delta) = \mathrm{rk}(\Delta)$ and $\Delta \subseteq \delta$, then Δ is said to be *primitive* in Λ if $\delta = \Delta$.

A trivial example of this is the existence of a primitive submodule over the division ring D. For a module M over a division ring D, the division D-submodule is defined as

$$M[D] = \{x \in M : \alpha x = 0, \forall \alpha \in D\}$$

This is primitive as $M[D] = \{0\}$, this clearly has rank 0 so any other submodule contained inside of $M[D]$ of the same rank must in fact be equal to $M[D]$.

For a example where the primitive submodule is not just the element 0, consider the $\mathbb{Z}^2$-submodule $(2,4)\mathbb{Z}$. This is can be seen to be not primitive by considering the submodule $(1,2)\mathbb{Z}$. Both of these have rank one and clearly $(2,4)\mathbb{Z} \subset (1,2)\mathbb{Z}$ but it is not true that $(2,4)\mathbb{Z} = (1,2)\mathbb{Z}$. Indeed $(1,2)\mathbb{Z}$ is primitive in $\mathbb{Z}^2$.

This definition of primitive stated above is the one presented by Kleinbock and Tomanov but it is not the one that can be seen in many introductions to module theory. This more standard definition will be stated now and can be seen to be equivalent. First the following definitions are required.

Definition 4.2.3. Let M be a left R-module. The collection of scalars that act trivially on M is called the *annihilator*:

$$\mathrm{Ann}_R(M) := \{r \in R : r \cdot m = 0 \quad \forall m \in M\}. \tag{4.7}$$

Further, we call M *faithful* if all non-zero elements in R act non-trivially upon M (i.e. $\mathrm{Ann}_R(M) = \{0\}$).

It can be seen that the field of rationals $\mathbb{Q}$ is a faithful $\mathbb{Z}$-module as every element of $\mathbb{Z}$ acts non trivially on $\mathbb{Q}$ and so $\mathrm{Ann}_{\mathbb{Z}}(\mathbb{Q}) = \{0\}$. However, $\mathbb{Z}/n\mathbb{Z}$ is a $\mathbb{Z}$-module that is not faithful as the annihilator of M is the set of multiples of n, i.e

$$\mathrm{Ann}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}) = \{k \cdot n \in R : k \in \mathbb{Z}\}. \tag{4.8}$$

An alternative definition for primitive is that the module is simple and faithful. These two versions will now be shown to be equivalent.

A submodule Δ is simple and faithful iff Δ has no non-zero proper subgroups on which the ring acts non-trivially. That is, any proper submodule of Δ either has strictly smaller rank, or there exists a non-zero element of the ring that annihilates it (i.e. a non-zero ring element that sends all the elements of the submodule to zero). This is true iff when $\mathrm{rk}(\delta) = \mathrm{rk}(\Delta)$ and $\delta \subseteq \Delta$ it must be that $\delta = \Delta$. Otherwise, δ would be a proper submodule of full rank, contradicting simplicity. This is exactly the definition of primitive as presented by Kleinbock and Tomanov.

The following notation will now be introduced:

- $\mathcal{D}$ is an integral domain;

- K is the quotient field of $\mathcal{D}$;
- $\mathcal{R}$ is a commutative ring that contains K as a subring;
- For Δ a $\mathcal{D}$-submodule of $\mathcal{R}^m$, $K\Delta$ is the K-linear span inside $\mathcal{R}^m$;
- For Δ a $\mathcal{D}$-submodule of $\mathcal{R}^m$, $\mathcal{R}\Delta$ is the $\mathcal{R}$-linear span inside $\mathcal{R}^m$.

The rank of a submodule can also be defined as

$$\mathrm{rk}(\Delta) := \dim_K(K\Delta).$$

The following is a classification of primitive submodules.

Lemma 4.2.4 (Lemma 7.2 of [35]). *The following are equivalent for a submodule Δ of $\mathcal{D}^m$:*

(i) *Δ is primitive;*

(ii) *$\Delta = K\Delta \cap \mathcal{D}^m$;*

(iii) *$\Delta = \mathcal{R}\Delta \cap \mathcal{D}^m$ for any commutative ring $\mathcal{R}$ containing K as a subring.*

A partial proof is present in the paper but a full proof will be provided here.

Proof. If $\Delta = \{0\}$, then the result is trivial. It must be primitive as it has rank 1, so any other submodule that contains Δ and has rank 1 must be equal to Δ. The K-linear span of Δ is $\{0\}$, hence by intersecting with $\mathcal{D}^m$ the resulting element must just be $\{0\}$, i.e. Δ. In a similar way it must be that $\Delta = \mathcal{R}\Delta \cap \mathcal{D}^m$. Hence it shall be assumed that $\Delta \neq \{0\}$.

(i $\Rightarrow$ iii) If $x \in \mathcal{R}\Delta \cap \mathcal{D}^m$, then $x \in \mathcal{R}\Delta$ so it can be rewritten as

$$x = \sum_{i=0}^{n} r_i \gamma_i$$

for $r_i \in \mathcal{D}$ and $\gamma_i \in \Delta$. As $x \in \mathcal{D}^m$ and $\mathcal{D}$ is an integral domain, it must be possible to write r_i as an element of K. Therefore $x \in K\Delta \cap \mathcal{D}^m$ and further it can be seen that $K\Delta \cap \mathcal{D}^m$ is a submodule of $\mathcal{D}^m$ that contains Δ. This submodule must also have the same rank as Δ and hence by the primitively of Δ it must be that $\Delta = \mathcal{R}\Delta \cap \mathcal{D}^m$.

(iii $\Rightarrow$ ii) It must be that $\Delta \subseteq K\Delta \cap \mathcal{D}^m$ as $\Delta \subseteq K\Delta$ and $\Delta \subseteq \mathcal{D}^m$ by definition. Therefore the only thing left to show is that $\Delta \supseteq K\Delta \cap \mathcal{D}^m$. If $x \in K\Delta \cap \mathcal{D}^m$, then $x \in K\Delta$ so it can be rewritten as

$$x = \sum_{i=0}^{n} \frac{a_i}{a_j} \gamma_i$$

for $a_i, \in \mathcal{D}$ for all $0 \leq i \leq n$, $\gamma_i \in \Delta$ and $a_i, \in \mathcal{D}$ is a non-zero element chosen so that $\frac{a_i}{a_j}$ lie inside of K. The K-linear span is contained inside the $\mathcal{R}$-linear span so $x \in \mathcal{R}\Delta \cap \mathcal{D}^m$. Hence $\Delta \supseteq K\Delta \cap \mathcal{D}^m$.

(ii $\Rightarrow$ i) By assuming otherwise, it follows that there exists a submodule Δ' with $\Delta \subseteq \Delta'$ and $\text{rk}(\Delta) = \text{rk}(\Delta')$. As they have the same rank, it must then be that Δ and Δ' span the same space over $\mathcal{D}^m$, hence $\Delta K = \Delta' K$ and thereby $\Delta' \subseteq K\Delta$. As $\Delta' \subseteq \mathcal{D}^m$, it must be that $\Delta' \subseteq K\Delta \cap \mathcal{D}^m$. Then as $\Delta = K\Delta \cap \mathcal{D}^m$, it must be that $\Delta' \subseteq \Delta$ and so by the initial assumption of Δ' it must be that $\Delta = \Delta'$ and thereby Δ is primitive. □

The next thing to consider is the group $\text{GL}(m, \mathcal{R})$. Any element $g \in \text{GL}(m, \mathcal{R})$ maps $\mathcal{D}$-submodules of $\mathcal{R}^m$ to $\mathcal{D}$-submodules of $\mathcal{R}^m$ and preserves the rank and inclusion relation. This is because for a $\mathcal{D}$-submodule Δ, an element $g\Delta$ must remain within $\mathcal{R}^m$ as any $\mathcal{D}$-linear combination of elements in Δ is preserved by g. Applying an invertible matrix does not change the number of linearly independent vectors within the submodule Δ and so the rank does not change. Regarding the inclusion relation it can be seen that if we have two submodules Δ_1, Δ_2 such that $\Delta_1 \subseteq \Delta_2$ then for all elements $\delta \in \Delta_1$ it must be that $g\delta \in g\Delta_1$ and $g\delta \in g\Delta_2$, hence $g\Delta_1 \subseteq g\Delta_2$.

It is now possible to define the sets

$$\mathfrak{M}(\mathcal{R}, \mathcal{D}, m) := \{g\Delta : g \in \text{GL}(m, \mathcal{R}), \Delta \text{ is a submodule of } \mathcal{D}^m\}, \tag{4.9}$$

and

$$\mathfrak{B}(\mathcal{D}, m) := \text{ the set of all primitive submodules of } \mathcal{D}^m. \tag{4.10}$$

These sets will be important in the following Section as we look at specific functions whose domain is $\mathfrak{M}(\mathcal{R}, \mathcal{D}, m)$. These functions will be defined in more detail later in subsection 4.3.1 but essentially they map a matrix multiplied by a submodule from $\mathfrak{B}(\mathcal{D}, m)$.

4.3 QUANTITATIVE NON-DIVERGENCE ESTIMATE

Recall that the Kleinbock and Tomanov paper generalises work of Kleinbock and Margulis [33]. More specifically it is defined for functions on arbitrary metric spaces. Here partially ordered sets (here after referred to as posets) $\mathfrak{B}$ are mapped into functions on a metric space X with measure μ.

The notation used is as follows. Let $l(\mathfrak{B})$ denote the length of the poset $\mathfrak{B}$ (that is the number of elements in a maximal linearly ordered subset of $\mathfrak{B}$) and for a subset $\mathfrak{G}$ of $\mathfrak{B}$ denote $\mathfrak{B}(\mathfrak{G})$ to be the poset of elements in $\mathfrak{B}$ but not in $\mathfrak{G}$ such that they are comparable with all elements of $\mathfrak{G}$. Additionally, let $C(B)$ denote the space of continuous functions whose range consists of real numbers on some subset B of X. The maps that are considered are denoted $\psi : \mathfrak{B} \to C(B)$ which takes a value $s \in \mathfrak{B}$ and maps it to what shall be denoted as $\psi_s \in C(B)$.

For such maps and positive numbers $\varepsilon < \rho$, it is said that a point $z \in B$ is (ε, ρ)-marked relative to the poset $\mathfrak{B}$ if there exists a linearly ordered subset $\mathfrak{G}_z \subseteq \mathfrak{B}$ such that

(M1) $\varepsilon \leq |\psi_s(z)| \leq \rho$ for all $s \in \mathfrak{G}_z$;

(M2) $|\psi_s(z)| \geq \rho$ for all $s \in \mathfrak{B}(\mathfrak{G}_z)$.

The set of all such points is denoted by $\Phi(\varepsilon, \rho, \mathfrak{B})$. This translates to the set of points such that there exists a linearly ordered subset $\mathfrak{G}_z$ of $\mathfrak{B}$ such that for all $s \in \mathfrak{G}_z$ the function ψ assigned to that s lies in absolute values between the two constants ε and ρ. Additionally, for any element in $\mathfrak{B} \setminus \mathfrak{G}_z$ that is comparable to an element in $\mathfrak{G}_z$, it must be that $\psi_s(z)$ is greater in absolute value than the original upper bound.

We can now state the quantitative non-divergence result.

Theorem 4.3.1 (Theorem 6.1 of [35])**.** *Let X be a Besicovitch metric space, μ a uniformly Federer measure on X, $m \in \mathbb{Z}_+$ and $C, \alpha, \rho > 0$. Suppose that we are given a poset $\mathfrak{B}$, a ball $B = B(x, r)$ in X, and a mapping $\psi : \mathfrak{B} \to C(\tilde{B})$, where $\tilde{B} := B(x, 3^m r)$, such that the following holds:*

(A0) $l(\mathfrak{B}) \leq m$;

(A1) ψ_s is (C, α)-good on $\tilde{B}$ with respect to μ for all $s \in \mathfrak{B}$;

(A2) $||\psi_s||_{\mu,B} \geq \rho$ for all $s \in \mathfrak{B}$;

(A3) $\#\{s \in \mathfrak{B} : |\psi_s(y)| < \rho\} < \infty$ for all $y \in \tilde{B} \cap \operatorname{supp} \mu$.

Then one has that

$$\mu\left(B \setminus \Phi(\varepsilon, \rho, \mathfrak{B})\right) \leq Cm\left(N_X D_\mu^2\right)^m \left(\frac{\varepsilon}{\rho}\right)^\alpha \mu(B), \tag{4.11}$$

for all $\varepsilon \leq \rho$.

A proof of this theorem is given in [35]. The idea of the proof is to do an induction on m (where the claim is trivial for $m = 0$). That is it will be assumed that for $m \geq 1$ the statement of equation (4.11) is true for some $m-1$. A poset $\mathfrak{B}'$ then of length less than $m-1$ will be introduced that can be shown to satisfy the conditions (A0-3) and will be used to show that the statement is true for the originally defined poset $\mathfrak{B}$.

The theorem is proved for a subset E of the ball B where

$$E := \{y \in B \cap \operatorname{supp} \mu : H(y) \neq \emptyset\},$$

and

$$H(y) := \{s \in \mathfrak{B} : |\psi_s(y)| < \rho\}.$$

This is because if $H(y)$ is empty then y must be (ε, ρ)-marked for any $\varepsilon > 0$ by just taking $\mathfrak{G} = \{\emptyset\}$. Therefore to prove the theorem we instead only need to show that

$$\mu\left(E \setminus \Phi(\varepsilon, \rho, \mathfrak{B})\right) \leq Cm\left(N_X D_\mu^2\right)^m \left(\frac{\varepsilon}{\rho}\right)^\alpha \mu(B).$$

This implies the theorem as the smaller set E is considered rather than the whole ball.

4.3.1 Application to a Specific Poset

The next step to create an auxiliary lemma which will be used in the case studied is to apply theorem 4.3.1 to the poset $\mathfrak{B}(\mathcal{D}, m)$ as defined by (4.10) where the relation is the inclusion relation $\subseteq$. To do this, it is needed to define a function $\nu : \mathfrak{M}(\mathcal{R}, \mathcal{D}, m) \mapsto \mathbb{R}_+$ to be *norm-like* if the following holds:

(N1) for any $\Delta, \Delta' \in \mathfrak{M}(\mathcal{R}, \mathcal{D}, m)$ with $\Delta' \subset \Delta$ and $\operatorname{rk}(\Delta') = \operatorname{rk}(\Delta)$ then

$$\nu(\Delta') \geq \nu(\Delta);$$

(N2) there exists $C_\nu > 0$ such that for any $\Delta \in \mathfrak{M}(\mathcal{R}, \mathcal{D}, m)$ and any $\gamma \notin \mathcal{R}\Delta$,

$$\nu(\Delta + \mathcal{D}\gamma) \leq C_\nu \cdot \nu(\Delta) \cdot \nu(\mathcal{D}\gamma);$$

(N3) for every submodule Δ of $\mathcal{D}^m$, the function $\mathrm{GL}(m, \mathcal{R}) \to \mathbb{R}_+$, $g \mapsto \nu(g\Delta)$, is continuous.

This function will allow the notion of size to be associated to submodules.

Theorem 4.3.2 (theorem 7.3 of [35]). *Let X be a Besicovitch metric space, μ a uniformly Federer measure on X, and let $\mathcal{D} \subset K \subset \mathcal{R}$ be as described on page 45, $\mathcal{R}$ being a topological ring. For $m \in \mathbb{N}$, let a ball $B = B(x_0, r_0) \subset X$ and a continuous map $h : \tilde{B} \to GL(m, \mathcal{R})$ be given, where $\tilde{B}$ stands for $B(x_0, 3^m r_0)$. Also let ν be a norm-like function on $\mathfrak{M}(\mathcal{R}, \mathcal{D}, m)$. For any $\Delta \in \mathfrak{B}(\mathcal{D}, m)$ denote by ψ_Δ the function $x \mapsto \nu(h(x)\Delta)$ on $\tilde{B}$. Now suppose for some $C, \alpha > 0$ and $0 < \rho < 1/C_\nu$ one has*

(i) for every $\Delta \in \mathfrak{B}(\mathcal{D}, m)$, the function ψ_Δ is (C, α)-good on $\tilde{B}$ with respect to μ;

(ii) for every $\Delta \in \mathfrak{B}(\mathcal{D}, m)$, $||\psi_\Delta||_{\mu,B} \geq \rho$;

(iii) $\#\{\Delta \in \mathfrak{B}(\mathcal{D}, m) : \psi_\Delta(x) < \rho\} < \infty$ for all $x \in \mathfrak{B} \cap \operatorname{supp} \mu$.

Then for any positive $\varepsilon \leq \rho$ one has

$$\mu\left(\{x \in B : \nu(h(x)\gamma) < \varepsilon \text{ for some } \gamma \in \mathcal{D}^m \setminus \{0\}\}\right) \leq mC\left(N_X D_\mu^2\right)^m \left(\frac{\varepsilon}{\rho}\right)^\alpha \mu(B).$$

The proof of this is more apparent and can be seen in full in [35] but a brief outline will be given here for completeness. The conditions given in the theorem readily give (A1-3) and (A0) is true as $\mathfrak{B}(\mathcal{D}, m)$ is a poset of length m. Therefore the only thing to prove is that

$$B \setminus \Phi(\varepsilon, \rho, \mathfrak{B}) = \{x \in B : \nu(h(x)\gamma) < \varepsilon \text{ for some } \gamma \in \mathcal{D}^m \setminus \{0\}\}$$

or equivalently

$$\Phi(\varepsilon, \rho, \mathfrak{B}) \subset \{x \in B : \nu(h(x)\gamma) \geq \varepsilon \text{ for some } \gamma \in \mathcal{D}^m \setminus \{0\}\}.$$

This is done by taking a (ε, ρ)-marked point $x \in B$ and letting $\{0\} = \Delta_0 \subsetneq \Delta_1 \subsetneq \cdots \subsetneq \Delta_l = \mathcal{D}^m$ be the elements of $\mathfrak{G}_x \cup \{\{0\}, \mathcal{D}^m\}$. Then take any $\gamma \in \mathcal{D}^m \setminus \{0\}$ so that for some $1 \leq i \leq l$ it is that $\gamma \in \Delta_i \setminus \Delta_{i-1}$. It is then shown that for $\Delta' := \mathcal{D}\Delta_{i-1} + \mathcal{D}\gamma$,

$$\Delta := K\Delta' \cap \mathcal{D}^m = K\Delta \cap \mathcal{D}^m \subset K\Delta_i \cap \mathcal{D}^m = \Delta_i,$$

so that Δ is then comparable to any element of $\mathfrak{G}_x$. Finally the properties (M1-2) can be used with this to conclude that $\nu(h(x)\gamma) \geq \varepsilon$.

4.3.2 Specialising the Theorem Further

Define first the function $\delta : \Omega_{S,m} \to \mathbb{R}_+$ by

$$\delta(\Lambda) := \min\{c(\mathbf{x}) : \mathbf{x} \in \Lambda \setminus \{0\}\}, \tag{4.12}$$

where $c(\mathbf{x})$ is defined by equation (4.1). This defines the smallest value of the product of all the norms $||\cdot||_v$ across all $v \in S$. This therefore is a strictly positive number for any $\mathbf{x} \neq \mathbf{0}$. Now there is enough information to state the final specialisation of Theorem 4.3.1 as presented by Kleinbock and Tomanov.

Theorem 4.3.3 (Theorem 9.3 of [35]). *Let X be a Besicovitch metric space, μ a uniformly Federer measure on X, and let S be as above. For any $m \in \mathbb{N}$, let a ball $B = B(x_0, r_0) \subset X$ and a continuous map $h : \tilde{B} \to GL(m, \mathbb{Q}_S)$ be given, where $\tilde{B}$ stands for $B(x_0, 3^m r_0)$. Now suppose that for some $C, \alpha > 0$ and $0 < \rho < 1$ one has*

1. *for every $\Delta \in \mathfrak{B}(\mathbb{Z}_S, m)$, the function $\operatorname{cov}(h(\cdot)\Delta)$ is (C, α)-good on $\tilde{B}$ with respect to μ;*
2. *for every $\Delta \in \mathfrak{B}(\mathbb{Z}_S, m)$, $||\operatorname{cov}(h(\cdot)\Delta)||_{\mu,B} \geq \rho$.*

Then for any positive $\varepsilon \leq \rho$ one has

$$\mu\left(\{x \in B : \delta(h(x)\mathbb{Z}_S^m) < \varepsilon\}\right) \leq mC\left(N_X D_\mu^2\right)^m \left(\frac{\varepsilon}{\rho}\right)^\alpha \mu(B). \tag{4.13}$$

The remainder of this Chapter will be spent looking at how this specialisation is derived from Theorem 4.3.2 by looking at a specific set $\mathfrak{M}(\mathcal{D}, K, \mathcal{R})$ and the covolume function.

The set $\mathfrak{M}(\mathbb{Q}_S, \mathbb{Z}_S, m)$ is the set of elements $g\Delta$ such that $g \in GL(m, \mathbb{Q}_S)$ and Δ is a submodule of $\mathbb{Z}_S^m$. Consider Δ to be a discrete $\mathbb{Z}_S$-submodule of $\mathbb{Q}_S^m$. This can be then seen to be a free $\mathbb{Z}_S$-submodule as it is possible to find a basis $\{\mathbf{a}_1, \mathbf{a}_2, ..., \mathbf{a}_r\}$ in $\mathbb{Q}_S^m$ for some $r \leq m$ such that

$$\Delta = \mathbb{Z}_S\mathbf{a}_1 \oplus \cdots \oplus \mathbb{Z}_S\mathbf{a}_r.$$

A proof of this statement can be found as Proposition 8.1 in [35]. The consequence of this is that the set of discrete $\mathbb{Z}_S$-submodules of $\mathbb{Q}_S^m$ coincides with $\mathfrak{M}(\mathbb{Q}_S, \mathbb{Z}_S, m)$ and so we can consider the elements to be lattices in the set

$$\Omega_{S,m} = \{g\mathbb{Z}_S^m : g \in \mathrm{GL}(m, \mathbb{Q}_s)\}. \tag{4.14}$$

It can then be seen by Lemma 8.2 of [35], that for such a $\mathbb{Z}_S$-submodule Δ of $\mathbb{Q}_S^m$, its (appropriately normalized) covolume can be computed as the content of the wedge product of its $\mathbb{Z}_S$-basis vectors:

$$\operatorname{cov}(\Lambda) = c(\mathbf{a}_1 \wedge \cdots \wedge \mathbf{a}_k)\,. \tag{4.15}$$

This covolume function can be seen to be norm-like by the checking properties (N1-3). The proof of this can be seen as Lemma 9.1 of [35].

A property of the covolume function is that it is not possible to have an infinite number of sublattices of Λ whose covolume is at most ρ. This statement was proved as Corollary 8.7 of [35]. As a consequence of this property it means that the third condition of Theorem 4.3.2 is true by definition.

The last thing to consider is the condition that $\mathrm{cov}(h(x)\gamma) < \varepsilon$ for some $\gamma \in \mathbb{Z}_S^m \setminus \{0\}$ implies that $\delta(h(x)\mathbb{Z}_S^m) < \varepsilon$. The condition that $\delta(h(x)\mathbb{Z}_S^m) < \varepsilon$ means that there exists a vector $\mathbf{x} \in \delta(h(x)\mathbb{Z}_S^m) \setminus \{0\}$ with $c(\mathbf{x}) < \varepsilon$. By the definition of covolume it must then be that $\mathrm{cov}(\mathbf{x}\mathbb{Z}_S^m) < \varepsilon$ and so it must be possible to find some $\gamma \in \mathbb{Z}_S^m \setminus \{0\}$ such that $\mathrm{cov}(h(x)\gamma) < \varepsilon$.

4.3.3 Specialisation for the Case Considered

We will now specialise Theorem 5.3.1 for our specific case:

Terms in Theorem 5.3.1	Specific definition in the case considered
Besicovitch Metric Space X	$\mathbb{Q}_p$
Federer Measure μ	Haar measure μ on $\mathbb{Q}_p$ with $\mu(\mathbb{Z}_p) = 1$
Set of valuations S	$\{p, \infty\}$
Besicovitch constant N_X	1
Federer constant D_μ	$\leq 3p$

Now we use this information to specialise Theorem 5.3.1 to our case in the following corollary.

Corollary 4.3.4. *Let μ be Haar measure on $\mathbb{Q}_p$ normalized so that $\mu(\mathbb{Z}_p) = 1$, $S = \{p, \infty\}$, and $h : \tilde{B} \to \mathrm{GL}(n+1, \mathbb{Q}_S)$ be a map, where $B := B(x_0, r)$ and $\tilde{B} = B(x_0, 3^{n+1}r)$ are balls in $\mathbb{Q}_p$. Suppose that for some $C, \alpha > 0$ and $0 < \rho < 1$ one has*

(1) *for every $\Delta \in \mathfrak{B}(\mathbb{Z}_S, n+1)$, the function $\mathrm{cov}(h(\cdot)\Delta)$ is (C, α)-good on $\tilde{B}$ with respect to μ;*

(2) *for every $\Delta \in \mathfrak{B}(\mathbb{Z}_S, n+1)$, $\|\mathrm{cov}(h(\cdot)\Delta)\|_B \geq \rho$.*

Then for any positive $\varepsilon \leq \rho$ one has

$$\mu\left(\{x \in B : \delta(h(x)\mathbb{Z}_S^{n+1}) < \varepsilon\}\right) \leq C(n+1)(3p)^{2(n+1)} \left(\frac{\varepsilon}{\rho}\right)^{\alpha} \mu(B). \tag{4.16}$$

— 5 —

Results

The work in this chapter comes from joint work with Victor Beresnevich [6].

5.1 INTRODUCTION

Throughout this Section $p \in \mathbb{Z}$ is as usual a prime number and $n \in \mathbb{Z}$, $n \geq 2$. Given an integer polynomial $P = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, we define the height of P as

$$H(P) := \max_{0 \leq i \leq n} |a_i|. \tag{5.1}$$

In this Section we build on the approach of [5], which also enables quantitative bounds for the number of polynomials with 'close' roots. But first, for convenience, we will restate our main non-quantitative result.

Theorem A. *For any $n \geq 2$ and any prime p, we have that*

$$\kappa_{\text{irr}}(n, p) \geq \frac{n+1}{3}.$$

5.1.1 The quantitative theory of p-adic root separation

Throughout $n \geq 2$ is an integer. Given $Q \geq 1$, let

$$\mathcal{P}_n(Q) := \{P \in \mathbb{Z}[x] : \deg(P) = n \text{ and } H(P) \leq Q\}. \tag{5.2}$$

Let $\theta \geq 0$, $Q \geq 1$ and $C_0, C_1, C_2 > 0$. Define the following set

$$\mathbb{A}_n(Q, \theta, C_0, C_1, C_2) := \left\{ \alpha \in \mathbb{Z}_p : \begin{array}{l} \exists \text{ irreducible } P \in \mathbb{Z}[x] \text{ with } \deg P = n, \\ P(\alpha) = 0 \text{ and } C_1 Q \leq H(P) \leq C_2 Q \\ \text{such that } \exists\ \beta \in \overline{\mathbb{Q}_p} \text{ with } P(\beta) = 0 \\ \text{and } 0 < |\alpha - \beta|_p \leq C_0 Q^{-\theta} \end{array} \right\}.$$

The following is our main result on p-adic algebraic numbers with a conjugate at a specified distance. In what follows μ will denote the Haar measure on $\mathbb{Q}_p$ normalized so that $\mu(\mathbb{Z}_p) = 1$.

Theorem 5.1.1. *Let $n \geq 2$, p be a prime and $0 < \kappa < 1$. Then there are constants $C_0, C_1, C_2 > 0$ depending on n, p and κ only such that the following holds. For any θ satisfying*

$$0 \leq \theta \leq \frac{n+1}{3}, \tag{5.3}$$

and any ball $B := B(x_0, r) = \{x \in \mathbb{Z}_p : |x - x_0|_p \leq r\} \subset \mathbb{Z}_p$

$$\mu\left(\bigcup_{\alpha \in \mathbb{A}_n(Q,\theta,C_0,C_1,C_2)} B(\alpha, C_0 Q^{-n-1+2\theta}) \cap B \right) \geq \kappa \mu(B) \tag{5.4}$$

for all sufficiently large Q.

Corollary 5.1.2. *Let $n \geq 2$, p be a prime and $0 < \kappa < 1$. Then there are constants $C_0, C_1, C_2 > 0$ depending on n, p and κ only such that for any θ satisfying (5.3) and any ball $B \subset \mathbb{Z}_p$*

$$\#(\mathbb{A}_n(Q, \theta, C_0, C_1, C_2) \cap B) \geq \frac{\kappa}{pC_0} \cdot Q^{n+1-2\theta} \mu(B) \tag{5.5}$$

for all sufficiently large Q.

Proof. By the obvious covering argument it follows that

$$\begin{aligned} &\#(\mathbb{A}_n(Q, \theta, C_0, C_1, C_2) \cap B) pC_0 \cdot Q^{-n-1+2\theta} \\ &\geq \mu\left(\bigcup_{\alpha \in \mathbb{A}_n(Q,\theta,C_0,C_1,C_2)} B(\alpha, Q^{-n-1+2\theta}) \cap B \right) \\ &\geq \kappa \mu(B) \end{aligned}$$

where the final line comes from using (5.4). From this equation (5.5) follows by rearranging. □

Corollary 5.1.3. *Let $n \geq 2$. Then for all sufficiently large Q the number of p-adic algebraic numbers $\alpha \in \mathbb{Z}_p$ of degree n with height $H(\alpha) \leq Q$ such that*

$$|\alpha - \beta|_p \ll Q^{-\frac{n+1}{3}} \tag{5.6}$$

for some $\beta \in \overline{\mathbb{Q}_p}$ that is conjugate to α, is $\gg Q^{\frac{n+1}{3}}$. The implied constants depend on n and p only.

Proof. This result follows from Corollary 5.1.2 by taking $\theta = (n+1)/3$, $\kappa = 1/2$ and $B = \mathbb{Z}_p$. □

Proof of Theorem A. This immediately follows on from Corollary 5.1.3. □

5.1.2 New results on Discriminants

For a sufficiently large Q we want to estimate the number of irreducible polynomials P of degree n which have a small discriminant satisfying

$$0 < |D(P)|_p \ll Q^{-2\nu} \tag{5.7}$$

for some fixed $\nu > 0$ where

$$D(P) := a_n^{2n-2} \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2. \tag{5.8}$$

Here a_n is the leading coefficient of P and $\alpha_1, \ldots, \alpha_n$ are the roots of P. Define now the set of polynomials of interest

$$\mathcal{D}_{n,p,\gamma}(Q,\nu) := \left\{ P \in \mathcal{P}_n(Q) : \begin{array}{l} 0 < |D(P)|_p \leq \gamma Q^{-2\nu} \text{and} \\ P \text{ is irreducible over } \mathbb{Q} \end{array} \right\}. \tag{5.9}$$

The notation here is a simplified version of that used above in Section 3.3 as we only use one condition on the discriminant.

Theorem B. *Let $n \geq 2$ be an integer, p be a prime. Then there exist constants $Q_0 = Q_0(n,p) > 1$, $\gamma = \gamma(n,p) > 0$ and $C' = C'(n,p) > 0$ such that for all $Q \geq Q_0$ and any*

$$0 \leq \nu \leq n - 1 \tag{5.10}$$

we have that

$$\#\mathcal{D}_{n,p,\gamma}(Q,\nu) \geq C' Q^{n+1-\frac{n+2}{n}\nu}. \tag{5.11}$$

5.2 AUXILIARY RESULTS FOR POLYNOMIALS

In this Section we state and discuss the following statement, which is instrumental in establishing all the new results obtained in this work. In short, it allows us to find many irreducible polynomials with fixed sizes of height and derivatives.

Lemma 5.2.1. *Let $n \geq 2$ be an integer, p be a prime, $v > 0$ and $0 < \kappa < 1$. Then there exists positive constants δ_0, C_1 and C_2 depending only on n, p and κ only such that for any ball*

$$B := B(x_0, r) = \{x \in \mathbb{Z}_p : |x - x_0|_p \leq r\}, \tag{5.12}$$

where $x_0 \in \mathbb{Z}_p$ and $0 \leq r \leq 1$, there exists $Q_0 = Q_0(B, n, p, v, \kappa)$ such that for any $Q \geq Q_0$ and any parameters

$$0 < \xi_0 \leq \cdots \leq \xi_{n-1} \leq \xi_n = 1 \tag{5.13}$$

satisfying

$$\prod_{i=0}^{n} \xi_i = Q^{-(n+1)} \qquad \text{and} \qquad \xi_0 \leq Q^{-1-v}, \tag{5.14}$$

there exists a measurable set $G_B \subset B$, depending on n, p, B, κ, Q and ξ_i's, such that

$$\mu(G_B) \geq \kappa\mu(B), \tag{5.15}$$

and for every $x \in G_B$ there are $n+1$ linearly independent primitive irreducible polynomials $P \in \mathbb{Z}[x]$ of degree n and height $C_1 Q \leq H(P) \leq C_2 Q$ satisfying

$$\delta_0 \xi_i \leq \left|\frac{1}{i!} P^{(i)}(x)\right|_p \leq \xi_i \tag{5.16}$$

for all $0 \leq i \leq n$, where $P^{(i)}(x)$ denotes the i-th derivative of the polynomial P at x.

The proof of this result will be given in Section 5.4, and it relies on the quantitative non-divergence estimate of Kleinbock and Tomanov as seen in Chapter 4. In this Section we provide a reformulation of the r.h.s. inequality of (5.16) in a matrix form necessary for the use of the quantitative non-divergence estimate.

5.2.1 OUTLINING THE APPROACH

Our first observation is that in the proof of Lemma 5.2.1 it suffices to assume that the parameters ξ_i and Q are integer powers of p. Indeed, suppose that we are given

parameters $0 < \xi_i \leq 1$ for $0 \leq i \leq n$ and $Q > 1$. Then we can find integers $b_i \in \mathbb{Z}_{\geq 0}$ such that

$$p^{-b_i} \leq \xi_i \leq p^{-b_i+n} \tag{5.17}$$

and

$$\sum_{i=0}^{n} b_i = t(n+1), \tag{5.18}$$

for some $t \in \mathbb{N}$. Then, clearly $\tilde{Q}/Q$, where $\tilde{Q} = p^t$, is bounded below and above by constants depending on n and p only and $p^{-n}\xi_i \leq \tilde{\xi}_i \leq \xi_i$. It is then readily seen that it suffices to consider $\tilde{\xi}_i = p^{-b_i}$ and $\tilde{Q} = p^t$ instead of the initial parameters ξ_i and Q. Thus for the rest of the proofs we will assume that

$$\xi_i = p^{-b_i} \qquad \text{and} \qquad Q = p^t \tag{5.19}$$

for some integers $b_i \in \mathbb{Z}_{\geq 0}$ and $t \in \mathbb{N}$ satisfying (5.18). In particular, we have that

$$0 < \xi_i \leq 1 \quad \text{and} \quad \prod_{i=0}^{n} \xi_i = Q^{-(n+1)}. \tag{5.20}$$

In what follows we will assume that

$$C_2 = p^{2u} \qquad \text{for some } u \in \mathbb{Z}_{\geq 0}. \tag{5.21}$$

Let $x \in \mathbb{Z}_p$, and let P denote a polynomial in $\mathcal{P}_{\leq n}(Q)$ with coefficients $(a_0, \ldots, a_n)$. Consider the system of inequalities

$$\left|\frac{1}{i!}P^{(i)}(x)\right|_p \leq \xi_i \qquad (0 \leq i \leq n)\,. \tag{5.22}$$

This can be rewritten in the following matrix form:

$$\begin{pmatrix} 1 & x & x^2 & \cdots & x^n \\ 0 & 1 & 2x & \cdots & nx^{n-1} \\ 0 & 0 & 1 & \cdots & \frac{1}{2}n(n-1)x^{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \overset{p}{\leq} \begin{pmatrix} \xi_0 \\ \xi_1 \\ \xi_2 \\ \vdots \\ \xi_n \end{pmatrix}, \tag{5.23}$$

where $\overset{p}{\leq}$ is the component-wise inequality obtained by taking the p-adic norm of the left hand side. Additionally, rewrite the bound $H(P) \leq C_2 Q$ on the height of P in

the matrix form as follows:

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_n \end{pmatrix} \overset{\infty}{\leq} \begin{pmatrix} C_2 Q \\ C_2 Q \\ \vdots \\ C_2 Q \end{pmatrix}, \tag{5.24}$$

where $\overset{\infty}{\leq}$ is the component-wise inequality obtained by taking the usual absolute value on the left.

The following statement will be required to use Minkowski's Theorem for convex bodies in order to find solutions to the combination of (5.23) and (5.24):

Proposition 5.2.2. *Let $x \in \mathbb{Z}_p$ and ξ_i be given by (5.19) for some integers $b_i \in \mathbb{Z}_{\geq 0}$. Let Γ be the collection of integer points $(a_0, \ldots, a_n)$ satisfying (5.22). Then Γ is a sublattice of $\mathbb{Z}^{n+1}$ such that*

$$\operatorname{cov}(\Gamma) = \prod_{i=0}^{n} \xi_i^{-1}. \tag{5.25}$$

Proof. To show Γ is a sublattice of $\mathbb{Z}^{n+1}$ it is enough to show for all $\mathbf{a}, \mathbf{a}' \in \Gamma$ we have $\mathbf{a} - \mathbf{a}' \in \Gamma$. Let $P_1(x)$ and $P_2(x)$ be polynomials with coefficients $\mathbf{a} = (a_0, \ldots, a_n)$ and $\mathbf{a}' = (a_0', \ldots, a_n')$ respectively that satisfy equation (5.22). Then by the ultrametic property we have that

$$|P(x)|_p = |(i!)^{-1} P_1^{(i)}(x) - (i!)^{-1} P_2^{(i)}(x)|_p \leq \xi_i,$$

where $P = P_1 - P_2 \in \mathbb{Z}[x]$, $\deg P \leq n$ has coefficients $\mathbf{a} - \mathbf{a}'$. Hence $\mathbf{a} - \mathbf{a}' \in \Gamma$. The covolume (the volume of the fundamental domain) of the lattice Γ can be found by reinterpreting (5.22) in the following way. Since the integers are dense in $\mathbb{Z}_p$, we can find $\tilde{x} \in \mathbb{Z}$ such that $|x - \tilde{x}| < \xi_i$. Then by the ultrametric property we have that $|i!^{-1} P^{(i)}(x)|_p = |i!^{-1} P^{(i)}(\tilde{x})|_p$. Thus within (5.22) we can assume without loss of generality that $x \in \mathbb{Z}$. Then, the quantity $(i!)^{-1} P^{(i)}(x)$ is in $\mathbb{Z}$ and, by using (5.19), we have that

$$\left| \frac{1}{i!} P^{(i)}(x) \right|_p \leq p^{-b_i} \quad \Longleftrightarrow \quad \frac{1}{i!} P^{(i)}(x) \equiv 0 \mod p^{b_i}. \tag{5.26}$$

From the congruence condition, we see that each element of Γ satisfies

$$\frac{1}{i!} P^{(i)}(x) \equiv 0 \mod p^{b_i},$$

which implies that the i-th coordinate lies in $p^{b_i}\mathbb{Z}$. Therefore, Γ contains the lattice generated by $p^{b_0}e_0, \ldots, p^{b_n}e_n$ hence it follows then that Γ has covolume

$$\mathrm{cov}(\Gamma) = \mathrm{vol}(\mathbb{R}^{n+1}/\Gamma) = \prod_{i=0}^{n} p^{b_i} = \prod_{i=0}^{n} \xi_i^{-1}\,,$$

which verifies (5.25). □

Using this proposition and Minkowski's first Theorem it can be easily shown for all $x \in \mathbb{Z}_p$ that we can find a solution to (5.22). Indeed, in Section 5.4 we will demonstrate, by using the second theorem of Minkowski, that under a 'mild' restriction on x and a suitable choice of C_2 we can find $n+1$ primitive linearly independent points of Γ in B_{Q,C_2} which will define irreducible polynomials $P_1, \ldots, P_{n+1}$. Here we outline the approach for obtaining lower bounds in (5.16) as well as lower bound on the heights of P_i.

If we strengthen one of the inequalities in equation (5.22), say with the index i' between 0 and n, by multiplying the right hand side by some small constant $\delta^{2(n+1)} > 0$, where δ is a negative integer power of p, we obtain the inequalities

$$\left|\frac{1}{i!}P^{(i)}(x)\right|_p \leq \delta_i \xi_i \qquad (0 \leq i \leq n), \tag{5.27}$$

where

$$\delta_i = \begin{cases} \delta^{2(n+1)} C_2^{-n-1} & \text{if } i = i', \\ 1 & \text{otherwise}\,. \end{cases} \tag{5.28}$$

Doing this, we can then show using the quantitative non-divergence estimate, as stated above in Section 4.3.2, that this forces x to lie in a very small set. Hence by then taking x to lie outside of the union of these sets, taken over all $i' \in \{0, \ldots, n\}$, we can find a lower bound required (5.16).

To use the quantitative non-divergence estimate we need to re-normalize both systems of matrix inequalities (5.23) and (5.24) so as to get the same values, to be denoted R, on the right hand side of the inequalities. This is achieved by multiplying each matrix on the left hand sides of (5.23) and (5.24) by diagonal matrices filled with g_i's and d_i's respectively, where $g_i = |g_i|_p^{-1}$ is a power of p and $d_i \in \mathbb{Q}_{>0}$ for $0 \leq i \leq n$. The precise choice of these scaling factors will depend on the inequalities (5.23) and (5.24). Additionally we will require the normalisation condition

$$\prod_{i=0}^{n} |g_i|_p |d_i| = 1\,. \tag{5.29}$$

Obviously, we then get that for all $0 \leq i \leq n$

$$|g_i|_p \delta_i \xi_i = R, \tag{5.30}$$

$$d_i C_2 Q = R. \tag{5.31}$$

Multiplying these equations together we get that

$$C_2^{n+1} Q^{n+1} \prod_{i=0}^{n} |g_i|_p d_i \delta_i \xi_i = R^{2(n+1)} \tag{5.32}$$

and by the conditions placed on ξ_i, Q, g_i and d by equations (5.20), (5.28) and (5.29) this becomes

$$\delta = R. \tag{5.33}$$

Therefore we have that

$$|g_i|_p = \frac{R}{\delta_i \xi_i} = \frac{\delta}{\delta_i \xi_i} = \begin{cases} \dfrac{\delta^{1-2(n+1)} C_2^{n+1}}{\xi_i} & \text{if } i = i', \\ \dfrac{\delta}{\xi_i} & \text{otherwise}, \end{cases} \tag{5.34}$$

$$d_i = \frac{R}{Q} = \frac{\delta}{Q}. \tag{5.35}$$

It should be noted that each d_i does not depend on i hence we must have $d = d_0 = \cdots = d_n$. From here the following matrices are defined:

$$h_1(x) = \begin{pmatrix} g_0 & 0 & \cdots & 0 \\ 0 & g_1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & g_n \end{pmatrix} \begin{pmatrix} 1 & x & \cdots & x^n \\ 0 & 1 & \cdots & n x^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}, \tag{5.36}$$

$$h_2(x) = d \cdot I_{n+1}. \tag{5.37}$$

This now gives us the map

$$h := (h_1, h_2) : \mathbb{Q}_p \to \mathrm{GL}(n+1, \mathbb{Q}_S), \tag{5.38}$$

where $S = \{p, \infty\}$ and $\mathrm{GL}(n+1, \mathbb{Q}_S) = \mathrm{GL}(n+1, \mathbb{Q}_p) \times \mathrm{GL}(n+1, \mathbb{R})$, so that h_1 defines a linear transformation in $\mathrm{GL}(n+1, \mathbb{Q}_p)$ and h_2 defines a linear transformation in $\mathrm{GL}(n+1, \mathbb{R})$.

Using equations (5.36) and (5.37) with g_i and d defined by equations (5.34) and (5.35), we get that

$$\|h_1(x)\mathbf{a}\|_p \leq \delta, \tag{5.39}$$

$$\|h_2(x)\mathbf{a}\|_\infty \leq \delta. \tag{5.40}$$

We now summarise the above discussion as the following statement.

Proposition 5.2.3. *Let $\xi_0, \cdots, \xi_n, Q$ be as in (5.19) and (5.20) for some integers $b_i \in \mathbb{Z}_{\geq 0}$ and $t \in \mathbb{N}$. Let $\delta > 0$ be a negative integer power of p. Let C_2 be defined by (5.21). Fix any $i' \in \{0, \ldots, n\}$ and define δ_i $(0 \leq i \leq n)$ as in equation (5.28). Let $x \in \mathbb{Z}_p$. Suppose that (5.27) holds for some non-zero polynomial $P \in \mathbb{Z}[x]$ of degree $\leq n$ and height $\leq C_2 Q$. Then (5.39) and (5.40) hold, where $\mathbf{a} \in \mathbb{Z}^{n+1} \setminus \{\mathbf{0}\}$ is the vector of coefficients of P, h_1 and h_2 are given by (5.36) and (5.37) with $g_i = |g_i|_p^{-1}$ and d_i defined by (5.34) and (5.35).*

In a similar way we can ensure a lower bound on the height of the polynomial by considering the system (5.22) together with

$$\max_{0 \leq i \leq n} |a_i| \leq \delta^2 Q\,. \tag{5.41}$$

By using the quantitative non-divergence estimate we will demonstrate that the measure of x satisfying the above inequalities is small provided that δ is small enough. Then on taking x outside the set defined by (5.22) and (5.41) we will ensure a lower bound of $H(P)$.

We re-normalize (5.22) and (5.41) in the same way as before where $g_i = |g_i|_p^{-1}$ is a power of p and $d_i \in \mathbb{Q}_{>0}$ for $0 \leq i \leq n$ such that equation (5.29) holds to get

$$|g_i|_p \xi_i = R, \tag{5.42}$$

$$|d_i| \delta^2 Q = R. \tag{5.43}$$

By multiplying these $2(n+1)$ equations together and simplifying we obtain that $R = \delta$ and the constants are now defined as

$$|g_i|_p = \frac{R}{\xi_i} = \frac{\delta}{\xi_i}, \tag{5.44}$$

$$d_i = \frac{R}{\delta^2 Q} = \frac{1}{\delta Q}. \tag{5.45}$$

In a similar way we can then define the matrices $h_1(x)$ and $h_2(x)$ as in equation (5.36) and (5.37) with the g_i's as defined in equation (5.44) and $d = d_i$ for all i as defined in equation (5.45). Once again we arrive at (5.39) and (5.40). We now summaries the above discussion as the following statement.

Proposition 5.2.4. *Let $\xi_0, \cdots, \xi_n, Q$ be as in (5.19) and (5.20) for some integers $b_i \in \mathbb{Z}_{\geq 0}$ and $t \in \mathbb{N}$. Let $\delta > 0$ be an integer power of p. Let $x \in \mathbb{Z}_p$. Suppose that (5.22) and (5.41) hold for some non-zero polynomial $P \in \mathbb{Z}[x]$ of degree $\leq n$. Then (5.39) and (5.40) hold, where $\mathbf{a} \in \mathbb{Z}^{n+1} \setminus \{\mathbf{0}\}$ is the vector of coefficients of P, h_1 and h_2 are given by (5.36) and (5.37) with $g_i = |g_i|_p^{-1}$ and d_i defined by (5.44) and (5.45).*

5.3 A QUANTITATIVE NON-DIVERGENCE ESTIMATE

5.3.1 A result of Kleinbock and Tomanov

In this subsection we shall recall appropriate material already discussed in Chapter 4. In this work we will be working with $X = \mathbb{Q}_p$ and Haar measure μ and as seen above it is that $D_\mu \leq 3p$.

Given a function $f : X \to F$ with values in a valued field F, recall from equation (4.4) the following norm:

$$\|f\|_{\mu,B} = \sup\{c : \mu(\{x \in B : |f(x)| > c\}) > 0\}\,, \tag{5.46}$$

where B is a ball in X with $\mu(B) > 0$.

Let S be a finite set of normalised valuations of $\mathbb{Q}$ including the Archimedean one. Let $\mathbb{Q}_S$ be the direct product of completions $\mathbb{Q}_v$ of $\mathbb{Q}$ over $v \in S$ and $\mathrm{GL}(n+1, \mathbb{Q}_S) := \prod_{v\in S} \mathrm{GL}(n+1, \mathbb{Q}_v)$. Given $\mathbf{x} = (\mathbf{x}^{(v)})_{v\in S} \in \mathbb{Q}_S^{n+1}$, recall from equation (4.2) the content of $\mathbf{x}$ is defined as

$$c(\mathbf{x}) := \prod_{v\in S} \|\mathbf{x}^{(v)}\|_v\,, \tag{5.47}$$

where the v-norm of $\mathbf{x}^{(v)} = (x_0^{(v)}, \ldots, x_n^{(v)})$ is given by

$$\|\mathbf{x}^{(v)}\|_v = \max\{|x_0^{(v)}|_v, \ldots, |x_n^{(v)}|_v\}\,.$$

Also recall from equation (4.12) for a given subset $\Lambda \subset \mathbb{Q}_S^{n+1}$, the function

$$\delta(\Lambda) := \min\{c(\mathbf{x}) : \mathbf{x} \in \Lambda \setminus \{\mathbf{0}\}\}\,.$$

In the case that $S = \{\infty\}$, $\mathbb{Q}_S^{n+1} = \mathbb{R}^{n+1}$. Then for a lattice, or a discrete subgroup, Λ of $\mathbb{R}^{n+1}$, $\delta(\Lambda)$ is simply the length of its shortest vector with respect to the supremum norm. We note that Λ can be obtained by a applying a linear transformation

$g \in \mathrm{GL}(n+1,\mathbb{R})$ to a discrete subgroup Δ of $\mathbb{Z}^{n+1}$, thus $\Lambda = g\Delta$. In this work we will be interested in the case $S = \{p, \infty\}$ for a prime p. In this case, Λ will be a discrete $\mathbb{Z}_S$-submodule of $\mathbb{Q}_S^{n+1}$, where $\mathbb{Z}_S = \mathbb{Z}[\frac{1}{p}]$. Respectively, Λ will be of the form $g\Delta$ for some $g \in \mathrm{GL}(n+1,\mathbb{Q}_S)$ and a discrete submodule Δ of $\mathbb{Z}_S$. Following [35] let $\mathfrak{B}(\mathbb{Z}_S, n+1)$ be the set of all non-zero primitive submodules of $\mathbb{Z}_S^{n+1}$.

Recall also the calculation of covolume from equation (4.15), namely that for given a $\mathbb{Z}_S$-submodule

$$\Lambda = \mathbb{Z}_S\mathbf{a}_1 \oplus \cdots \oplus \mathbb{Z}_S\mathbf{a}_k$$

of $\mathbb{Q}_S^{n+1}$, can be computed as the content of the wedge product of its $\mathbb{Z}_S$-basis vectors:

$$\mathrm{cov}(\Lambda) = c(\mathbf{a}_1 \wedge \cdots \wedge \mathbf{a}_k)\,. \tag{5.48}$$

Additionally recall Theorem 4.3.3, as

Theorem 5.3.1 (Theorem 9.3 of [35]). *Let X be a Besicovitch metric space, μ a uniformly Federer measure on X, and let S be a finite collection of valuations of $\mathbb{Q}$ including the Archimedean one. Let $m \in \mathbb{N}$, and let a ball $B = B(x_0, r_0) \subset X$ and a continuous map $h : \tilde{B} \to \mathrm{GL}(m, \mathbb{Q}_S)$ be given, where $\tilde{B}$ stands for $B(x_0, 3^m r_0)$. Now suppose that for some $C, \alpha > 0$ and $0 < \rho < 1$ one has*

(1) *for every $\Delta \in \mathfrak{B}(\mathbb{Z}_S, m)$, the function $\mathrm{cov}(h(\cdot)\Delta)$ is (C,α)-good on $\tilde{B}$ with respect to μ;*

(2) *for every $\Delta \in \mathfrak{B}(\mathbb{Z}_S, m)$, $\|\mathrm{cov}(h(\cdot)\Delta)\|_{\mu,B} \geq \rho$.*

Then for any positive $\varepsilon \leq \rho$ one has

$$\mu\left(\{x \in B : \delta(h(x)\mathbb{Z}_S^m) < \varepsilon\}\right) \leq mC\left(N_X D_\mu^2\right)^m \left(\frac{\varepsilon}{\rho}\right)^\alpha \mu(B). \tag{5.49}$$

In the application of Theorem 5.3.1 considered in this chapter the corresponding function will always be polynomials. Hence finally we recall Lemma 4.1.3 as

Lemma 5.3.2 (Lemma 3.4 of [35]). *Let F be either $\mathbb{R}$ or a locally compact ultrametric valued field. Then for any $d, k \in \mathbb{N}$, any polynomial $f \in F[x_1, x_2, \ldots, x_d]$ of degree not greater than k is $(C, 1/dk)$-good on F^d with respect to Haar measure λ, where C is a constant depending only on d and k.*

Recall now the specialisation of Theorem 5.3.1 for our specific case from section 4.3.3

Corollary 5.3.3. *Let μ be Haar measure on $\mathbb{Q}_p$ normalized so that $\mu(\mathbb{Z}_p) = 1$, $S = \{p, \infty\}$, and $h : \tilde{B} \to \mathrm{GL}(n+1, \mathbb{Q}_S)$ be a map, where $B := B(x_0, r)$ and $\tilde{B} = B(x_0, 3^{n+1}r)$ are balls in $\mathbb{Q}_p$. Suppose that for some $C, \alpha > 0$ and $0 < \rho < 1$ one has*

(1) *for every $\Delta \in \mathfrak{B}(\mathbb{Z}_S, n+1)$, the function $\mathrm{cov}(h(\cdot)\Delta)$ is (C, α)-good on $\tilde{B}$ with respect to μ;*

(2) *for every $\Delta \in \mathfrak{B}(\mathbb{Z}_S, n+1)$, $\|\mathrm{cov}(h(\cdot)\Delta)\|_B \geq \rho$.*

Then for any positive $\varepsilon \leq \rho$ one has

$$\mu\left(\{x \in B : \delta(h(x)\mathbb{Z}_S^{n+1}) < \varepsilon\}\right) \leq C(n+1)(3p)^{2(n+1)} \left(\frac{\varepsilon}{\rho}\right)^{\alpha} \mu(B). \tag{5.50}$$

The aim is now to show that the map h as defined in equations (5.36)–(5.38) satisfies the properties required in Corollary 5.3.3.

5.3.2 Verifying conditions (1) and (2) in Corollary 5.3.3

It should be noted that Condition (1) has been mostly verified above by Lemma 5.3.2 but it must also be checked that the coordinates of the corresponding multivector are in fact polynomials in order to use the lemma. This will be done later in this Section. The main content here will concentrate on establishing Condition (2). We begin with auxiliary statements regarding the parameters g_i and d defined in Section 5.2.

Proposition 5.3.4. *For $0 \leq i \leq n$, let g_i and d be integer powers of p such that $\prod_{i=0}^{n}(|g_i|_p d) = 1$. Further suppose that for some parameters $s_1, \ldots, s_n \geq s_0 := 1$, we have that*

$$s_i g_i \leq s_{i+1} g_{i+1} \qquad \text{for } 0 \leq i \leq n-1. \tag{5.51}$$

Then for all $1 \leq k \leq n$

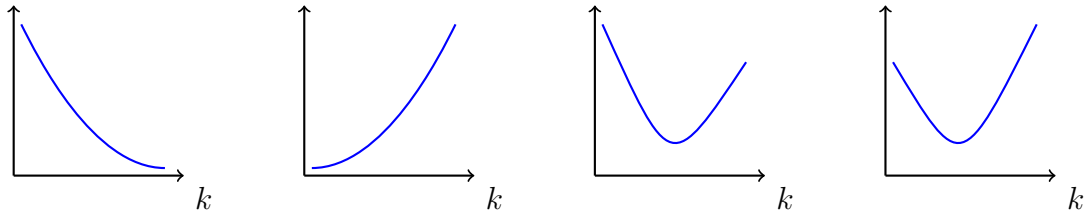
$$\left(\prod_{i=0}^{k-1} d|g_i|_p\right)^{-1} \leq \max\left\{\frac{1}{d|g_0|_p}, |g_n|_p d \prod_{i=1}^{n-1} s_i\right\}. \tag{5.52}$$

Proof. First note that $(\prod_{i=0}^{k-1} d|g_i|_p)^{-1} = \prod_{i=0}^{k-1} d^{-1} g_i$ since each g_i is a power of p. Using the inequalities $s_i g_i \leq s_{i+1} g_{i+1}$ we get that

$$\frac{g_0}{d} \leq \frac{s_1 g_1}{d} \leq \cdots \leq \frac{s_n g_n}{d}. \tag{5.53}$$

Define j_0 (if it exists) to be the minimum of all possible j such that $s_j g_j d^{-1} \geq 1$, then it is readily seen that there are 4 different types of behaviour of the product

$\Pi_k := \prod_{i=0}^{k} s_i g_i d^{-1}$ as function of k, summarized in Figure 5.1, and in each case the maximal value of the product is achieved at either $k = 0$ or $k = n - 1$.



(a) (b) (c) (d)

Figure 5.1: (a) j_0 does not exist, (b) $j_0 = 0$, (c) $j_0 > 0$, $\Pi_0 \geq \Pi_{n-1}$, (d) $j_0 > 0$, $\Pi_0 \leq \Pi_{n-1}$

Indeed, we must have that

$$\frac{g_0}{d} \geq \frac{g_0}{d} \cdot \frac{s_1 g_1}{d} \geq \cdots \geq \prod_{i=0}^{j_0-1} \frac{s_i g_i}{d} \leq \prod_{i=0}^{j_0} \frac{s_i g_i}{d} \leq \cdots \leq \prod_{i=0}^{n-1} \frac{s_i g_i}{d}. \tag{5.54}$$

It is then clear that the largest of all possible values of $\prod_{i=0}^{k} s_i g_i d^{-1}$ must be $\max\{g_0 d^{-1}, \prod_{i=0}^{n-1} \frac{s_i g_i}{d}\}$. Since $\prod_{i=0}^{n} g_i d^{-1} = 1$ and $g_i = |g_i|_p^{-1}$ we obtain (5.52).

If j_0 does not exist, then we just have the left part of (5.54) so that the maximal value is $g_0 d^{-1}$ and we again obtain (5.52). □

We now specialise Proposition 5.3.4 further by using specific values of $|g_i|_p$ and d given by (5.34) and (5.35).

Corollary 5.3.5. *Let $n \geq 2$, $0 < \delta < 1$ be an integer power of p, $Q \geq 1$,*

$$\xi_0 \leq \cdots \leq \xi_n \tag{5.55}$$

and (5.19) and (5.20) hold. Fix any $0 \leq i' \leq n$ and define d and g_i for $0 \leq i \leq n$ by equations (5.34) and (5.35) respectively. Assume that $\xi_n = 1$ and $\xi_0 \leq Q^{-1-v}$ for some $0 < v \leq 1$. Then for every $1 \leq k \leq n$

$$\prod_{i=0}^{k-1} d|g_i|_p \geq Q^v \delta^{4n+2} C_2^{-2n-2}. \tag{5.56}$$

Proof. From the definition of d and g_i it can be seen that

$$\prod_{i=0}^{n} d|g_i|_p = 1. \tag{5.57}$$

Using equations (5.34) and (5.35) with δ_i defined by equation (5.28) it can be easily seen that

$$\frac{1}{d|g_0|_p} = \begin{cases} \frac{Q\xi_0}{\delta\delta^{1-2(n+1)}C_2^{n+1}} & \text{if } i'=0, \\ \frac{Q\xi_0}{\delta^2} & \text{otherwise.} \end{cases} \le \begin{cases} \frac{\delta^{2n}}{Q^v C_2^{n+1}} & \text{if } i'=0, \\ \frac{1}{Q^v\delta^2} & \text{otherwise.} \end{cases} \tag{5.58}$$

$$d|g_n|_p = \begin{cases} \frac{\delta\delta^{1-2(n+1)}C_2^{n+1}}{Q\xi_n} & \text{if } i'=n, \\ \frac{\delta^2}{Q\xi_n} & \text{otherwise.} \end{cases} = \begin{cases} \frac{C_2^{n+1}}{Q\delta^{2n}} & \text{if } i'=n, \\ \frac{\delta^2}{Q} & \text{otherwise.} \end{cases} \tag{5.59}$$

Recall, by (5.34), that

$$g_i = \begin{cases} \frac{\xi_i}{\delta^{1-2(n+1)}C_2^{n+1}} & \text{if } i=i', \\ \frac{\xi_i}{\delta} & \text{otherwise}\,. \end{cases}$$

Then, by (5.55), inequalities (5.51) are fulfilled with $(s_1,\dots,s_n)=(1,\dots,1)$ if $i'=0$ and with

$$(s_1,\dots,s_n) = (\underbrace{1,\dots,1}_{i'-1}, \delta^{-2(n+1)}C_2^{n+1}, \underbrace{1,\dots,1}_{n-i'}) \quad \text{if } i'>0\,.$$

Combining (5.58) and (5.59) with Proposition 5.3.4 and using the fact that $0<\delta<1$ we obtain that

$$\left(\prod_{i=0}^{k-1} d|g_i|_p\right)^{-1} \le \max\left\{\frac{1}{Q^v\delta^2}, \frac{C_2^{n+1}}{Q^v\delta^{2n}}\prod_{i=0}^{n-1}s_i\right\} \le \frac{C_2^{2n+2}}{Q^v\delta^{4n+2}}\,,$$

implying (5.56), as required. □

The following statement is an analogue of Corollary 5.3.5 for the case (5.44) and (5.45) instead of (5.34) and (5.35).

Corollary 5.3.6. *Let $n\ge 2$, $0<\delta<1$ be an integer power of p, $Q\ge 1$,*

$$\xi_0 \le \dots \le \xi_n \tag{5.60}$$

and (5.19) and (5.20) hold. Define d and g_i for $0\le i\le n$ by equations (5.44) and (5.45) respectively. Assume that $\xi_n=1$ and $\xi_0\le Q^{-1-v}$ for some $0<v\le 1$. Then for every $1\le k\le n$

$$\prod_{i=0}^{k-1} d|g_i|_p \ge Q^v\,. \tag{5.61}$$

Proof. The proof of this is similar to that of Corollary 5.3.5. Again from the definition of d and g_i it can be seen that

$$\prod_{i=0}^{n} d|g_i|_p = 1\,. \tag{5.62}$$

Using equations (5.44) and (5.45) with δ_i defined by equation (5.28) it can be easily seen that

$$\frac{1}{d|g_0|_p} = \xi_0 Q \leq Q^{-v} \tag{5.63}$$

$$d|g_n|_p = \frac{1}{Q\xi_n} = Q^{-1} \tag{5.64}$$

Recall, by (5.44), that

$$g_i = \frac{\xi_i}{\delta}$$

Then, by (5.55), inequalities (5.51) are fulfilled with $(s_1, \ldots, s_n) = (1, \ldots, 1)$. Combining (5.63) and (5.64) with Proposition 5.3.4 we obtain that

$$\left(\prod_{i=0}^{k-1} d|g_i|_p\right)^{-1} \leq \max\left\{\frac{1}{Q^v}, \frac{1}{Q}\right\} = \frac{1}{Q^v}\,,$$

implying (5.61), as required. □

We now have all the parts to show that the map h as defined above satisfies the properties stated in Corollary 5.3.3.

Proposition 5.3.7. *Let $\Delta \in \mathfrak{B}(\mathbb{Z}_S, n+1)$ where $S = \{p, \infty\}$ and $\mathbf{a}_1, \ldots, \mathbf{a}_k$ be a basis of Δ, let h_1 and h_2 be given by (5.36)and (5.37) respectively. Then*

$$h_2\mathbf{a}_1 \wedge \cdots \wedge h_2\mathbf{a}_k = d^k(\mathbf{a}_1 \wedge \cdots \wedge \mathbf{a}_k) \tag{5.65}$$

and the coordinates of $h_1(x)\mathbf{a}_1 \wedge \cdots \wedge h_1(x)\mathbf{a}_k$ in the standard basis are

$$\left(\prod_{i\in I} g_i\right) p^{-l} R_I(x)\,, \tag{5.66}$$

where $I = \{i_1 < \cdots < i_k\} \subset \{0, \ldots, n\}$, $R_I(x) \in \mathbb{Z}[x]$ is a polynomial of degree $\leq M = \left[(\frac{n+1}{2})^2\right]$ and height

$$H(R_I) \ll \|p^l(\mathbf{a}_1 \wedge \cdots \wedge \mathbf{a}_k)\|_\infty \tag{5.67}$$

and l is the smallest integer such that $p^l(\mathbf{a}_1 \wedge \cdots \wedge \mathbf{a}_k)$ is an integer multivector. Furthermore, R_I is non-zero for $I = \{0, \ldots, k-1\}$.

Proof. First, we note that (5.67) is an immediate consequence of the fact that $h_2\mathbf{a}_i = d\mathbf{a}_i$ for every $1 \le i \le k$. Now, consider the matrix

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1k} \\ a_{21} & a_{22} & \cdots & a_{2k} \\ a_{31} & a_{32} & \cdots & a_{3k} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n+1,1} & a_{n+1,2} & \cdots & a_{n+1,k} \end{pmatrix} \tag{5.68}$$

of the coordinates of $\mathbf{a}_1, \ldots, \mathbf{a}_k$. Then, the coordinates of $h_1(x)\mathbf{a}_1 \wedge \cdots \wedge h_1(x)\mathbf{a}_k$ in the standard basis are the determinants $\det(h_{1,I}(x)A)$, where $I = \{i_1 < \cdots < i_k\} \subset \{0, \ldots, n\}$ and $h_{1,I}(x)$ is the matrix composed of the rows number $i_1 + 1, \ldots, i_k + 1$ from $h_1(x)$.

When $I = \{0, \ldots, k-1\}$. Then, it is readily seen that

$$\det\left(h_{1,I}(x)A\right) = \\ = \det \begin{pmatrix} g_0 P_1(x) & g_0 P_2(x) & \cdots & g_0 P_k(x) \\ g_1 P_1'(x) & g_1 P_2'(x) & \cdots & g_1 P_k'(x) \\ \vdots & \vdots & \ddots & \vdots \\ \frac{g_k}{(k-1)!} P_1^{(k-1)}(x) & \frac{g_k}{(k-1)!} P_2^{(k-1)}(x) & \cdots & \frac{g_k}{(k-1)!} P_k^{(k-1)}(x) \end{pmatrix}, \tag{5.69}$$

where $P_i(x) = \sum_{j=0}^{n} a_{j+1,i} x^j$. It can be easily verified that the right hand side of (5.69) is a constant times the Wronskian of $P_1, \ldots, P_k$ so we know it is non-zero. This follows from the fact that $P_1, \ldots, P_k$ are linearly independent over $\mathbb{R}$, and this is because $\mathbf{a}_1, \ldots, \mathbf{a}_k$ are linearly independent over $\mathbb{Q}$.

Another way to work out $\det\left(h_{1,I}(x)A\right)$ is by using the Laplace identity:

$$\det\left(h_{1,I}(x)A\right) = (g_{i_1}\mathbf{r}_{i_1} \wedge \cdots \wedge g_{i_k}\mathbf{r}_{i_k}) \cdot (\mathbf{a}_1 \wedge \cdots \wedge \mathbf{a}_k)\,, \tag{5.70}$$

where $\mathbf{r}_i$ is the i-th row of $h_1(x)$.

Expanding $\mathbf{r}_{i_1} \wedge \cdots \wedge \mathbf{r}_{i_k}$ out we obtain a vector of $N = \binom{n+1}{k}$ polynomials, say $\hat{Q}_1, \ldots, \hat{Q}_N \in \mathbb{Z}[x]$, of degree

$$\le n + \cdots + (n+1-k) - 1 - \cdots - (k-1) \le \left[\left(\tfrac{n+1}{2}\right)^2\right] = M\,.$$

Then we can write $\hat{Q}_i(x) = \sum_{j=0}^{M} \hat{q}_{j,i} x^j$ for $1 \le i \le N$ where $\hat{q}_{j,i} \in \mathbb{Z}$ depend only on n and k. In turn, we can write $\mathbf{a}_1 \wedge \cdots \wedge \mathbf{a}_k = (\hat{a}_1, \ldots, \hat{a}_N)$, where $\hat{a}_j \in \mathbb{Z}\left[\frac{1}{p}\right]$ for

each j. By definition, l is the smallest integer such that

$$(\hat{b}_1, \dots, \hat{b}_N) := p^l(\hat{a}_1, \dots, \hat{a}_N) \in \mathbb{Z}^N \,. \tag{5.71}$$

Hence, by (5.70) and (5.71),

$$\begin{aligned}
\det(h_{1,I}(x)A) &= \left(\prod_{i\in I} g_i\right)(\hat{Q}_1(x), \dots, \hat{Q}_N(x)) \cdot (\hat{a}_1, \dots, \hat{a}_N) \\
&= \left(\prod_{i\in I} g_i\right) p^{-l}(\hat{Q}_1(x), \dots, \hat{Q}_N(x)) \cdot (\hat{b}_1, \dots, \hat{b}_N) \\
&= \left(\prod_{i\in I} g_i\right) p^{-l} \sum_{i=1}^{N} \hat{b}_i Q_i(x) \\
&= \left(\prod_{i\in I} g_i\right) p^{-l} \sum_{i=1}^{N} \hat{b}_i \sum_{j=0}^{M} \hat{q}_{j,i} x^j \\
&= \left(\prod_{i\in I} g_i\right) p^{-l} \sum_{j=0}^{M} c_j x^j, \quad \text{where } c_j := \sum_{i=1}^{N} \hat{b}_i \hat{q}_{j,i} \,.
\end{aligned} \tag{5.72}$$

Define

$$R_I(x) := \sum_{j=0}^{M} c_j x^j \,. \tag{5.73}$$

Clearly $R_I(x) \in \mathbb{Z}[x]$. Finally, it can be seen that

$$|c_j| \le \sum_{i=1}^{M} \left|\hat{b}_i \hat{q}_{j,i}\right| \ll_n \max_i |\hat{b}_i| = \|(\mathbf{b}_1 \wedge \cdots \wedge \mathbf{b}_k)\|_\infty = \|p^l(\mathbf{a}_1 \wedge \cdots \wedge \mathbf{a}_k)\|_\infty \,,$$

whence (5.67) follows. □

Proposition 5.3.8. *Let $\Delta \in \mathfrak{B}(\mathbb{Z}_S, n+1)$ where $S = \{p, \infty\}$ and $h_1(x)$ and $h_2(x)$ be the matrices from equations (5.36) and (5.37) respectively. Then*

$$\operatorname{cov}(h(x)\Delta) \gg \left(\prod_{i=0}^{k-1} d|g_i|_p\right) |\widetilde{R}(x)|_p \tag{5.74}$$

for some $\widetilde{R} \in \mathbb{Z}_S[x]$ such that

$$\widetilde{R} = \sum_{j=0}^{M} \tilde{c}_j x^j \quad \textit{with} \quad \max_j |\tilde{c}_j|_p = 1 \,. \tag{5.75}$$

Proof. Using the same notation as in the proof of Proposition 5.3.7, let

$$I = \{0, \dots, k-1\}$$

where $k = \operatorname{rank}\Delta$. By Proposition 5.3.7, equations (5.47) and (5.48), we have that

$$\begin{aligned}\operatorname{cov}(h(x)\Delta) &\geq |\det(h_{1,I}(x)A)|_p \cdot \|d^k(\mathbf{a}_1 \wedge \cdots \wedge \mathbf{a}_k)\|_\infty, \\ &= \left|\left(\prod_{i=0}^{k-1} g_i\right) p^{-l} R_I(x)\right|_p \cdot \|d^k p^{-l} p^l(\mathbf{a}_1 \wedge \cdots \wedge \mathbf{a}_k)\|_\infty, \\ &= \left(\prod_{i=0}^{k-1} d|g_i|_p\right) |R_I(x)|_p \, \|p^l(\mathbf{a}_1 \wedge \cdots \wedge \mathbf{a}_k)\|_\infty.\end{aligned} \tag{5.76}$$

As in the proof of Proposition 5.3.7, let c_j denote the coefficients of R_I, so that R_I has form (5.73). Let $\widetilde{C} = \max_j |c_j|_p$ and define

$$\widetilde{R}(x) := R_I(x)\widetilde{C} = \sum_{j=0}^{M} \tilde{c}_j x^j\,, \quad \text{where } \tilde{c}_j = c_j\widetilde{C}\,.$$

Note that

$$\max_j |\tilde{c}_j|_p = \max_j |c_j\widetilde{C}|_p = \max_j |c_j|_p \widetilde{C}^{-1} = 1\,. \tag{5.77}$$

Thus the vector $(\tilde{c}_0, \ldots, \tilde{c}_M)$ of coefficients of $\widetilde{R}$ is placed on the unit ball in $\mathbb{Q}_p^{M+1}$. Since $|c_j|_p|c_j| \geq 1$, we have that $|c_j|_p\|\mathbf{c}\|_\infty = |c_j|_p H(R_I) \geq 1$. Therefore, $\widetilde{C}H(R_I) \geq 1$ and, by (5.67), we get that

$$\widetilde{C} \cdot \|p^l(\mathbf{a}_1 \wedge \cdots \wedge \mathbf{a}_k)\|_\infty \gg 1\,. \tag{5.78}$$

Observe that

$$|R(x)|_p = \left|\widetilde{R}(x)\widetilde{C}^{-1}\right|_p = \left|\tilde{R}(x)\right|_p \cdot \widetilde{C} \tag{5.79}$$

using (5.76),(5.78) and (5.79) we obtain that

$$\begin{aligned}\operatorname{cov}(h(x)\Delta) &\geq \left(\prod_{i=0}^{k-1} d|g_i|_p\right) |\tilde{R}(x)|_p \cdot \widetilde{C} \cdot \|p^l(\mathbf{a}_1 \wedge \cdots \wedge \mathbf{a}_k)\|_\infty \\ &\gg \left(\prod_{i=0}^{k-1} d|g_i|_p\right) |\tilde{R}(x)|_p\end{aligned}$$

as required. □

Proposition 5.3.9. *Let δ, Q, $\xi_0, \ldots, \xi_n$, $g_0, \ldots, g_n$, d be as in Corollary 5.3.5 or Corollary 5.3.6. Let $\rho = 1$ and $\alpha = M^{-1}$, where $M = [\left(\frac{n+1}{2}\right)^2]$. Then for any non-empty ball $B \subset \mathbb{Z}_p$ the map $h := (h_1, h_2) := \mathbb{Q}_p \to \mathrm{GL}(n+1, \mathbb{Q}_p) \times \mathrm{GL}(n+1, \mathbb{R})$ as defined in (5.38) satisfies the conditions stated in Corollary 5.3.3, in which $C > 0$ depends on n only, for all sufficiently large Q.*

Proof. The validity of condition (1) in Corollary 5.3.3 follows from Lemma 5.3.2. Indeed, by Proposition 5.3.7 and the definition of $\operatorname{cov}(h(\cdot)\Delta)$, the function $\operatorname{cov}(h(\cdot)\Delta)$ is the maximum of p-adic absolute values of polynomials in one variable of degree at most M, and therefore, by Lemma 5.3.2 and Lemma 3.1 in [35], it is (C,α) good for $\alpha = M^{-1}$ and some $C > 0$ depending only on M. Thus, ultimately C depends on n only.

Now we verify condition (2) in Corollary 5.3.3. Fix any non-empty ball $B \subset \mathbb{Z}_p$. If $k = n+1$ then, since $\prod_{i=0}^{n}(d|g_i|_p) = 1$, using the explicit form of h_1 and h_2 given by (5.36) and (5.37) one readily verifies that $\operatorname{cov}(h(x)\Delta) = 1 \geq \rho$. Indeed, since Δ is primitive the standard basis $\mathbf{e}_i = (\delta_{i,1}, \dots, \delta_{i,n+1})$ with $1 \leq i \leq n+1$, where $\delta_{i,j} = 1$ if $i = j$ and 0 otherwise, is a basis of Δ. Then $\|h_1(x)\mathbf{e}_1 \wedge \cdots \wedge h_1(x)\mathbf{e}_{n+1}\|_p = \prod_{i=0}^{n}|g_i|_p$ and $\|h_2(x)\mathbf{e}_1 \wedge \cdots \wedge h_2(x)\mathbf{e}_{n+1}\|_\infty = d^{n+1}$. Then

$$\begin{aligned}\operatorname{cov}(h(x)\Delta) &= \|h_1(x)\mathbf{e}_1 \wedge \cdots \wedge h_1(x)\mathbf{e}_{n+1}\|_p \times \\ &\quad \times \|h_2(x)\mathbf{e}_1 \wedge \cdots \wedge h_2(x)\mathbf{e}_{n+1}\|_\infty = \prod_{i=0}^{n}(d|g_i|_p) = 1\,,\end{aligned}$$

as claimed above.

Naturally, for the rest of the proof we will assume that $1 \leq k \leq n$. By (5.74) we have that

$$\|\operatorname{cov}(h(x)\Delta)\|_B \gg \left(\prod_{i=0}^{k-1} d|g_i|_p\right) \sup_{x\in B}|\widetilde{R}_{\tilde{\mathbf{c}}}(x)|_p\,, \tag{5.80}$$

where $\tilde{\mathbf{c}} = (\tilde{c}_0, \dots, \tilde{c}_M) \in \mathbb{Z}[\frac{1}{p}]^{M+1}$ and $\widetilde{R}_{\tilde{\mathbf{c}}}$ satisfies (5.75). Define

$$\tilde{\rho} := \inf_{\|\tilde{\mathbf{c}}\|_p=1} \sup_{x\in B}|\widetilde{R}_{\tilde{\mathbf{c}}}(x)|_p\,. \tag{5.81}$$

Clearly $\tilde{\rho}$ is a constant depending on k, n, p and B only. Since B is non-empty, we have that for every choice of $\tilde{\mathbf{c}} \in \mathbb{Q}_p^{M+1}$ with $\|\tilde{\mathbf{c}}\|_p = 1$ the quantity

$$\sup_{x\in B}|\widetilde{R}_{\tilde{\mathbf{c}}}(x)|_p \tag{5.82}$$

is strictly positive. Also, since for every fixed $x \in \mathbb{Q}_p$, $\widetilde{R}_{\tilde{\mathbf{c}}}(x)$ is a linear function of $\tilde{\mathbf{c}}$, we have that (5.82) depends on $\tilde{\mathbf{c}}$ continuously. Since the set of $\tilde{\mathbf{c}} \in \mathbb{Q}_p^{M+1}$ subject to $\|\tilde{\mathbf{c}}\|_p = 1$ is compact, we conclude that $\tilde{\rho}$, given by (5.81), is strictly positive.

Now, combining (5.80) and (5.81), and using Corollary 5.3.5 and Corollary 5.3.6 together with the facts that $\delta \leq 1$ and $C_2 \geq 1$, we obtain that

$$\|\operatorname{cov}(h(x)\Delta)\|_B \gg Q^v\delta^{4n+2}C_2^{-2n-2}\tilde{\rho}\,,$$

where the implied constant depends on n only. Therefore, since δ, C_2 and $\tilde{\rho}$ do not depend on Q, we have that

$$\|\operatorname{cov}(h(x)\Delta)\|_B \geq \rho = 1$$

provided that Q is sufficiently large. □

Combining Proposition 5.3.9 with Corollary 5.3.3 we obtain the following:

Corollary 5.3.10. *Let $n \geq 2$ be an integer, p be a prime number, μ be Harr measure on $\mathbb{Q}_p$, δ, Q, $\xi_0, \ldots, \xi_n$, $g_0, \ldots, g_n$, d be as in Corollary 5.3.5 or Corollary 5.3.6, in particular $\xi_n = 1$ and $\xi_0 \leq Q^{-1-v}$ for some fixed $v > 0$. Let $\alpha = [\left(\frac{n+1}{2}\right)^2]^{-1}$ and $h := (h_1, h_2) := \mathbb{Q}_p \to \mathrm{GL}(n+1, \mathbb{Q}_p) \times \mathrm{GL}(n+1, \mathbb{R})$ be as defined in (5.38). Then there exists a constant $K > 0$ depending on n and p only satisfying the following statement. For any non-empty ball $B \subset \mathbb{Z}_p$ there exists $Q_0 = Q_0(B, n, p, v, C_2)$ such that for all $Q \geq Q_0$ and $\varepsilon > 0$ one has that*

$$\mu\left(\{x \in B : \delta(h(x)\mathbb{Z}_S^{n+1}) < \varepsilon\}\right) \leq K\varepsilon^{\alpha}\mu(B). \tag{5.83}$$

We remark that the constant K appearing in (5.83) is given by

$$K = C(n+1)(3p)^{2(n+1)},$$

where C arises from condition (2) of Corollary 5.3.3 and, as established in Proposition 5.3.9, depends only on n and p.

5.4 PROOF OF LEMMA 5.2.1

The proof of Lemma 5.2.1 will now be given. As outlined in §5.2.1, we can assume without loss of generality that ξ_i and Q are powers of p, that is (5.19) and (5.20) are satisfied for some integers $b_i \in \mathbb{Z}_{\geq 0}$ and $t \in \mathbb{N}$ satisfying (5.18). Let $B_{Q,1}$ be the convex body defined by (5.24) with $C_2 = 1$. It is readily seen that

$$\operatorname{vol}(B_{Q,1}) = (2Q)^{n+1}. \tag{5.84}$$

Let Γ be the lattice defined in Proposition 5.2.2. Let $\lambda_1, \ldots, \lambda_{n+1}$ be the successive minima of $B_{Q,1}$ on Γ, that is

$$\lambda_i := \inf\left\{\lambda > 0 : \operatorname{rank}\left(\Gamma \cap (\lambda B_{Q,1})\right) \geq i\right\}.$$

By (5.84), (5.25) and Minkowski's second theorem, we get that

$$(2Q)^{n+1}\prod_{i=1}^{n+1}\lambda_i \le 2^{n+1}\left(\prod_{i=0}^{n}\xi_i\right)^{-1}. \tag{5.85}$$

Hence, by (5.20) and the inequalities $\lambda_1 \le \ldots, \le \lambda_{n+1}$, we get that

$$\lambda_1^n\lambda_{n+1} \le \prod_{i=1}^{n+1}\lambda_i \le Q^{-(n+1)}\left(\prod_{i=0}^{n}\xi_i\right)^{-1} = 1\,. \tag{5.86}$$

Now define the following 'exceptional' set

$$E(B;\varepsilon_0) = \{x \in B : \lambda_1 \le \varepsilon_0\}\,, \tag{5.87}$$

where $\varepsilon_0 > 0$ is a small parameter, to be determined soon. By the definition of λ_1, there must exist a polynomial $P = a_nx^n + \cdots + a_0 \in \mathbb{Z}[x]$ satisfying (5.22) and

$$0 < \max_{0\le i\le n}|a_i| \le \varepsilon_0 Q. \tag{5.88}$$

By Proposition 5.2.4 we must have that $c(h(x)\mathbb{Z}_S^m) \le \varepsilon_0$ for the h as in that proposition with $\delta^2 = \varepsilon_0$. In particular, we assume that ε_0 is an even power of p. Then, by Corollary 5.3.10, we have that

$$\mu(E(B;\varepsilon_0)) \le K\varepsilon_0^{\alpha}\mu(B)\,, \tag{5.89}$$

provided that Q is sufficiently large. Choose

$$\varepsilon_0 \le \left(\frac{1-\kappa}{(n+2)K}\right)^{1/\alpha}.$$

Then

$$\mu(E(B;\varepsilon_0)) \le \frac{1-\kappa}{n+2}\,\mu(B). \tag{5.90}$$

Then if $x \notin E(B;\varepsilon_0)$ we must have that $\lambda_1 \ge \varepsilon_0$ and so combining this with equation (5.86) gives

$$\lambda_{n+1} \le c_0 := (\varepsilon_0)^{-n}. \tag{5.91}$$

A polynomial of degree at most n can be identified with a vector in $\mathbb{R}^{n+1}$ by associating it with its coefficient vector $\{a_0, a_1, ..., a_n\}$. This allows us to view the space of such polynomials as an $(n+1)$-dimensional vector space over $\mathbb{R}$. The subset of integer polynomials, where each coefficient is in $\mathbb{Z}$ forms a full-rank discrete subgroup of $\mathbb{R}^{n+1}$ which is precisely the lattice Γ. Hence by the definition of λ_{n+1}, there are $n+1$

linearly independent polynomials $P_j(x) = a_{j,n}x^n + \cdots + a_{j,0} \in \mathbb{Z}[x]$ for $0 \leq j \leq n$ satisfying (5.22) and

$$\max_{0\leq i\leq n} |a_{j,i}| \leq c_0 Q. \tag{5.92}$$

Define the sub-lattice Λ of Γ as the $\mathbb{Z}$-span of $\mathbf{a}_j = (a_{j,0}, \ldots, a_{j,n+1})$ for $0 \leq j \leq n$. Then

$$\operatorname{cov}(\Lambda) = m \cdot \operatorname{cov}(\Gamma)\,,$$

where $m \in \mathbb{N}$ is the index of Λ in Γ. Since the fundamental domain of Λ can be chosen to be contained in the body defined by (5.92), we have that

$$\operatorname{cov}(\Lambda) \leq (2c_0Q)^{n+1} = (2c_0)^{n+1} \operatorname{cov}(\Gamma)\,,$$

where the latter follows from (5.20) and (5.25). Hence, $m \leq (2c_0)^{n+1}$. Recall now Bertrand's Postulate that for every $n > 1$, there is always at least one prime p such that $n < p < 2n$. In this way it is possible to choose a fixed prime number q such that $m < q < 4m$ and $q \neq p$. The width of the gap is chosen so that we can find at least two primes by Bertrand's Postulate so at least one of them is not p.

Let A be the matrix with the vectors $\mathbf{a}_j$, the basis of Λ, being its columns. Then $1 \leq |\det A| = \operatorname{cov}(\Lambda) = m \operatorname{cov}(\Gamma)$ and since $\operatorname{cov}(\Gamma) = Q^{n+1}$ is a power of p and $q > m$, then q does not divide $\operatorname{cov}(\Lambda)$. Therefore q does not divide $\det A$ and the following system of congruence equations has a unique non-zero solution $\mathbf{t} = (t_0, t_1, \ldots, t_n)^T \in [0, q-1]^{n+1}$

$$A\mathbf{t} \equiv \mathbf{s} \mod q, \tag{5.93}$$

where $\mathbf{s} = (0, 0, \ldots, 0, 1)^T$ and ^{T} means a transpose. In particular, we have that $q \mid (A\mathbf{t} - \mathbf{s})$.

Now for each $l \in [0, n]$ define $\mathbf{r}_l := (1, 1, \ldots, 1, 0 \ldots, 0)^T$, where the number of zeros is l, and let $\boldsymbol{\gamma}_l := (\gamma_{l,0}, \gamma_{l,1}, \ldots, \gamma_{l,n})^T \in [0, q-1]^{n+1}$ be the unique integer solution to the system

$$A\boldsymbol{\gamma}_l \equiv -\left(\frac{A\mathbf{t} - \mathbf{s}}{q}\right) + \mathbf{r}_l \mod q. \tag{5.94}$$

Let $\boldsymbol{\eta}_l := \mathbf{t} + q\boldsymbol{\gamma}_l$, where $\boldsymbol{\eta}_l = (\eta_{l,0}, \eta_{l,1}, \ldots, \eta_{l,n})^T$ is an integer vector. Then, clearly $\boldsymbol{\eta}_l \equiv \mathbf{t} \mod q$ and so $\boldsymbol{\eta}_l$ is a solution to (5.93). Furthermore, by our choice, the vectors $\mathbf{r}_l$ are linearly independent, and therefore the vectors $\boldsymbol{\eta}_l$ and consequently

the vectors $\boldsymbol{\eta_l}$ are linearly independent. Therefore the following polynomials with integer coefficients are linearly independent:

$$\widetilde{P}_l(x) := \sum_{i=0}^{n} \eta_{l,i} P_i(x) \qquad (0 \le l \le n)\,. \tag{5.95}$$

Fix any l and write $\tilde{P}_l(x)$ as $\tilde{a}_0 + \tilde{a}_1 x + \cdots + \tilde{a}_n x^n$. Then, as is easily seen, that $(\tilde{a_0}, \tilde{a}_1, \ldots, \tilde{a}_n)^t = A\boldsymbol{\eta}_l$ and so it must be that $A\boldsymbol{\eta}_l \equiv \mathbf{s} \mod q$. Therefore, $\tilde{a}_i \equiv 0 \mod q$ for $0 \le i \le n-1$, $\tilde{a}_n \equiv 1 \mod q$ and $\tilde{a}_0 \not\equiv 0 \mod q^2$. Thereby, $\deg P_l = n$ and, by Eisenstein's criterion, $\widetilde{P}_l$ is irreducible, for all $0 \le l \le n$.

Further, without loss of generality we can assume $\widetilde{P}_l$ are primitive, as otherwise we can just divide through by the greatest common divisor. The height of the polynomials can be estimated by calculating an upper bound on $\boldsymbol{\eta}_l$:

$$\begin{aligned} \eta_{l,i} &= t_i + q\gamma_{l,i} \\ &\le q - 1 + q(q-1) \\ &\le q^2 - 1 \\ &\le (4m)^2 - 1. \end{aligned} \tag{5.96}$$

Define $C_2 \ge c_0((4m)^2 - 1)$ to be the smallest value satisfying (5.21), hence by equation (5.95) it is obtained that

$$\max_{0 \le i \le n} |\tilde{a}_i| \le C_2 Q. \tag{5.97}$$

Also, by construction, the coefficients of every polynomial $\widetilde{P}_l$ are in $\Lambda \subset \Gamma$ and hence the right hand side inequalities of (5.16) hold. The remainder of the proof is dedicated to establishing the lower bounds in (5.16).

To do this we use equation (5.27) with δ_i defined by equation (5.28) for some sufficiently small $\delta = \delta_0 > 0$, to be determined soon. Define the set

$$E_{i'}(B, \delta_0) := \left\{ x \in B : \begin{array}{c} \exists\ P \in \mathbb{Z}[x] \text{ with } \deg(P) = n \\ \text{and } H(P) \le C_2 Q \text{ such that} \\ \text{equations } (5.27)_{\delta=\delta_0} \text{ hold} \end{array} \right\}. \tag{5.98}$$

Now we can use Corollary 5.3.10 similarly to the above argument to get that

$$\mu(E_j(B, \delta_0)) \le \frac{1-\kappa}{n+2} \mu(B) \tag{5.99}$$

for sufficiently large Q. Define

$$G_B := B \setminus \left(\bigcup_{j=0}^{n} E_j(B, \delta_0) \cup E(B, \varepsilon_0) \right) . \tag{5.100}$$

Then for any $x \in G_B$ the polynomials $\widetilde{P}_l$ we have constructed necessarily satisfy equations (5.16) and $C_1 Q \leq H(\widetilde{P}_l) \leq C_2 Q$ with $C_1 = \varepsilon_0$. Further we estimate the measure of G_B, to show that equation (5.15) holds, as follows

$$\begin{aligned} \mu(G_B) &\geq \mu(B) - \sum_{i=0}^{n} \mu(E_j(B, \delta_0)) - \mu(E(B, \varepsilon_0)) \\ &\geq \mu(B) - (n+2)\frac{1-\kappa}{n+2}\mu(B) = \kappa\mu(B). \end{aligned} \tag{5.101}$$

This completes the proof.

5.5 FINDING CLOSE ROOTS

In this Section we will establish how close to x the roots of a polynomial satisfying system (5.16) are. The associated parameters ξ_i will be suitably chosen. We will use Hensel's Lemma, which we already discussed in Section 2.2.3 to identify a suitable root $\alpha \in \mathbb{Q}_p$ of P close to x. For convenience, we repeat the statement of Hensel's Lemma here.

Lemma 5.5.1 (Hensel's Lemma)**.** *Suppose that $f \in \mathbb{Z}_p[x]$ and $x \in \mathbb{Z}_p$ satisfy $|f(x)|_p < |f'(x)|_p^2$. Then there exists a unique $\alpha \in \mathbb{Z}_p$ such that*

1. $f(\alpha) = 0$,
2. $|f'(\alpha)|_p = |f'(x)|_p$,
3. $|x - \alpha|_p < |f(x)| \cdot |f'(x)|_p^{-1} < |f'(x)|_p$.

Now we specialise Hensel's Lemma to the setup of Lemma 5.2.1.

Corollary 5.5.2. *Let $n \geq 2$, $0 < \delta_0 < 1$ be a sufficiently small constant, $Q > 1$ and $\xi_0 = Q^{-\theta_0}$, $\xi_1 = Q^{-\theta_1} \leq \xi_2 = \cdots \leq \ldots \xi_{n-1} \leq \xi_n = 1$. Suppose that*

$$Q^{-\theta_0} < (\delta_0 Q^{-\theta_1})^2 . \tag{5.102}$$

Let $x \in \mathbb{Z}_p$. Then for any polynomial $P \in \mathcal{P}_n(Q)$ satisfying system (5.16) there exists a unique root $\alpha \in \mathbb{Z}_p$ of P such that

$$|x - \alpha|_p \leq \delta_0^{-1} Q^{-\theta_0 + \theta_1}. \tag{5.103}$$

Proof. Obviously, with $f = P$, (5.16) and (5.102) verify the condition $|f(x)|_p < |f'(x)|_p^2$ in Hensel's Lemma, and therefore (5.103) follows immediately from conclusion 3 of Hensel's Lemma combined with (5.16) and the condition $\theta_0 + \theta_1 = n + 1$. Indeed, we have that

$$|\alpha - \xi|_p \leq \xi_0(\delta_0\xi_1)^{-1} = \delta_0^{-1}Q^{-\theta_0+\theta_1}. \tag{5.104}$$

□

Lemma 5.5.3. *Let $x \in \mathbb{Z}_p$ be a fixed point and $P \in \mathbb{Z}_p[x]$ be a polynomial of degree $n \geq 2$, with the leading coefficient a_n and roots $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}_p}$, some possibly repeated, ordered so that*

$$|x - \alpha_1|_p \leq |x - \alpha_2|_p \leq \cdots \leq |x - \alpha_n|_p. \tag{5.105}$$

Then for any $0 \leq j < n$, the following bound holds

$$\left|\tfrac{1}{j!}P^{(j)}(x)\right|_p \leq |a_n|_p|x - \alpha_{j+1}|_p \cdots |x - \alpha_n|_p. \tag{5.106}$$

Furthermore, if $|x - \alpha_j|_p < |x - \alpha_{j+1}|_p$ then we have equality in (5.106).

Proof. To begin with, write the polynomial P as the product

$$P(x) = a_n(x - \alpha_1)\cdots(x - \alpha_n)\,.$$

Then on differentiating this expression we obtain that

$$\tfrac{1}{j!}P^{(j)}(x) = a_n \sum_{1\leq i_1<\cdots<i_{n-j}\leq n} (x - \alpha_{i_1})\cdots(x - \alpha_{i_{n-j}}). \tag{5.107}$$

Define $T_{j+1} = (x - \alpha_{j+1})\cdots(x - \alpha_n)$. By (5.105), this can be seen to be the term with the largest p-adic value in the sum. We will also define $\widehat{T}_{j+1}$ to be the term with the second largest p-adic value. The p-adic value of each term in the sum in (5.107) is less than or equal to $|T_{j+1}|_p$. Hence by the ultrametric property it must be that

$$\left|\tfrac{1}{j!}P^{(j)}(x)\right|_p \leq |a_n|_p|T_{j+1}|_p\,, \tag{5.108}$$

which is exactly (5.106). Next, we can rewrite equation (5.107) as

$$\tfrac{1}{j!}P^{(j)}(x) = a_n \sum_{1\leq i_1<\cdots<i_{n-j}\leq n} (x - \alpha_{i_1})\cdots(x - \alpha_{i_{n-j}}) - T_{j+1} + T_{j+1}. \tag{5.109}$$

By the ultrametric property again, we must have that

$$\left| \sum_{1 \le i_1 < \cdots < i_{n-j} \le n} (x - \alpha_{i_1}) \cdots (x - \alpha_{i_{n-j}}) - T_{j+1} \right|_p \le \left| \widehat{T}_{j+1} \right|_p , \tag{5.110}$$

as by taking away the largest term we are left with the second largest term. Observe that $|x - \alpha_j|_p < |x - \alpha_{j+1}|_p$ implies that $\widehat{T}_{j+1} < T_{j+1}$, and therefore by, (5.109), (5.110) and the ultrametric property, we obtain that $|\frac{1}{j!} P^{(j)}(x)|_p = |a_n|_p |T_{j+1}|_p$. This means exactly the equality in (5.106). □

Lemma 5.5.4. *Let $x \in \mathbb{Z}_p$ and $Q > 1$. Let $P \in \mathcal{P}_n(Q)$ be such that inequalities (5.16) hold with $\xi_i = Q^{-\theta_i}$ for some θ_i, where $0 \le i \le n$. Let $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}_p}$ be the roots of P ordered as in Lemma 5.5.3. Define*

$$d_j = \theta_{j-1} - \theta_j \tag{5.111}$$

for $1 \le j \le n$ and suppose that

$$d_1 \ge d_2 \ge \cdots \ge d_n \ge 0 \,. \tag{5.112}$$

Then the roots of P satisfy the inequalities

$$|x - \alpha_j|_p \le \delta_0^{-1} Q^{-d_j} \qquad (1 \le j \le n). \tag{5.113}$$

Proof. We will prove (5.113) by induction on j. First consider $j = 1$. Then, using (5.106), we obtain that

$$|P'(x)|_p \le |a_n|_p |x - \alpha_2|_p \cdots |x - \alpha_n|_p = \frac{|P(x)|_p}{|x - \alpha_1|_p}. \tag{5.114}$$

By rearranging and using the bounds from equation (5.16) we obtain that

$$|x - \alpha_1|_p \le \frac{|P(x)|_p}{|P'(x)|_p} \le \frac{Q^{-\theta_0}}{\delta_0 Q^{-\theta_1}} = \delta_0^{-1} Q^{-d_1} \tag{5.115}$$

as required in (5.113) for $j = 1$.

Now suppose that $1 \le j < n$ and (5.113) holds for this j. We shall prove (5.113) for $j + 1$. Define $T_{j+1} = (x - \alpha_{j+1}) \cdots (x - \alpha_n)$ and $T_{j+2} = (x - \alpha_{j+2}) \cdots (x - \alpha_n)$, as in Lemma 5.5.3, where $T_{j+2} = 1$ if $j = n - 1$. By Lemma 5.5.3, we get that

$$\begin{aligned} \left| \tfrac{1}{(j+1)!} P^{(j+1)}(x) \right|_p \cdot |x - \alpha_{j+1}|_p &\le |a_n|_p |T_{j+2}|_p |x - \alpha_{j+1}|_p \\ &= |a_n|_p |T_{j+1}|_p \,, \end{aligned} \tag{5.116}$$

and so

$$|x-\alpha_{j+1}|_p \le \frac{|a_n|_p|T_{j+1}|_p}{\left|\frac{1}{(j+1)!}P^{(j+1)}(x)\right|_p}. \tag{5.117}$$

If additionally, we assume that $|x-\alpha_j|_p < |x-\alpha_{j+1}|_p$ then by Lemma 5.5.3, we obtain that $|a_n|_p|T_{j+1}|_p = \left|\frac{1}{j!}P^{(j)}(x)\right|_p$ and so together with (5.117) and (5.16) it follows that

$$|x-\alpha_{j+1}|_p \le \frac{\left|\frac{1}{j!}P^{(j)}(x)\right|_p}{\left|\frac{1}{(j+1)!}P^{(j+1)}(x)\right|_p} \le \frac{Q^{-\theta_j}}{\delta_0 Q^{-\theta_{j+1}}} = \delta_0^{-1}Q^{-d_{j+1}}. \tag{5.118}$$

If $|x-\alpha_j|_p < |x-\alpha_{j+1}|_p$ does not hold, then, by the ordering (5.105), we have that $|x-\alpha_j|_p = |x-\alpha_{j+1}|_p$. Then, by (5.112) and the induction assumption, we get that

$$|x-\alpha_{j+1}|_p = |x-\alpha_j|_p \le \delta_0^{-1}Q^{-d_j} \le \delta_0^{-1}Q^{-d_{j+1}}, \tag{5.119}$$

thereby proving the required statement for $j+1$ and finishing the proof. □

5.6 PROOF OF THEOREM 5.1.1

Let $n \ge 2$, p be a prime, $v = 1$, $0 < \kappa < 1$ and δ_0, C_1 and C_2 be the constants arising form Lemma 5.2.1. Take any ball $B \subset \mathbb{Z}_p$ and let $Q > Q_0$, where Q_0 is as in Lemma 5.2.1.

Let θ satisfy equation (5.3). Define $\xi_2 = \cdots = \xi_n = 1$,

$$\xi_0 = \begin{cases} \delta_0 Q^{-n-1+\theta} & \text{if } \theta > 1, \\ Q^{-n-1+\theta} & \text{if } \theta \le 1, \end{cases} \quad \text{and} \quad \xi_1 = \begin{cases} \delta_0^{-1} Q^{-\theta} & \text{if } \theta > 1, \\ Q^{-\theta} & \text{if } \theta \le 1. \end{cases}$$

Define θ_i by the equation $\xi_i = Q^{-\theta_i}$ for $0 \le i \le n$. Then, it is readily verified that

$$2 \le \frac{2}{3}(n+1) < \theta_0 \le n+1, \tag{5.120}$$

$$0 \le \theta_1 < \frac{n+1}{3} \tag{5.121}$$

and that for all sufficiently large Q the conditions of Corollary 5.5.2 are satisfied by $\xi_0, \ldots, \xi_n$ for any choice of θ.

Then, clearly (5.13) and $(5.14)_{v=1}$ hold and Lemma 5.2.1 is applicable, and we have a measurable set $G_B \subset B$ satisfying (5.15). Take any $x \in G_B$ and fix, by

Lemma 5.2.1, any primitive irreducible polynomials $P \in \mathbb{Z}[x]$ of degree n and height $C_1 Q \le H(P) \le C_2 Q$ satisfying (5.16).

Let $\alpha_1, \dots \alpha_n \in \overline{\mathbb{Q}_p}$ be the roots of P ordered as in equation (5.105). It is readily seen that (5.112) hold. Then by Lemma 5.5.4 we have

$$\begin{aligned} |x - \alpha_1|_p &\le \delta_0^{-1} Q^{-\theta_0+\theta_1} \le \delta_0^{-1} Q^{-(n+1-2\theta)}, \\ |x - \alpha_2|_p &\le \delta_0^{-1} Q^{-\theta_1} \le \delta_0^{-2} Q^{-\theta}. \end{aligned} \tag{5.122}$$

By Corollary 5.5.2, α_1 must be the same as α arising from Corollary 5.5.2 and therefore $\alpha_1 \in \mathbb{Z}_p$. By the ultrametric property $\alpha_1 \in B$ provided that Q is sufficiently large. By (5.3) and the ultrametric property again

$$|\alpha_1 - \alpha_2|_p \le \max\{|x - \alpha_i|_p, |x - \alpha_j|_p\} \le \delta_0^{-2} Q^{-\theta}. \tag{5.123}$$

This completes the proof of Theorem 5.1.1, with $C_0 = \delta_0^{-2}$. Indeed, (5.4) follows from (5.122) and (5.15), while (5.123) together with the aforementioned properties of P ensures that $\alpha = \alpha_1$ belongs to $\mathbb{A}_n(Q, \theta, C_0, C_1, C_2)$.

5.7 PROOF OF THEOREM B

Let $n \ge 2$, p be a prime, $v = 1$, $\kappa = 1/2$ and δ_0, C_1 and C_2 be the constants arising form Lemma 5.2.1. Take any ball $B = \mathbb{Z}_p$ and let $Q > Q_0$, where Q_0 is again as in Lemma 5.2.1.

Let ν satisfy equation (5.10). Let $\theta_n = 0$, $d_1, \dots, d_n$ satisfy (5.112) and let θ_{n-1}, θ_0 be defined by (5.111). Clearly, we have that

$$\theta_0 \ge \cdots \ge \theta_n = 0. \tag{5.124}$$

We also set $\xi_i = Q^{-\theta_i}$ and require that $\theta_0 + \cdots + \theta_n = n + 1$. By (5.124), we have that $\theta_0 \ge 1 + 1/n$. Hence (5.13) and $(5.14)_{v=1/n}$ hold and Lemma 5.2.1 is applicable. Therefore, there is a measurable set $G_B \subset B$ satisfying (5.15), where $B = \mathbb{Z}_p$. Take any $x \in G_B$ and fix, by Lemma 5.2.1, any primitive irreducible polynomials $P \in \mathbb{Z}[x]$ of degree n and height $C_1 Q \le H(P) \le C_2 Q$ satisfying (5.16).

Let $\alpha_1, \dots \alpha_n \in \overline{\mathbb{Q}_p}$ be the roots of P ordered such as in equation (5.105). It is readily seen that (5.112) hold. Then by Lemma 5.5.4 and the ultrametric property we have that

$$|\alpha_i - \alpha_j|_p \le \delta_0^{-1} Q^{-d_j} \tag{5.125}$$

for any $1 \leq i < j \leq n$. It follows that

$$0 < |D(P)|_p \leq |a_n|_p^{2n-2} \prod_{0 \leq i < j \leq n} Q^{-2d_j} \ll Q^{-2\sum_{j=2}^{n}(j-1)d_j}. \tag{5.126}$$

Setting

$$\nu = \sum_{j=1}^{n}(j-1)d_j. \tag{5.127}$$

gives that $0 < |D(P)|_p \ll Q^{-2\nu}$.

Rearranging (5.111) we get $\theta_{j-1} = d_j + \theta_j$, and then we obtain that $\theta_{j-1} = d_j + \cdots + d_n + \theta_n = d_j + \cdots + d_n$ since $\theta_n = 0$. Hence,

$$\sum_{j=1}^{n} j d_j = \sum_{j=0}^{n-1} d_{j+1} + \cdots + d_n = \sum_{j=0}^{n-1} \theta_j = n+1, \tag{5.128}$$

where we have used the fact that $\theta_n = 0$. Now it is possible to compute ν by expanding the right hand side of equation (5.127):

$$\nu = n + 1 - \sum_{j=1}^{n} d_j \,. \tag{5.129}$$

By Lemmas 5.2.1 and 5.5.4, for every $x \in G_B$ there exists an irreducible polynomial $P \in \mathbb{Z}[x]$ of degree n with one of its roots $\alpha = \alpha(P)$ satisfying

$$|x - \alpha(P)|_p \leq \delta_0^{-1} Q^{-d_1} \,. \tag{5.130}$$

Hence,

$$G_B \subset \bigcup_{P \in \mathcal{D}_{n,p,\gamma}(C_2 Q, \nu)} \bigcup_{j=1}^{n} \left\{ x \in \mathbb{Z}_p : |x - \alpha_j(P)|_p \leq \delta_0^{-1} Q^{-d_1} \right\}, \tag{5.131}$$

where $\alpha_1(P), \ldots, \alpha_n(P) \in \overline{\mathbb{Q}_p}$ are the roots of P. Therefore, since we have taken $B = \mathbb{Z}_p$, we have that

$$\frac{1}{2} = \frac{1}{2}\mu(B) \leq \#\mathcal{D}_{n,p,\gamma}(C_2 Q, \nu) \cdot n \delta_0^{-1} Q^{-d_1} \tag{5.132}$$

and so by rearranging we get

$$\#\mathcal{D}_{n,p,\gamma}(C_2 Q, \nu) \geq \frac{\delta_0}{2n} Q^{d_1}. \tag{5.133}$$

It can be further seen that the best possible lower bound is obtained by maximising the value of d_1, or by (5.129), minimizing $d_2, \ldots, d_n$. By (5.112), this can be done by letting $d_2 = d_3 = \cdots = d_n$, and, by solving (5.128) and (5.129), we obtain that

$$d_1 = n + 1 - \frac{n+2}{n}\nu \qquad \text{and} \qquad d_2 = \frac{2\nu}{n(n-1)}. \tag{5.134}$$

It is readily seen that $d_1 \geq d_2$ for $0 \leq \nu \leq n-1$. Substituting d_1 into (5.133) and rescaling the bound for the height by letting $\tilde{Q} = C_2 Q$ we complete the proof.

References

[1] D. Badziahin. “Simultaneous Diophantine approximation to points on the Veronese curve”. In: *Advances in Mathematics* 468 (2025).

[2] D. Badziahin and J. Schleischitz. *An improved bound in Wirsing’s problem*. 2019. arXiv: 1912.09013 [math.NT].

[3] V. Beresnevich, V. Bernik, and F. Goetze. “Simultaneous approximations of zero by an integral polynomial, its derivative, and small values of discriminants”. In: *Dokl. Nats. Akad. Nauk Belarusi* 54 (2010), pp. 26–28.

[4] V. Beresnevich, V. Bernik, and F. Götze. “Integral polynomials with small discriminants and resultants”. In: *Advances in Mathematics* 298 (2016), pp. 393–412.

[5] V. Beresnevich, V. Bernik, and F. Götze. “The distribution of close conjugate algebraic numbers”. In: *Compositio Mathematica* 146.5 (2010), pp. 1165–1179.

[6] V. Beresnevich and B. Dixon. *p-adic root separation and the discriminant of integer polynomials*. 2025. arXiv: 2504.03851 [math.NT].

[7] V. Bernik, N. Budarina, and H. O’Donnell. “Discriminants of polynomials in the Archimedean and non-Archimedean metrics”. In: *Acta Mathematica Hungarica* 154 (2018), pp. 265–278.

[8] V. Bernik, N. Budarina, and H. O’Donnell. “How do discriminants of integer polynomials depend on the mutual arrangement of roots?” In: *Chebyshev collection* 16.1 (2015), pp. 153–162.

[9] V. Bernik, O. Kukso, and F. GöTze. “Lower bounds for the number of integral polynomials with given order of discriminants”. In: *Acta Arithmetica* 133.4 (2008), pp. 375–390.

[10] V. I. Bernik, D. V. Vasilyev, N. I. Kalosha, and Z. I. Panteleeva. "Metric theory of Diophantine approximation and asymptotic estimates for the number of polynomials with given discriminants divisible by a large power of a prime number". In: *Doklady of the National Academy of Sciences of Belarus* 67.4 (2023), pp. 271–278.

[11] V. Bernik, N. Budarina, and F. Goetze. "Exact upper bounds for the number of the polynomials with given discriminants". In: *Lithuanian Mathematical Journal* 57.3 (2017), pp. 283–293.

[12] V. Bernik, F. Goetze, and O. Kukso. "On the divisibility of the discriminant of an integral polynomial by prime powers". In: *Lithuanian Mathematical Journal* 48 (2008), pp. 380–396.

[13] V. Bernik, D. Kleinbock, and G. A. Margulis. "Khintchine-type theorems on manifolds: the convergence case for standard and multiplicative versions". In: *International Mathematics Research Notices* 2001.9 (2001), pp. 453–486.

[14] N. V. Budarina. "Exact bounds for the special class of integer polynomials with given discriminant". In: *Chebyshevskii Sbornik* 20.2 (2019), pp. 39–46.

[15] N. Budarina, V. Bernik, and H. O'Donnell. "New estimates for the number of integer polynomials with given discriminants". In: *Lithuanian Mathematical Journal* 60 (2020), pp. 1–8.

[16] Y. Bugeaud. *Approximation by algebraic numbers*. Vol. 160. Cambridge University Press, 2004.

[17] Y. Bugeaud and A. Dujella. "Root separation for irreducible integer polynomials". In: *Bulletin of the London Mathematical Society* 43.6 (2011), pp. 1239–1244.

[18] Y. Bugeaud and A. Dujella. "Root separation for reducible integer polynomials". eng. In: *Acta Arithmetica* 162.4 (2014), pp. 393–403.

[19] Y. Bugeaud and M. Mignotte. "POLYNOMIAL ROOT SEPARATION". In: *International Journal of Number Theory* 06 (2011).

[20] Y. Bugeaud and T. Pejković. "Quadratic approximation in $\mathbb{Q}_p$". In: *International Journal of Number Theory* 11.01 (2015), pp. 193–209.

[21] J. W. S. Cassels. *Local fields*. Vol. 3. Cambridge University Press Cambridge, 1986.

[22] K. Conrad. “Hensel’s lemma”. In: *Unpublished notes* (2015).

[23] H. Davenport and W. Schmidt. “Approximation to real numbers by quadratic irrationals”. In: *Acta Arithmetica* 13.2 (1967), pp. 169–176.

[24] A. Dubickas. “Root separation for polynomials with reducible derivative”. In: *Mathematica slovaca* 70(5) (2020), pp. 1079–1086.

[25] A. Dujella and T. Pejković. “Root separation for reducible monic polynomials of odd degree”. In: *Mathematika* 21 (2017), pp. 21–27.

[26] J.-H. Evertse. *Distances between the conjugates of an algebraic number*. 2004. arXiv: math/0408304 [math.NT].

[27] F. Götze, D. Kaliada, and M. Korolev. *On the number of integral quadratic polynomials with bounded heights and discriminants*. 2013. arXiv: 1308.2091 [math.NT].

[28] F. Q. Gouvêa. *P-adic numbers : an introduction / Fernando Q. Gouvêa.* eng. Universitext. Berlin ; New York: Springer-Verlag, 1993.

[29] K. Hensel. “Über eine neue Begründung der Theorie der algebraischen Zahlen”. In: *Jahresbericht der Deutschen Mathematiker-Vereinigung* 6 (1897), pp. 83–88.

[30] K. Hensel. *Theorie der algebraischen Zahlen*. Vol. 1. BG Teubner, 1908.

[31] D. Kaliada, F. Götze, and O. Kukso. “The asymptotic number of integral cubic polynomials with bounded heights and discriminants”. In: *Lithuanian Mathematical Journal* 54.2 (2014), pp. 150–165.

[32] S. Kieffer. “Computability in principle and in practice in algebraic number theory: Hensel to zassenhaus”. PhD thesis. Simon Fraser University, 2012.

[33] D. Y. Kleinbock and G. A. Margulis. “Flows on homogeneous spaces and Diophantine approximation on manifolds”. In: *The Annals of Mathematics* 148.1 (1998), p. 339.

[34] D. Kleinbock. “Quantitative nondivergence and its Diophantine applications”. In: *Homogeneous flows, moduli spaces and arithmetic* 10 (2010), pp. 131–153.

[35] D. Kleinbock and G. Tomanov. *Flows on S-arithmetic homogeneous spaces and applications to metric Diophantine approximation*. 2005.

[36] D. Y. Kleinbock and G. A. Margulis. “Flows on homogeneous spaces and Diophantine approximation on manifolds”. In: *Annals of mathematics* (1998), pp. 339–360.

[37] N. Koblitz. *P-adic numbers, p-adic analysis, and zeta-functions*. Graduate texts in mathematics ; 58. New York: Springer-Verlag, 1977.

[38] D. V. Koleda. "On the distribution of polynomial discriminants: totally real case". In: *Lithuanian Mathematical Journal* 59.1 (2019), pp. 67–80.

[39] K. Mahler. "An inequality for the discriminant of a polynomial." In: *Michigan Mathematical Journal* 11.3 (1964), pp. 257–262.

[40] J. Morrison. "Approximation of p-adic Numbers by Algebraic Numbers of Bounded Degree". In: *Journal of Number Theory* (1978).

[41] T. Pejković. "P-adic root separation for quadratic and cubic polynomials". In: *Rad HAZU, Matematičke znanosti* (2016), pp. 9–18.

[42] A. Poëls. *On approximation to a real number by algebraic numbers of bounded degree*. 2024. arXiv: 2405.08341 [math.NT].

[43] W. M. Schmidt. *Diophantine Approximation*. Springer, 1980.

[44] A. Schönhage. "Polynomial root separation examples". In: *Journal of Symbolic Computation* 41.10 (2006), pp. 1080–1090.

[45] G. Tomanov. "Orbits on Homogeneous Spaces of Arithmetic Origin and Approximations". In: *Analysis on Homogeneous Spaces and Representation Theory of Lie Groups* (2000).

[46] P. Ullrich. "The genesis of Hensel's p-adic numbers". In: *Charlemagne and his heritage: 1200 years of civilization and science in Europe. Volume 2: Mathematical Arts*. Brepols Publishers, 1998, pp. 195–205.

[47] E. Wirsing. "Approximation mit algebraischen Zahlen beschränkten Grades." In: *Journal für die reine und angewandte Mathematik* (1961).

[48] J. Yuan, N. Budarina, and D. Dickinson. "On the number of polynomials with small discriminants in the Euclidean and p-adic metrics". In: *Acta Mathematica Sinica, English Series* 28 (2012).