DIOPHANTINE APPROXIMATIONS

Gaurish Korpal[1]
gaurish.korpal@niser.ac.in

Winter Internship Project Report

[1] 2^{nd} year Int. MSc. Student, National Institute of Science Education and Research, Jatni (Bhubaneswar, Odisha)

Certificate

Certified that the winter internship project report "Diophantine Approximations" is the work of "Gaurish Korpal", 2^{nd} Year Int. MSc. student at National Institute of Science Education and Research, Jatni (Bhubaneswar, Odisha) carried out under my supervision during December 13, 2015 to January 8, 2016.

Place: Allahabad
Date: January 8, 2016

Prof. Ravindranathan Thangadurai
Supervisor
Associate Professor - G,
Harish-Chandra Research Institute,
Jhusi, Allahabad 211 019

Abstract

Diophantine approximation has quite old history, it includes, for instance, early estimates for π, computations related to astronomical studies, the theory of continued fraction expansion. This term was coined in honor of *Diophantus of Alexandria* (3^{rd} century), who was the author of a series of books called *Arithmetica*, which lead to tremendous advances in number theory. A basic objective of this subject is to investigate the rational approximations to a single real number. In this report we will study the elementary results in this subject.

Contents

Introduction

Let $f(x_1, \ldots, x_n)$ be a function of n variables, which is always positive or zero. As stated by Davenport[1], the general problem of Diophantine approximation is of a mixed arithmetic and analytic nature, since the variables are integers and the coefficients of f are supposed to be arbitrary real numbers.

One main goal of the theory of Diophantine approximation is to compare, on the one hand, the distance between a given real number α and a rational number a/b, with, on the other hand, the denominator b of the approximant. An approximation is considered as sharp if $|\alpha - a/b|$ is small compared to b.

Several questions arise when α is algebraic, one may consider either asymptotic or else uniform approximation. After rational approximation to a single real number, one may investigate, the algebraic approximation properties of real or complex numbers, replacing the set of rational numbers by the set of real or complex algebraic numbers.[11]

Suppose[2] we wish to prove that *the equation* $x^2 - 2y^2 = \pm 1$ *has an infinitely many integral solutions.* We can do so by proving that the inequality $|x^2 - 2y^2| < 2$ has infinitely many integral solutions; and on factorising this we find that it is sufficient to prove that there are infinitely many fractions x/y for which

$$\left| \frac{x}{y} - \sqrt{2} \right| < \frac{c}{y^2}$$

for some constant c less than $1/\sqrt{2}$. Thus a problem of a purely arithmetical character is reduced to a problem of Diophantine approximation.

First and second chapter are devoted to those theorems, whose proofs are based on simple continued fractions and elementary concepts of geometry of numbers respectively. But, major part of this report is devoted to proof of Roth's Theorem. In his paper[7], Roth wrote:

"As regards the substance of the present paper, it will be appreciated that many of the ideas and methods are not new. The novel part of the proof is that culminating in Lemma 7, and even here we make much use of ideas that have occurred before in the literature of the subject."

[1] Davenport, H., 'The Geometry of Numbers', The Mathematical Gazette, Vol. 31, No. 296 (Oct., 1947), 206-210.

[2] In my past report on Diophantine equations, I didn't discuss that Diophantine equations can often be best approached from the corresponding inequalities.

Chapter 1

Rational Approximation to Irrational Number

Since the rational numbers are dense on the real line, we surely can make the difference between α and its rational approximation $\frac{a}{b}$ as small as we wish. But, as we try to make $\frac{a}{b}$ closer and closer to α, we may have to use larger and larger a and b. So, in this chapter we will see that how well we can approximate α by rational numbers with not too large denominators. Using simple continued fractions we can give "best"[1] rational approximation to the irrational number.

1.1 Simple Continued Fractions

Let α be an irrational number, then:

$$\alpha = \lfloor \alpha \rfloor + \{\alpha\}$$

where $\{\alpha\} \in (0, 1)$, thus:

$$\alpha = a_0 + \frac{1}{\alpha_1}, \qquad \text{where } a_0 = \lfloor \alpha \rfloor \text{ and } \alpha_1 \notin \mathbb{Z}$$

$$\Rightarrow \alpha = a_0 + \frac{1}{a_1 + \frac{1}{\alpha_2}}, \qquad \text{where } a_1 = \lfloor \alpha_1 \rfloor \text{ and } \alpha_2 \notin \mathbb{Z}$$

$$\vdots$$

The above process will go on. We can prove it by contradiction, since if it terminates, α will be a rational number (Euclid's Division Algorithm). Hence we will get *simple continued fraction* expansion of α as:

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}} = [a_0; a_1, a_2, \ldots]$$

[1] see Corollary 1.2.1

where a_i for $i \geq 1$ is a positive integer and a_n is called n^{th} *partial quotient*. Note that,

$$\frac{1}{\alpha} = [0; a_0, a_1, \ldots]$$

Also, n^{th} *complete quotient*, α_n, is:

$$\alpha_n = [a_n; a_{n+1}, a_{n+2}, \ldots] = \frac{1}{\alpha_{n-1} - a_{n-1}}$$

Hence, if $\alpha_n = \alpha_{n+k}$ then $\alpha_n = \alpha_{n+k} = \alpha_{n+2k} = \cdots$ where $k \in \mathbb{N}$.
We define *convergent*, δ_n as:

$$\delta_n = [a_0; a_1, a_2, \ldots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}} = \frac{p_n}{q_n}$$

thus, $\delta_0 = a_0$, $\delta_1 = \frac{a_1 a_0 + 1}{a_1} = \frac{p_1}{q_1}$, so on. But, calculation of δ_n is tedious in this way, so we rather use the following recursive definition to calculate δ_n, for $n \geq 2$,

$$\begin{cases} p_n = p_{n-1}a_n + p_{n-2} & \text{where } p_0 = a_0 \text{ and } p_1 = a_0 a_1 + 1 \\ q_n = q_{n-1}a_n + q_{n-2} & \text{where } q_0 = 1 \text{ and } q_1 = a_1 \end{cases} \tag{1.1}$$

The above result can be proved using induction, note that to go from $\frac{p_k}{q_k}$ to $\frac{p_{k+1}}{q_{k+1}}$ it is necessary to replace a_k by $a_k + \frac{1}{a_{k+1}}$. Thus for $n \geq 2$,

$$\delta_n = \frac{p_n}{q_n} = \frac{p_{n-1}a_n + p_{n-2}}{q_{n-1}a_n + q_{n-2}} \tag{1.2}$$

Also, since:

$$\alpha = [a_0; a_1, \ldots, a_{n-1}, \alpha_n] = [a_0; a_1, \ldots, a_{n-1} + \frac{1}{\alpha_n}]$$

using this in (1.2) and simplifying using (1.1), we get::

$$\alpha = \frac{p_{n-2}\left(a_{n-1} + \frac{1}{\alpha_n}\right) + p_{n-3}}{q_{n-2}\left(a_{n-1} + \frac{1}{\alpha_n}\right) + q_{n-3}} = \frac{p_{n-1}\alpha_n + p_{n-2}}{q_{n-1}\alpha_n + q_{n-2}} \tag{1.3}$$

Also, (p_n) and (q_n) are increasing sequences. Moreover, we can prove by induction that for $n \geq 0$,

$$p_n q_{n+1} - p_{n+1} q_n = (-1)^n \tag{1.4}$$

Thus, using (1.2) along with (1.4), we get *increment of* n^{th} *convergent*, Δ_n, is:

$$\Delta_n = \delta_{n+1} - \delta_n = \frac{(-1)^n}{q_n q_{n+1}} \tag{1.5}$$

Hence, we observe that $|\Delta_n| > |\Delta_{n+1}|$ and exact value of α lies between two neighbouring convergents.

I will end this section with following observations:

$$\beta_n = \frac{p_n}{p_{n-1}} = \begin{cases} [a_n; a_{n-1}, \ldots, a_0] & \text{if } a_0 \neq 0 \\ [a_n; a_{n-1}, \ldots, a_2] & \text{if } a_0 = 0 \end{cases}$$

and

$$\gamma_n = \frac{q_n}{q_{n-1}} = [a_n; a_{n-1}, \ldots, a_2, a_1] \tag{1.6}$$

1.2 Elementary Approximation Theorems

Lemma 1.2.1. *For any $n \geq 0$,*

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n+1}} \qquad \textit{and} \qquad |\alpha q_n - p_n| < \frac{1}{q_{n+1}}$$

Proof. The second inequality will follow from the first by multiplication by q_n. By, (1.3) and (1.4):

$$\left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{q_n(\alpha_{n+1}q_n + q_{n-1})}$$

But, $\alpha_{n+1} > a_{n+1}$, so:

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n(a_{n+1}q_n + q_{n-1})} = \frac{1}{q_n q_{n+1}}$$

□

Theorem 1.2.1 (Dirichlet[2], 1842)**.** *Given any irrational number α, there are infinitely many distinct rational numbers $\frac{a}{b}$ with $b \geq 1$ such that*

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b^2}$$

Proof. From Lemma 1.2.1 and $q_n < q_{n+1}$, we get:

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n+1}} < \frac{1}{q_n^2}$$

[2]for Dirichlet's proof using *pigeonhole principle* see Borwein, J., van der Poorten, A. J., Shallit, J. and Zudilin, W., Neverending Fractions. An Introduction to Continued Fractions, Australian Mathematical Society Lecture Series 23 (Cambridge University Press, Cambridge, 2014) pp. 14-17. The method is of great importance because it can be extended to multi-dimensional problems, that of the simultaneous approximation of k numbers, see Theorem 2.1.1

Hence, there are infinitely many distinct rational numbers $\frac{a}{b}$ with $b \geq 1$ such that:

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b^2}$$

□

Remark. From Dirichlet's proof of this theorem we can conclude that: *if* $\alpha \in \mathbb{R}, k \in \mathbb{Z}$, *there exist integers* a, b, *where* $b \in \{1, 2, 3, \ldots, k\}$, *such that* $|\alpha b - a| < 1/k$. Generalisation of this statement is Lemma 2.1.1.

Lemma 1.2.2. *If* $\frac{a}{b}$ *is a rational number with positive denominator such that*

$$\left|\alpha - \frac{a}{b}\right| < \left|\alpha - \frac{p_n}{q_n}\right|$$

for some $n \geq 1$, *then* $b \geq q_n$. *Moreover, if*

$$|\alpha b - a| < |\alpha q_n - p_n|$$

for some $n \geq 0$, *then* $b \geq q_{n+1}$.

Proof. Observe that the second part of the lemma implies the first. Suppose that the first part is false so that an a/b with

$$\left|\alpha - \frac{a}{b}\right| < \left|\alpha - \frac{p_n}{q_n}\right| \qquad \text{and} \qquad b \leq q_n$$

The product of these inequalities give:

$$|\alpha b - a| < |\alpha q_n - p_n|$$

But, the second part of lemma says that this implies $b \geq q_{n+1}$, so we have a contradiction, since $q_n < q_{n+1}$ for $n \geq 1$.

We will use proof by contradiction for second part. Suppose,

$$|\alpha b - a| < |\alpha q_n - p_n| \qquad \text{and} \qquad b < q_{n+1} \tag{1.7}$$

Now consider the linear equations in x and y:

$$\begin{cases} p_n x + p_{n+1} y = a \\ q_n x + q_{n+1} y = b \end{cases}$$

These equations have an integral solution (x, y), since determinant of coefficients is ± 1 (by (1.4)).

Observe that neither x nor y is zero, since if any one of them become zero, we get a contradiction to one of the inequalities in (1.7).

Moreover, x and y are of opposite signs, since $b < q_{n+1}$. Also, $\alpha q_n - p_n$ and $\alpha q_{n+1} - p_{n+1}$ have opposite signs.. Now,

$$\alpha b - a = x(\alpha q_n - p_n) + y(\alpha q_{n+1} - p_{n+1})$$

Since the two terms on the right have same sign:

$$|\alpha b-a| = |x(\alpha q_n-p_n)+y(\alpha q_{n+1}-p_{n+1})| = |x(\alpha q_n-p_n)|+|y(\alpha q_{n+1}-p_{n+1})|$$

$$\Rightarrow |\alpha b - a| > |x(\alpha q_n - p_n)| = |x||(\alpha q_n - p_n)|$$

$$\Rightarrow |\alpha b - a| \geq |\alpha q_n - p_n|$$

This is a contradiction to (1.7). Thus proving our lemma. □

Corollary 1.2.1. *The convergent $\delta_n = \frac{p_n}{q_n}$ is the best approximation of α of all the rational fractions with denominator less than or equal to q_n.*

Theorem 1.2.2 (Legendre)**.** *Let a and b be coprime integers, $b > 0$, and let*

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{2b^2}$$

Then $\frac{a}{b}$ is a convergent of α.

Proof. We are given that:

$$|\alpha b - a| < \frac{1}{2b} \tag{1.8}$$

Let the convergents of the simple continued fraction expansion of α be p_n/q_n, and suppose a/b is not a convergent. The inequality $q_n \leq b \leq q_{n+1}$ determine the integer n. For this n, the inequality $|\alpha b - a| < |\alpha q_n - p_n|$ is impossible due to Lemma 1.2.2.

Thus from (1.8), we have:

$$|\alpha q_n - p_n| \leq |\alpha b - a| < \frac{1}{2b}$$

$$\Rightarrow \left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{2bq_n} \tag{1.9}$$

Using the facts that $a/b \neq p_n/q_n$ and that $bp_n - aq_n$ is an integer, we get:

$$\frac{1}{bq_n} \leq \frac{|bp_n - aq_n|}{bq_n} = \left|\frac{p_n}{q_n} - \frac{a}{b}\right| = \left|\left(\frac{p_n}{q_n} - \alpha\right) + \left(\alpha - \frac{a}{b}\right)\right|$$

By triangle inequality,

$$\Rightarrow \frac{1}{bq_n} \leq \left|\alpha - \frac{p_n}{q_n}\right| + \left|\alpha - \frac{a}{b}\right|$$

From (1.9) and given conditions, we get:

$$\Rightarrow \frac{1}{bq_n} < \frac{1}{2bq_n} + \frac{1}{2b^2}$$

This implies that, $b < q_n$, which is a contradiction. □

Lemma 1.2.3. *If x is a real number, $x > 1$, and $x + \frac{1}{x} < \sqrt{5}$, then*

$$x < \frac{\sqrt{5}+1}{2} \qquad \text{and} \qquad \frac{1}{x} > \frac{\sqrt{5}-1}{2}$$

Remark. If the partial quotient, a_n, behaves regularly, and doesn't become too large, then α may reasonably be regarded as a 'simple number'; and in this case the rational approximation of α can't be good. Hence, from the point if view of rational approximation, the simplest numbers are worst[3]. Thus, the simplest of all irrationals, from this point of view is, $\alpha = [0; 1, 1, 1, \ldots] = \frac{\sqrt{5}-1}{2}$, in which every a_n has smallest possible value.[4]

Theorem 1.2.3 (Hurwitz, 1891)**.** *Given any irrational number α, there exist infinitely many different rational numbers $\frac{a}{b}$ such that:*

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{\sqrt{5}b^2}$$

Moreover, above statement doesn't hold if $\sqrt{5}$ is replaced by any larger value.

Proof. We will show that, of every three consecutive convergents of simple continued fraction expansion of α at least one satisfies the given inequality.

From, (1.6), we note that $\gamma_n = q_n/q_{n-1}$. We first claim that

$$\gamma_m + \frac{1}{\gamma_m} < \sqrt{5}$$

if given inequality is false for both $a/b = p_{m-1}/q_{m-1}$ and $a/b = p_m/q_m$.

Suppose, given inequality is false, i.e. $|\alpha - a/b| \geq 1/\sqrt{5}b^2$ for these two values of a/b. We have

$$\left|\alpha - \frac{p_{m-1}}{q_{m-1}}\right| + \left|\alpha - \frac{p_m}{q_m}\right| \geq \frac{1}{\sqrt{5}q_{m-1}^2} + \frac{1}{\sqrt{5}q_m^2} \tag{1.10}$$

But, we observed from (1.5) that, α lies between p_{m-1}/q_{m-1} and p_m/q_m; thus $\alpha - p_{m-1}/q_{m-1}$ and $\alpha - p_m/q_m$ are of opposite sign. Hence using (1.5) we get:

$$\left|\alpha - \frac{p_{m-1}}{q_{m-1}}\right| + \left|\alpha - \frac{p_m}{q_m}\right| = \left|\frac{p_m}{q_m} - \frac{p_{m-1}}{q_{m-1}}\right| = |\Delta_{m-1}| = \frac{1}{q_{m-1}q_m} \tag{1.11}$$

Combining (1.10) and (1.11), we get:

$$\frac{q_m}{q_{m-1}} + \frac{q_{m-1}}{q_m} \leq \sqrt{5}$$

[3] refer section 11.8 of [2]

[4] note that, golden ratio $= \varphi = [1; 1, 1, \ldots] = \frac{2}{\sqrt{5}-1} = \frac{\sqrt{5}+1}{2}$

Since, the left hand side is rational, we actually have a strict inequality, and thus proving our first claim.

Now, suppose that given inequality is false for $a/b = p_r/q_r, r = n-1, n, n+1$, i.e. we have $|\alpha - a/b| \geq 1/\sqrt{5}b^2$ for these three values of a/b. Then we have $\gamma_m + 1/\gamma_m < \sqrt{5}$ for $m = n, n+1$.
By Lemma 1.2.3, we see that:

$$\frac{1}{\gamma_n} > \frac{\sqrt{5}-1}{2} \qquad \text{and} \qquad \gamma_{n+1} < \frac{\sqrt{5}+1}{2}$$

and, by (1.6), we have: $\gamma_{n+1} = a_{n+1} + \frac{1}{\gamma_n}$. This gives us:

$$\begin{aligned} \frac{\sqrt{5}+1}{2} > \gamma_{n+1} &= a_{n+1} + \frac{1}{\gamma_n} \\ \Rightarrow \frac{\sqrt{5}+1}{2} &> a_{n+1} + \frac{\sqrt{5}-1}{2} \\ \Rightarrow \frac{\sqrt{5}+1}{2} &\geq 1 + \frac{\sqrt{5}-1}{2} = \frac{\sqrt{5}+1}{2} \end{aligned}$$

and this is a contradiction. Hence proving first part of the theorem.

Now, second part of the theorem asserts that: *The constant $\sqrt{5}$ in above inequality is best possible.*
It is enough to show that, if $A > \sqrt{5}$ and $\alpha = [0; 1, 1, \ldots] = \frac{\sqrt{5}-1}{2}$ then the inequality

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{Ab^2}$$

has only a finite number of solutions.

Suppose the contrary. Then there are infinitely many a and b such that

$$\alpha = \frac{a}{b} + \frac{c}{b^2} \qquad \text{where} \qquad |c| < \frac{1}{A} < \frac{1}{\sqrt{5}}$$

Hence,

$$\begin{aligned} \frac{c}{b} = \alpha b - a \quad &\Rightarrow \frac{c}{b} = \frac{(\sqrt{5}-1)b}{2} - a \\ \Rightarrow \left(\frac{c}{b} - \frac{b\sqrt{5}}{2}\right)^2 &= \left(\frac{-b}{2} - a\right)^2 \\ \Rightarrow \frac{c^2}{b^2} - c\sqrt{5} &= a^2 + ab - b^2 \end{aligned}$$

The left hand side is numerically less than 1 when b is large, while the right hand side is an integer. Hence

$$a^2 + ab - b^2 = 0 \quad \Rightarrow (2a+b)^2 = 5b^2$$

which is impossible. Thus proving second part of the theorem. □

All the rational approximation theorems discussed above can also be proved using a sequence discovered by French mathematician Charles Haros in 1806, which Cauchy called Farey Sequence (named after John Farey).The sequence of all reduced fractions with denominators not exceeding n, listed in order of their size, is called *Farey sequence of order* n. For proofs using this method refer section 6.2 of [5].

1.3 Badly Approximable Irrationals

An irrational number α is *badly approximable* if there is a constant , $c(\alpha) > 0$ (which depends only on α) such that

$$\left|\alpha - \frac{a}{b}\right| > \frac{c(\alpha)}{b^2} \qquad \text{and} \quad 0 < c(\alpha) < \frac{1}{\sqrt{5}} \quad \text{(from Theorem 1.2.3)}$$

for every rational $\frac{a}{b}$. For example, since quadratic surds have periodic continued fractions, they are badly approximable.

Theorem 1.3.1. *Given irrational number α is badly approximable if and only if the partial quotients in its continued fraction expansion are bounded.*

Proof. To study the inequality,

$$\left|\alpha - \frac{a}{b}\right| < \frac{c(\alpha)}{b^2}$$

where $0 < c(\alpha) < \frac{1}{\sqrt{5}} < \frac{1}{2}$, we may restrict ourselves to convergents by Theorem 1.2.2. As seen in Lemma 1.2.1 we have:

$$\left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{q_n(\alpha_{n+1}q_n + q_{n-1})}$$

now using (1.6), we get:

$$\left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{q_n^2(\alpha_{n+1} + \frac{1}{\gamma_n})} = \frac{1}{q_n^2\left([a_{n+1}; a_{n+2}, \ldots] + \frac{1}{[a_n; a_{n-1}, a_{n-2}, \ldots, a_1]}\right)}$$

$$\Rightarrow \left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{q_n^2\Big(a_{n+1} + [0; a_{n+2}, a_{n+3}, \ldots] + [0; a_n, a_{n-1}, \ldots, a_1]\Big)}$$

Hence,

$$\frac{1}{q_n^2(a_{n+1}+2)} \leq \left|\alpha - \frac{p_n}{q_n}\right| \leq \frac{1}{q_n^2 a_{n+1}}$$

The theorem follows. □

Chapter 2

Simultaneous Approximation

In previous chapter we studied approximation to single number, now we will generalize our results for tuple of numbers.

2.1 Generalising Dirichlet's Theorem

In this section we will extend the "Dirichlet's Approximation Theorem" (Theorem 1.2.1) discussed in previous chapter to a tuple of real numbers containing irrational numbers.

Lemma 2.1.1 (Dirichlet, 1842)**.** *If α_{ij} with $1 \leq i \leq n$ and $1 \leq j \leq m$, are nm real numbers and $k > 1$ is an integer, then there exist integers $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_m$ with*

$$1 \leq \max(|b_1|, \ldots, |b_m|) < k^{\frac{n}{m}} \quad \text{and} \quad |\alpha_{i1}b_1 + \ldots + \alpha_{im}b_m - a_i| \leq \frac{1}{k}$$

where $1 \leq i \leq n$.

Proof. Consider points:

$$\Big(\{\alpha_{11}x_1 + \ldots + \alpha_{1m}x_m\}, \cdots\cdots, \{\alpha_{n1}x_1 + \ldots + \alpha_{nm}x_m\}\Big)$$

where

$$\{\alpha_{i1}x_1 + \ldots + \alpha_{im}x_m\} = \alpha_{i1}x_1 + \ldots + \alpha_{im}x_m - \lfloor \alpha_{i1}x_1 + \ldots + \alpha_{im}x_m \rfloor$$

and each x_j is an integer satisfying, $0 \leq x_j < k^{\frac{n}{m}}$ for $1 \leq j \leq m$.

There are at least k^n such points, and each of these points lie in the closed unit cube, denoted by $[0,1]^n$ or $\mathcal{I}^n$, consisting of points $(t_1, t_2, \ldots, t_n)$ with $0 \leq t_i \leq 1$ for $1 \leq i \leq n$. The point $(1, 1, \ldots, 1)$ also lies in $\mathcal{I}^n$, so together there are at least $k^n + 1$ points under consideration.

We divide $\mathcal{I}^n$ into k^n pair wise disjoint subcubes[1] of side length $1/k$. By pigeonhole principle, two of the points under consideration will be in the same subcube. These points are, say:

$$\Big(\{\alpha_{11}x_1 + \ldots + \alpha_{1m}x_m\}, \cdots\cdots, \{\alpha_{n1}x_1 + \ldots + \alpha_{nm}x_m\}\Big),$$

$$\Big(\{\alpha_{11}x'_1 + \ldots + \alpha_{1m}x'_m\}, \cdots\cdots, \{\alpha_{n1}x'_1 + \ldots + \alpha_{nm}x'_m\}\Big)$$

Let, y_i, y'_i be integers for $1 \leq i \leq n$, such that:

$$y_i = \lfloor \alpha_{i1}x_1 + \ldots + \alpha_{im}x_m \rfloor \quad \text{and} \quad y'_i = \lfloor \alpha_{i1}x'_1 + \ldots + \alpha_{im}x'_m \rfloor$$

then, we can re-write the points in consideration as:

$$\Big((\alpha_{11}x_1 + \ldots + \alpha_{1m}x_m - y_1), \cdots\cdots, (\alpha_{n1}x_1 + \ldots + \alpha_{nm}x_m - y_n)\Big),$$

$$\Big((\alpha_{11}x'_1 + \ldots + \alpha_{1m}x'_m - y'_1), \cdots\cdots, (\alpha_{n1}x'_1 + \ldots + \alpha_{nm}x'_m - y'_n)\Big)$$

Here, $(x_1, \ldots x_m) \neq (x'_1, \ldots, x'_m)$. Put, $b_j = x_j - x'_j$ for $1 \leq j \leq m$, and $a_i = y_i - y'_i$ for $1 \leq i \leq n$. Then:

$$|\alpha_{i1}b_1 + \ldots + \alpha_{im}b_m - a_i| \leq \frac{1}{k}$$

□

Theorem 2.1.1. *Let α_{ij} with $1 \leq i \leq n$ and $1 \leq j \leq m$, be nm real numbers and $k > 1$ be an integer, if for some i in $1 \leq i \leq n$, $\alpha_{i1}, \ldots, \alpha_{im}, 1$ are linearly independent over the rational numbers[2] , then there exist infinitely many coprime $(m+n)$-tuples*

$$(b_1, b_2, \ldots b_m, a_1, a_2, \ldots, a_n)$$

with

$$b = max(|b_1|, \ldots, |b_m|) > 0 \quad \textit{and} \quad |\alpha_{i1}b_1 + \ldots + \alpha_{im}b_m - a_i| \leq \frac{1}{b^{\frac{m}{n}}}$$

where $1 \leq i \leq n$.

Proof. The inequalities of Lemma 2.1.1 clearly imply this inequality.

Now, by linear independence, we always have

$$|\alpha_{i1}b_1 + \ldots + \alpha_{in}b_m - a_i| \neq 0$$

Hence for *fixed* $a_i, b_1, \ldots, b_m$,

$$|\alpha_{i1}b_1 + \ldots + \alpha_{im}b_m - a_i| \leq \frac{1}{k}$$

can hold only for $k \leq k_0$. Hence as $k \to \infty$, we obtain infinitely many solutions. □

[1] thus some of the cubes will contain some of their faces or edges and not others.

[2] we can even consider the stronger condition: $\Big((\alpha_{11}b_1 + \ldots + \alpha_{1m}b_m), \cdots\cdots, (\alpha_{n1}b_1 + \ldots + \alpha_{nm}b_m)\Big)$ is never an integer point when $(b_1, b_2, \ldots b_m)$ is a non-zero integer point.

2.2 Geometry of Numbers

Consider sets $\mathcal{S}$ that lie in real $n-$dimensional space[3], $\mathbb{R}^n$ and let, $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ denote[4] a point on $\mathbb{R}^n$. Now we want to find conditions which ensure that $\mathcal{S}$ contains a point whose coordinates are integers[5], that is, a point on $\mathbb{Z}^n$.

In this section we will restrict our attention to those sets $\mathcal{S}$ for which the volume $v(\mathcal{S})$ is defined by multiple Riemann Integrals (i.e. *Jordan Volume*)

Definition (Translation)**.** If $\mathbf{x} \in \mathbb{R}^n$ and $\mathcal{S} \subseteq \mathbb{R}^n$, then $\mathcal{S} + \mathbf{x}$ is set of all points $\mathbf{s} + \mathbf{x} = (s_1 + x_1, \cdots, s_n + x_n)$ with $\mathbf{s} \in \mathcal{S}$ and is called *translation* of $\mathcal{S}$ by $\mathbf{x}$.

Lemma 2.2.1 (Blichfeldt, 1914)**.** *Let $\mathcal{S}$ be a set in $\mathbb{R}^n$ with volume $v(\mathcal{S}) > 1$. Then there exist two distinct points $\mathbf{s}', \mathbf{s}'' \in \mathcal{S}$ such that $\mathbf{s}' - \mathbf{s}''$ has integral coordinates.*

Proof. Consider only those points $\mathbf{s} \in \mathcal{S}$ that lie in the sphere $|\mathbf{s}| \leq R$, with R suitably large, we may suppose that $\mathcal{S}$ is bounded.

For each point $\mathbf{k} = (k_1, k_2, \ldots, k_n)$ with integral coordinates, we let $\mathcal{U}(\mathbf{k})$ be unit $n-$dimensional cube consisting of those points $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ for which $k_i \leq x_i < k_i + 1$, for $1 \leq i \leq n$. That is, $\lfloor x_i \rfloor = k_i$ for $1 \leq i \leq n$. Since each point $\mathbf{x}$ in the space $\mathbb{R}^n$ lies in exactly one such cube, these cubes form a partitioning of $\mathbb{R}^n$.

For each integral point $\mathbf{k}$ we let $\mathcal{S}(\mathbf{k})$ denote the part of $\mathcal{S}$ that lies in $\mathcal{U}(\mathbf{k})$. In symbols

$$\mathcal{S}(\mathbf{k}) = \mathcal{S} \cap \mathcal{U}(\mathbf{k})$$

Thus the subsets $\mathcal{S}(\mathbf{k})$ partition $\mathcal{S}$, and consequently

$$\sum_{\mathbf{k} \in \mathbb{Z}^n} v(\mathcal{S}(\mathbf{k})) = v(\mathcal{S}) \tag{2.1}$$

Let

$$\mathcal{T}(\mathbf{k}) = -\mathbf{k} + \mathcal{S}(\mathbf{k})$$

so that $\mathcal{T}(\mathbf{k})$ is a translate of $\mathcal{S}(\mathbf{k})$ and $\mathcal{T}(\mathbf{k}) \subseteq \mathcal{U}(\mathbf{0})$.

Since translation does not disturb the volume of a set, we have

$$v(\mathcal{T}(\mathbf{k})) = v(\mathcal{S}(\mathbf{k}))$$

using this in (2.1) we get:

$$\sum_{\mathbf{k} \in \mathbb{Z}^n} v(\mathcal{T}(\mathbf{k})) = v(\mathcal{S})$$

[3] also called $n-$*dimensional Euclidean space*

[4] can also use $\underline{x}$ instead of $\mathbf{x}$ to denote tuple

[5] $\mathbf{x} = (a_1, x_2, \ldots, x_n)$ is said to an *integer point* if each x_i for $1 \leq i \leq n$ is an integer.

But, it is given that, $v(\mathcal{S}) > 1$, so:

$$\sum_{\mathbf{k}\in\mathbb{Z}^n} v(\mathcal{T}(\mathbf{k})) > 1$$

Since we assumed that $\mathcal{S}$ is a bounded set, only finitely many sets $\mathcal{T}(\mathbf{k})$ are non-empty. Moreover, the sets $\mathcal{T}(\mathbf{k})$ lie in unit cube $\mathcal{U}(\mathbf{0})$ whose volume is 1. Since the volumes of these sets sum more than 1, they all can't be disjoint. Thus there exist two distinct integral points, say $\mathbf{k}'$ and $\mathbf{k}''$ such that $\mathcal{T}(\mathbf{k}')$ and $\mathcal{T}(\mathbf{k}'')$ have a point $\mathbf{x}$ in common. Then:

$$\mathbf{x} = -\mathbf{k}' + \mathbf{s}' \qquad \text{and} \qquad \mathbf{x} = -\mathbf{k}'' + \mathbf{s}''$$

For some $\mathbf{s}' \in \mathcal{S}(\mathbf{k}')$ and $\mathbf{s}'' \in \mathcal{S}(\mathbf{k}'')$. Hence $\mathbf{s}', \mathbf{s}'' \in \mathcal{S}$, and $\mathbf{s}' - \mathbf{s}'' = \mathbf{k}' - \mathbf{k}''$ is a non-zero integral point. This completes the proof. □

Remark. For comments on this proof refer §6.4 oon pp. 322-324 of [5]. Also, this lemma can be used to extend Lemma 2.1.1 for $k > 1, k \in \mathbb{R}$ (hence removing restriction that $k \in \mathbb{Z}$), see remark on pp. 32 of [8].

Definition (Dilation)**.** If $\lambda \in \mathbb{R}$ and $\mathcal{S} \subseteq \mathbb{R}^n$, then $\lambda\mathcal{S}$ denotes the set of all points $\lambda\mathbf{s} = (\lambda s_1, \lambda s_2, \ldots, \lambda s_n)$ with $\mathbf{s} \in \mathcal{S}$and is called *dilation* of $\mathcal{S}$ by the factor λ.

Definition (Convex set)**.** A set $\mathcal{C}$ in $\mathbb{R}^n$ is said to be *convex* if for any two points $\mathbf{x}, \mathbf{y} \in \mathcal{C}$, the line segment joining them is contained in $\mathcal{C}$.

Definition (Symmetric set about $\mathbf{0}$)**.** A set $\mathcal{S}$ in $\mathbb{R}^n$ that has the property that $\mathbf{s} \in \mathcal{S}$ if and only if $-\mathbf{s} \in \mathcal{S}$ is said to be *symmetric* about $\mathbf{0}$.

Theorem 2.2.1 (Minkowski's Convex Body Theorem, 1896)**.** *Let $\mathcal{C}$ be a convex set in $\mathbb{R}^n$, symmetric about $\mathbf{0}$, bounded and with volume $v(\mathcal{C}) > 2^n$, then $\mathcal{C}$ contains a point whose coordinates are integers, not all of them* 0*.*

Proof. Let,

$$\mathcal{S} = \frac{1}{2}\mathcal{C}$$

Then,

$$v(\mathcal{S}) = \frac{1}{2^n} v(\mathcal{C}) > 1$$

By Lemma 2.2.1, there must exist points $\mathbf{s}', \mathbf{s}'' \in \mathcal{S}$ such that $\mathbf{s}' \neq \mathbf{s}''$ and $\mathbf{s}' - \mathbf{s}'' \in \mathbb{Z}^n$

Note that $2\mathbf{s}', 2\mathbf{s}'' \in \mathcal{C}$. Since, $\mathcal{C}$ is symmetric about $\mathbf{0}$, it follows that $-2\mathbf{s}'' \in \mathcal{C}$. Since $\mathcal{C}$ is convex, the line segment joining $2\mathbf{s}'$ to $-2\mathbf{s}''$ lies in $\mathcal{C}$. In particular, $\mathcal{C}$contains the midpoint of this segment, namely the point $\mathbf{s}' - \mathbf{s}''$. This is the point desired, as it has integral coordinates, not all zero. □

Remark. For another proof of this theorem by *Mordell* refer pp. 33 of [8].

2.3 Improving Approximation Constant

Suppose that $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{R}^n$, then we put:

$$[\![\mathbf{x}]\!] = \max(|x_1|, |x_2|, \ldots, |x_n|)$$

Lemma 2.3.1. *Suppose that $m \geq 1, n \geq 1$ are integers and that $t > 0$ is a real number. Let $\mathcal{K}(t)$ be the set of points $(\mathbf{x}, \mathbf{y}) = (x_1, \ldots, x_m, y_1, \ldots, y_n) \in \mathbb{R}^{m+n}$ satisfying:*

$$\frac{[\![\mathbf{x}]\!]}{t^n} + t^m [\![\mathbf{y}]\!] \leq 1$$

Then $\mathcal{K}(t)$ is compact, symmetric (with respect to $\mathbf{0}$) and convex, with volume

$$v(\mathcal{K}(t)) = 2^{m+n} \frac{m!n!}{(m+n)!}$$

Proof. Consider the transformation given by:

$$x_i \mapsto t^n x_i \qquad (1 \leq i \leq m)$$

$$y_j \mapsto \frac{y_j}{t^m} \qquad (1 \leq j \leq n)$$

This transformation is linear and has determinant $(t^n)^m (t^{-m})^n = 1$. Moreover, this transformation maps $\mathcal{K}(1)$ onto $\mathcal{K}(t)$. Since a linear transformation preserves compactness, symmetry and convexity, it is enough to that $\mathcal{K}(t)$ has these properties when $t = 1$.

Obviously, $\mathcal{K}(1) = \{(\mathbf{x}, \mathbf{y}) : [\![\mathbf{x}]\!] + [\![\mathbf{y}]\!] \leq 1\}$ is compact (i.e. closed and bounded) and symmetric (with respect to $\mathbf{0}$). To prove convexity, suppose that $(\mathbf{x}, \mathbf{y})$ and $(\mathbf{x}', \mathbf{y}')$ belong to $\mathcal{K}(1)$ and two non-negative real numbers λ, μ satisfy $\lambda + \mu = 1$. Then $\lambda(\mathbf{x}, \mathbf{y}) + \mu(\mathbf{x}', \mathbf{y}') = (\lambda\mathbf{x} + \mu\mathbf{x}', \lambda\mathbf{y} + \mu\mathbf{y}')$ belongs to $\mathcal{K}(1)$ since:

$$[\![\lambda\mathbf{x} + \mu\mathbf{x}']\!] + [\![\lambda\mathbf{y} + \mu\mathbf{y}']\!] \leq \lambda([\![\mathbf{x}]\!] + [\![\mathbf{y}]\!]) + \mu([\![\mathbf{x}']\!] + [\![\mathbf{y}']\!]) \leq \lambda + \mu = 1$$

It remains to compute $v(\mathcal{K}(t))$. Let, $\mathcal{J}(t)$ denote the set of points $(\mathbf{x}, \mathbf{y})$ in $\mathcal{K}(t)$ for which $x_i \geq 0 \quad (1 \leq i \leq m)$, $y_j \geq 0 \quad (1 \leq j \leq n)$ and $x_1 = [\![\mathbf{x}]\!]$. Thus, $\mathcal{J}(t) \subseteq \mathcal{K}(t)$, with $0 \leq x_1 \leq 1$, and for each fixed x_1

$$\begin{cases} 0 \leq x_i \leq x_1 & \text{for} \quad 2 \leq i \leq m \\ 0 \leq y_j \leq 1 - x_1 & \text{for} \quad 1 \leq j \leq n \end{cases}$$

It follows that:

$$v(\mathcal{K}(t)) = m2^{m+n} \cdot v(\mathcal{J}(t))$$

$$\Rightarrow v(\mathcal{K}(t)) = m2^{m+n} \int_0^1 x_1^{m-1} (1 - x_1)^n dx_1$$

observe that we have Beta function in right hand side, thus

$$\Rightarrow v(\mathcal{K}(t)) = m2^{m+n}B(m, n+1)$$

$$\Rightarrow v(\mathcal{K}(t)) = m2^{m+n}\frac{\Gamma(m)\Gamma(n+1)}{\Gamma(m+n+1)}$$

Since, $m, n \in \mathbb{Z}$ we get:

$$\Rightarrow v(\mathcal{K}(t)) = m2^{m+n}\frac{(m-1)!n!}{(m+n)!} = 2^{m+n}\frac{m!n!}{(m+n)!}$$

□

Theorem 2.3.1. *Consider linear forms*[6]

$$L_i(\mathbf{x}) = \alpha_{i1}x_1 + \ldots + \alpha_{im}x_m \qquad (1 \leq i \leq n)$$

where $\mathbf{x} = (x_1, \ldots, x_m)$. *Put*

$$\mathcal{L}(\mathbf{x}) = \Big(L_1(\mathbf{x}), L_2(\mathbf{x}), \ldots, L_n(\mathbf{x})\Big)$$

Then there is an integer point $(\mathbf{x}, \mathbf{y}) = (x_1, x_2, \ldots, x_m, y_1, y_2, \ldots, y_n) \in \mathbb{R}^{m+n}$ *with* $\mathbf{x} \neq 0$ *such that*

$$[\![\mathcal{L}(\mathbf{x}) - \mathbf{y}]\!]^n < c(m, n)\frac{1}{[\![\mathbf{x}]\!]^m}$$

where,

$$c(m, n) = \binom{m+n}{m}\left(\frac{m}{m+n}\right)^m\left(\frac{n}{m+n}\right)^n = \frac{m^m n^n}{(m+n)^{m+n}} \cdot \frac{(m+n)!}{m!n!} < 1$$

Furthermore, suppose that whenever $\mathbf{x} \neq \mathbf{0}$ *is an integer point in* $\mathbb{R}^m$ *then* $\mathcal{L}(\mathbf{x})$ *is not an integer point in* $\mathbb{R}^n$. *Then there exist infinitely many integer points* $(\mathbf{x}, \mathbf{y})$ *with* $\mathbf{x} \neq 0$ *and with coprime components satisfying the above inequality.*

Proof. As in Lemma 2.3.1, we have a set $\mathcal{K}(t)$ and let $\overset{\bullet}{\mathcal{K}}(t)$ be the set of points $(\mathbf{x}, \mathbf{y}) = (x_1, \ldots, x_m, y_1, \ldots, y_n) \in \mathbb{R}^{m+n}$ satisfying

$$\frac{[\![\mathbf{x}]\!]}{t^n} + t^m[\![\mathcal{L}(\mathbf{x}) - \mathbf{y}]\!] \leq C \qquad \text{where} \quad C = 2 \cdot \Big(v(\mathcal{K}(t))\Big)^{-1/(m+n)} \tag{2.2}$$

The linear transformation defined by:

$$x_i \mapsto Cx_i \qquad (1 \leq i \leq m)$$

[6]Given a vector, $\mathbf{x}$, we construct a scalar function $L_i(\mathbf{x})$, such that it satisfies that vector action, i.e. $L_i(\mathbf{x}+\mathbf{y}) = L_i(\mathbf{x}) + L_i(\mathbf{y})$, and $L_i(\lambda\mathbf{x}) = \lambda L_i(\mathbf{x})$, where λ is a scalar. Since, L_i is a scalar, it is a valid functional. Now, writing L_i when all but one of the x_k is zero for $1 \leq k \leq m$ and taking sum of them, we will get value of original vector.

$$y_j \mapsto C \cdot (L_j(\mathbf{x}) - y_i) \qquad (1 \leq j \leq n)$$

maps $\mathcal{K}(t)$ onto $\overset{\bullet}{\mathcal{K}}(t)$ and has determinant $(-1)^n C^{m+n}$, so that

$$v(\overset{\bullet}{\mathcal{K}}(t)) = C^{m+n} \cdot v(\mathcal{K}(t)) = 2^{m+n}$$

Since, compactness, symmetry and convexity are preserved under linear transformations, $\overset{\bullet}{\mathcal{K}}(t)$ has these three properties in view of Lemma 2.3.1. By, Theorem 2.2.1, it follows that $\overset{\bullet}{\mathcal{K}}(t)$ contains an integer point $(\mathbf{x}, \mathbf{y}) \neq (\mathbf{0}, \mathbf{0})$.

For a given integer point $(\mathbf{x}, \mathbf{y})$, equality in (2.2) can hold at most finitely many values of t. Since the number of integer points in $\mathbb{R}^{m+n}$ is countable, it follows that the strict inequality in (2.2) will hold for all except countably many t. In the remainder of the proof, we consider only those t which satisfy strict inequality in (2.2).

As per Arithmetic Mean-Geometric Mean Inequality, if $z_1, z_2, \ldots, z_\ell$ are ℓ non-negative numbers, then

$$(z_1 z_2 \cdots, z_\ell)^{1/\ell} \leq \frac{z_1 + z_2 + \cdots + z_\ell}{\ell}$$

We apply this with

$$\begin{cases} \ell = m + n \\ z_1 = z_2 = \ldots = z_m = \dfrac{[\![\mathbf{x}]\!]}{mt^n} \\ z_{m+1} = z_{m+2} = \ldots = z_{m+n} = \dfrac{t^m [\![\mathcal{L}(\mathbf{x}) - \mathbf{y}]\!]}{n} \end{cases}$$

to obtain,

$$\left(\frac{[\![\mathbf{x}]\!]}{mt^n}\right)^m \cdot \left(\frac{t^m [\![\mathcal{L}(\mathbf{x}) - \mathbf{y}]\!]}{n}\right)^n \leq \left(\frac{t^{-n}[\![\mathbf{x}]\!] + t^m [\![\mathcal{L}(\mathbf{x}) - \mathbf{y}]\!]}{\ell}\right)^\ell$$

Since we have considered only those values of t for which there is strict inequality in (2.2), we get:

$$\left(\frac{[\![\mathbf{x}]\!]}{mt^n}\right)^m \cdot \left(\frac{t^m [\![\mathcal{L}(\mathbf{x}) - \mathbf{y}]\!]}{n}\right)^n < \left(\frac{C}{\ell}\right)^\ell$$

Which yields,

$$[\![\mathbf{x}]\!]^m \cdot [\![\mathcal{L}(\mathbf{x}) - \mathbf{y}]\!]^n < \frac{m^m n^n}{(m+n)^{m+n}} C^{m+n} = \frac{m^m n^n}{(m+n)^{m+n}} 2^{m+n} \Big(v(\mathcal{K}(t))\Big)^{-1}$$

From Lemma 2.3.1, we substitute value of $v(\mathcal{K}(t))$ to get:

$$[\![\mathbf{x}]\!]^m \cdot [\![\mathcal{L}(\mathbf{x}) - \mathbf{y}]\!]^n < \frac{m^m n^n}{(m+n)^{m+n}} \frac{m!n!}{(m+n)!} = c(m, n)$$

This inequality is equivalent to the one given in statement of theorem, provided $[\![\mathbf{x}]\!] \neq 0$.

If we choose t to satisfy strict inequality in (2.2) and $t \geq C^{1/m}$, then $[\![\mathbf{x}]\!] \neq 0$, since otherwise, (2.2) implies that, $[\![\mathcal{L}(\mathbf{x}) - \mathbf{y}]\!] = [\![\mathbf{y}]\!] < Ct^{-m} \leq 1$ leading to $\mathbf{y} = \mathbf{0}$, a contradiction. This establishes first assertion of the theorem.

Now suppose that, whenever $\mathbf{x} \neq 0$ is an integer point in $\mathbb{R}^m$, $\mathcal{L}(\mathbf{x})$ is not an integer point in $\mathbb{R}^n$. Further suppose that t satisfies the strict inequality in (2.2) and $t \geq C^{1/m}$. Since, $[\![\mathbf{x}]\!] \neq 0$ by preceding paragraph, hence $L \neq 0$.

It follows that for fixed $(\mathbf{x}, \mathbf{y})$ the strict inequality in (2.2) can hold only for $t \leq t_0$. Hence as $t \to \infty$, there will be infinitely many distinct integer points $\mathbf{x}, \mathbf{y}$ with coprime components and with $\mathbf{x} \neq \mathbf{0}$ satisfying the inequality given in theorem. □

Inequality of Theorem 2.1.1 can be restated as:

$$[\![\mathcal{L}(\mathbf{x}) - \mathbf{y}]\!]^n < \frac{1}{[\![\mathbf{x}]\!]^m}$$

Hence, Theorem 2.3.1 is an improvement over Theorem 2.1.1.

Chapter 3

Rational Approximation to Algebraic Number

Major part of my exposition follows that of Prof. R. Thangadurai [9]

An *algebraic number* α is one which satisfies the equation

$$f(\alpha) = 0, \qquad f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$$

where $a_n, \ldots, a_0$ are rational numbers. On multiplying $f(x)$ by a suitable integer we may suppose that $a_n, \ldots, a_0$ are integers and, without loss of generality, that $a_n \neq 0$.

3.1 Liouville's Theorem

Liouville first remarked that, an irrational algebraic number can't be too closely approximated by rational numbers.

Definition (Algebraic Number of degree d)**.** A real number is called an algebraic number of degree d if this number is a root of an algebraic equation of degree d with integer coefficients but is not root of any other algebraic equation of lower degree with integer coefficients.

Thus, rational numbers are algebraic numbers of degree 1.

Theorem 3.1.1 (Liouville, 1844)**.** *Suppose α is a real algebraic number of degree d. Then there is a constant $c(\alpha) > 0$ such that*

$$\left|\alpha - \frac{a}{b}\right| > \frac{c(\alpha)}{b^d}$$

for every rational[1] *a/b different from α.*

[1] In considering inequalities of this type here and elsewhere, we implicitly assume that $b > 0$

Proof. Let $p(x)$ be the *defining polynomial* of α, i.e., the polynomial of degree d with root α which has coprime integer coefficients and a positive leading coefficient.

According to Taylor's formula,

$$\left|p\left(\frac{a}{b}\right)\right| = \left|\sum_{k=1}^{d}\left(\frac{a}{b}-\alpha\right)^k \frac{1}{k!} \quad p^k(\alpha)\right| \leq \frac{1}{c(\alpha)}\left|\frac{a}{b}-\alpha\right| \tag{3.1}$$

if $|a/b - \alpha| \leq 1$

Unless $d = 1$ and $\frac{a}{b} = \alpha$, we have $p(a/b) \neq 0$, from where we get $|p(a/b)| \geq 1/b^d$. Combining this with (3.1) we obtain the inequality in theorem if $|a/b - \alpha| \leq 1$. The theorem is obvious if $|a/b - \alpha| > 1$. □

Remark. Liouville used this theorem to construct transcendental numbers. See pp. 114 of [8] for examples.

Corollary 3.1.1. *Let α be an algebraic real number with degree, $d \geq 2$. For any $k > d$ we have*

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b^k}$$

has finitely many solutions in rational numbers.

Proof. On the contrary, suppose that above inequality has infinitely many solutions in rational numbers. Hence, b is unbounded and satisfy given inequality.

Let

$$\left\{\frac{a_1}{b_1}, \frac{a_2}{b_2}, \ldots, \frac{a_n}{b_n}, \ldots\right\}$$

be a set of solutions of

$$\left|\alpha - \frac{a_i}{b_i}\right| < \frac{1}{b_i^k}$$

Then, $b_i \to \infty$ as $i \to \infty$. By Theorem 3.1 we get:

$$\frac{c(\alpha)}{b_i^d} \leq \left|\alpha - \frac{a_i}{b_i}\right| < \frac{1}{b_i^k}$$

Thus,

$$c(\alpha) \leq \frac{b_i^d}{b_i^k} = \frac{1}{b_i^{k-d}}$$

Hence, $c(\alpha) \to \infty$ as $i \to \infty$. But this contradicts Theorem 3.1. Hence completing the proof. □

3.2 Statement of Roth's Theorem

Motivated by previous section we give following definition:

Definition (Approximable to order d)**.** Let $\alpha \in \mathbb{R}\backslash\{0\}$ be a real number. We say α is approximable to degree d (and to no higher) if following two conditions hold:

1. $|\alpha - a/b| < 1/b^d$ has infinitely many solutions in rational numbers.
2. For any $\varepsilon > 0$, the inequality $|\alpha - a/b| < 1/b^{d+\varepsilon}$ has only finitely many rational solutions.

Theorem 3.2.1 (Roth[2], 1955)**.** *Let $\varepsilon > 0$ be given positive real number and α be an algebraic number of degree $d \geq 1$. Then the inequality*

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b^{2+\varepsilon}}$$

has finitely many solutions in rational numbers.

Thus, Roth's theorem[3] implies that every algebraic real number is approximable to order 2 and to no higher. This had been conjectured by Siegel in 1921. Thue, Siegel, and Dyson had successively improved Liouville's original exponent d, until Roth proved Siegel's conjectured exponent in 1955. Now we will prove some corollaries which will guide us towards proof of main theorem.

Corollary 3.2.1. *Let $\varepsilon > 0$ be a given real number and α be an algebraic number of degree $d \geq 2$. Then there exist a constant $c(\alpha) > 0$ (depends only on α) such that for every rational number a/b we have*

$$\left|\alpha - \frac{a}{b}\right| \geq \frac{c(\alpha)}{b^{2+\varepsilon}}$$

Proof. Since α in algebraic number of degree $d \geq 2$, by Roth's Theorem, we have

$$\left|\alpha - \frac{x}{y}\right| < \frac{1}{y^{2+\varepsilon}}$$

[2]We will follow Cassels's rearrangement of Roth's proof, for proof outline see: Schmidt, W. M., 'Approximation to Algebraic Numbers', L'Enseignement Mathématique, 17 (1971), 187-253, doi:10.5169/seals-44578

[3]Personal anecdote of John Cosgrave, jbcosgrave@gmail.com. *"When I was a student in London, I once asked Roth (in his office at Imperial College) what were the circumstances in which he proved his famous 1955 result. Roth told me that when he worked with Davenport in University College London in the early 50's, Davenport had a practice of inviting colleagues to read up on some difficult piece of work, and then explain it in a seminar talk. Davenport asked him to read the Thue-Siegel result. He read it, understood it, explained it to everyone, and then (after all that effort) decided to give himself one year (Roth's standard practice) to solve Siegel's conjectured improvement. His year was almost up, he was just about to give up, when ..."*

has finitely many solutions in rationals. Let the solutions be $\frac{x_1}{y_1}, \frac{x_2}{y_2}, \ldots, \frac{x_M}{y_M}$. Now let,

$$c'(\alpha) = \min\left\{\left|\alpha - \frac{x_i}{y_i}\right| : i = 1, 2, \ldots, M\right\}$$

Then clearly $c'(\alpha) > 0$. Then by Liouville's Theorem, for any rational number $\frac{x_i}{y_i}$ where $i = 1, 2, \ldots, M$, we have

$$\left|\alpha - \frac{x_i}{y_i}\right| \geq c'(\alpha) \geq \frac{c'(\alpha)}{y_i^{2+\varepsilon}} \tag{3.2}$$

Also by Roth's Theorem, for any rational number, $\frac{a}{b} \neq \frac{x_i}{y_i}$ where $i = 1, 2, \ldots, M$ we have

$$\left|\alpha - \frac{a}{b}\right| \geq \frac{1}{b^{2+\varepsilon}} \tag{3.3}$$

Let, $c(\alpha) = \min\{1, c'(\alpha)\} > 0$, then from (3.2) and (3.3) we get

$$\left|\alpha - \frac{a}{b}\right| \geq \frac{c(\alpha)}{b^{2+\varepsilon}} \qquad \forall \quad \frac{a}{b} \in \mathbb{Q}$$

□

Corollary 3.2.2. *Let α be a non-zero real number, if the inequality*

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b^{2+\varepsilon}}$$

has infinitely many solutions in rational numbers for some $\varepsilon > 0$, then α is a transcendental number.

Proof. As per our assumption, there are infinitely many rational numbers such that

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b^{2+\varepsilon}}$$

we can choose rational solutions

$$\left\{\frac{a_1}{b_1}, \frac{a_2}{b_2}, \ldots, \frac{a_n}{b_n}, \ldots\right\}$$

such that $b_1 < b_2 < \ldots$.

Suppose α is an algebraic number of degree d. Since given inequality has infinitely many solutions, we conclude that $\alpha \notin \mathbb{Q}$. Therefore the degree of α is $d \geq 2$. By Corollary 3.2.1, we get:

$$\frac{c(\alpha)}{b_i^{2+\varepsilon/2}} \leq \left|\alpha - \frac{a_i}{b_i}\right| \leq \frac{1}{b_i^{2+\varepsilon}}$$

Hence,

$$c(\alpha) \leq \frac{1}{b_i^{\varepsilon/2}} \qquad \text{for} \quad i = 1, 2, 3, \ldots$$

Since, $b_i \to \infty$ as $i \to \infty$, we get $c(\alpha) \to 0$. It contradicts Corollary 3.2.1. Hence, our assumption of α being algebraic was wrong, and thus α is transcendental. □

Definition (Algebraic integer)**.** A complex number that is a root of some monic polynomial (a polynomial whose leading coefficient is 1) with integer coefficients is called algebraic integer.

Corollary 3.2.3. *It is enough to prove Roth's Theorem for algebraic integers.*

Proof. Suppose Theorem 3.2.1 (Roth's Theorem) is true for algebraic integers. Then our hypothesis is:

For any given $\varepsilon > 0$ and α be an algebraic integer of degree d, then we have

$$\left|\alpha - \frac{x}{y}\right| < \frac{1}{y^{2+\varepsilon}}$$

has finitely many rational solutions.

Now we will prove the result for any algebraic number.

Let α be an algebraic number of degree d. If, $\alpha \in \mathbb{Q}$, then clearly the result is true ($d = 1$ for rationals). So, we assume that for $d \geq 2$ the result is *not* true.

Thus, there exist a $\delta > 0$ such that

$$\left|\alpha - \frac{x}{y}\right| < \frac{1}{y^{2+\delta}} \tag{3.4}$$

has infinitely many rational solutions. Let the solutions be

$$\left\{\frac{x_1}{y_1}, \frac{x_2}{y_2}, \ldots, \frac{x_n}{y_n}, \ldots\right\}$$

such that $y_1 < y_2 < \ldots$, so that $y_i \to \infty$ as $i \to \infty$. Since α is an algebraic number, there exist $p_0 \in \mathbb{Z}\backslash\{0\}$ such that $\alpha = \frac{\beta}{p_0}$ where β is an algebraic integer. Then (3.4) becomes:

$$\left|\frac{\beta}{p_0} - \frac{x_i}{y_i}\right| < \frac{1}{y_i^{2+\delta}} \qquad \text{for} \quad i = 1, 2, 3, \ldots$$

$$\Leftrightarrow \left|\beta - p_0\frac{x_i}{y_i}\right| < \frac{p_0}{y_i^{2+\delta}} \qquad \text{for} \quad i = 1, 2, 3, \ldots$$

$$\Leftrightarrow \left|\beta - \frac{a_i}{b_i}\right| < \frac{p_0}{b_i^{2+\delta}} \qquad \text{for} \quad i = 1, 2, 3, \ldots$$

where $p_0 x_i = a_i$ and $y_i = b_i$. Now, we can write, $\delta = \delta_1 + \delta_2$ such that $\delta_1 > 0$ and $\delta_2 > 0$.

We apply hypothesis for $\alpha = \beta$ and $\varepsilon = \delta_1 > 0$.

Since, $b_i \to \infty$ as $i \to \infty$, we get, $b_i^{\delta_2} \to \infty$ as $i \to \infty$. Therefore, $\frac{p_0}{b_i^{\delta_2}} < 1$ for all $i \geq N_0 \in \mathbb{N}$. Thus we get:

$$\left|\beta - \frac{a_i}{b_i}\right| < \frac{1}{b_i^{2+\delta_1}} \times \frac{p_0}{b_i^{\delta_2}} < \frac{1}{b_i^{2+\delta_1}} \qquad \text{for all} \quad i \geq N_0$$

This leads to infinitely many solutions for inequality, thus contradicting our hypothesis. Hence our assumption was wrong and the result is true for all values of d.

□

3.3 Combinatorial Lemmas

Lemma 3.3.1. *Let $n \geq 1$ and $r \geq 0$ be integers. If $N(n,r)$ be the number of $n-$tuples $(x_1, x_2, \ldots, x_n)$ of non-negative integers such that $x_1 + x_2 + \ldots + x_n = r$, then*

$$N(n,r) = \binom{r+n-1}{r}$$

Proof. Symbolically,

$$N(n,r) := \#\{(x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n_{\geq 0} : x_1 + x_2 + \ldots + x_n = r\} \tag{3.5}$$

When $r = 0$ and $n \geq 1$, the result is true because $\binom{n-1}{0} = 1$ and the solution in non-negative integers such that $s_1 + x_2 + \ldots + x_r = 0$ is $(0, 0, \ldots, 0)$

When $r \geq 0$ and $n = 1$, the result is true because $\binom{r+1-1}{r} = 1$ and $x_1 = r$ is the only solution.

Now suppose that $r \geq 1$ and $n \geq 2$ are given. Assume that for all pairs (n', r') with $n' \leq n$, $r' \leq r$ and $(n', r') \neq (n, r)$,

$$N(n', r') = \binom{r'+n'-1}{r'}$$

Now we will prove (by induction) above formula for pair (n, r). Now, since $0 \leq x_1 \leq r$, we can re-write (3.5) as:

$$N(n,r) := \#\{(x_2, \ldots, x_n) \in \mathbb{Z}^{n-1}_{\geq 0} : x_2 + \ldots + x_n \leq r\}$$

Let

$$N^*(n,r) := \#\{(x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n_{\geq 0} : x_1 + x_2 + \ldots + x_n \leq r\}$$

Then

$$\begin{aligned} N(n,r) &= N^*(n-1,r) \\ &= N^*(n-1,r-1) + N(n-1,r) \\ &= N(n,r-1) + N(n-1,r) \\ &= \binom{n+r-2}{r-1} + \binom{n+r-2}{r} \\ &= \binom{n+r-1}{r} \end{aligned}$$

□

Lemma 3.3.2. *Let $n \geq 1$ and $r \geq 1$ be given integers. For any integer $0 \leq c \leq r$, we define*

$$F(c) = \#\{(x_2, x_3, \ldots, x_n) \in \mathbb{Z}_{\geq 0}^{n-1} : x_2 + x_3 + \ldots + x_n = r - c\}$$

Then as per notations in proof of Lemma 3.3.1,

1. $N^*(n-1, r) = \sum_{c=0}^{r} F(c) = N(n, r)$
2. $\sum_{c=0}^{r} cF(c) = \frac{r}{n} \sum_{c=0}^{r} F(c) = \frac{r}{n} N^*(n-1, r)$

Proof. 1. As per definition of $F(c)$ we get:

$$\begin{aligned} \sum_{c=0}^{r} F(c) &= \sum_{c=0}^{r} \#\{(x_2, \ldots, x_n) \in \mathbb{Z}_{\geq 0}^{n-1} : x_2 + \ldots + x_n = r - c\} \\ &= \#\{(x_2, \ldots, x_n) \in \mathbb{Z}_{\geq 0}^{n-1} : x_2 + \ldots + x_n \leq r\} \\ &= N^*(n-1, r) \\ &= N(n, r) \end{aligned}$$

2. We can re-write $F(c)$ as:

$$F(c) = \sum_{\substack{x_2, \ldots, x_n \in \mathbb{Z}_{\geq 0} \\ x_2 + \ldots + x_n = r - c}} 1 = \sum_{\substack{x_2, \ldots, x_n \in \mathbb{Z}_{\geq 0} \\ c + x_2 + \ldots + x_n = r}} 1$$

Let c be any integer where $0 \leq c \leq r$. Then

$$cF(c) = \sum_{\substack{x_2, \ldots, x_n \in \mathbb{Z}_{\geq 0} \\ c + x_2 + \ldots + x_n = r}} c$$

Now, do summation over c both sides to get:

$$\begin{aligned} \sum_{c=0}^{r} cF(c) &= \sum_{c=0}^{r} \sum_{\substack{x_2, \ldots, x_n \in \mathbb{Z}_{\geq 0} \\ c + x_2 + \ldots + x_n = r}} c \\ &= \sum_{\substack{c, x_2, \ldots, x_n \in \mathbb{Z}_{\geq 0} \\ c + x_2 + \ldots + x_n = r}} c \end{aligned}$$

But, note that

$$\sum_{\substack{c, x_2, \ldots, x_n \in \mathbb{Z}_{\geq 0} \\ c + x_2 + \ldots + x_n = r}} c = \sum_{\substack{c, x_2, \ldots, x_n \in \mathbb{Z}_{\geq 0} \\ c + x_2 + \ldots + x_n = r}} x_i \qquad \text{for } i = 2, \ldots, n$$

Therefore,

$$\begin{aligned}
\sum_{c=0}^{r} cF(c) &= \frac{1}{n}\left\{ \sum_{\substack{c,x_2,\ldots,x_n\in\mathbb{Z}_{\geq 0}\\ c+x_2+\ldots+x_n=r}} c + \cdots + \sum_{\substack{c,x_2,\ldots,x_n\in\mathbb{Z}_{\geq 0}\\ c+x_2+\ldots+x_n=r}} x_n \right\} \\
&= \frac{1}{n} \sum_{\substack{c,x_2,\ldots,x_n\in\mathbb{Z}_{\geq 0}\\ c+x_2+\ldots+x_n=r}} (c + x_2 + \ldots + x_n) \\
&= \frac{1}{n} \sum_{\substack{c,x_2,\ldots,x_n\in\mathbb{Z}_{\geq 0}\\ c+x_2+\ldots+x_n=r}} r \\
&= \frac{r}{n} \sum_{\substack{c,x_2,\ldots,x_n\in\mathbb{Z}_{\geq 0}\\ c+x_2+\ldots+x_n=r}} 1 \\
&= \frac{r}{n} \sum_{\substack{x_2,\ldots,x_n\in\mathbb{Z}_{\geq 0}\\ x_2+\ldots+x_n\leq r-c}} 1 \\
&= \frac{r}{n} N^*(n-1,r) \qquad \text{(from definition of } N^*(n,r)) \\
&= \frac{r}{n} \sum_{c=0}^{r} F(c) \qquad \text{(from part 1. of this lemma)}
\end{aligned}$$

□

Lemma 3.3.3. *For any $x \in \mathbb{R}$ such that $|x| \leq 1$, we have $1 + x \leq e^x \leq 1 + x + x^2$.*

Proof. Let $x \in \mathbb{R}$ such that $|x| \leq 1$.

Firstly we will prove the lower bound.

If $0 \leq x \leq 1$, then

$$1 + x \leq e^x = 1 + x + \frac{x^2}{2} + \ldots + \frac{x^n}{n!} + \ldots$$

since $x^k/k!$ is non-negative for all $k = 1, 2, \ldots$

If $-1 \leq x < 0$, then

$$\frac{x^{2n}}{(2n)!} + \frac{x^{2n+1}}{(2n+1)!} \geq 0$$

$$\Leftrightarrow \frac{x^{2n}}{(2n)!} \geq -\frac{x^{2n+1}}{(2n+1)!}$$

$$\Leftrightarrow 2n + 1 \geq -x$$

$$\Leftrightarrow 2n + 1 \geq 0$$

Hence, the above inequality is true for all $n \geq 1$ and $-1 \leq x < 0$. Thus

$$e^x = 1 + x + \left(\frac{x^2}{2} + \frac{x^3}{3!}\right) + \left(\frac{x^4}{4!} + \frac{x^5}{5!}\right) + \ldots \geq 1 + x$$

Now, we will prove the upper bound. Since we have to prove that $e^x \leq 1 + x + x^2$, it is equivalent to proving

$$1 + x + \frac{x^2}{2} + \ldots + \frac{x^n}{n!} + \ldots \leq 1 + x + x^2 \qquad \text{for} \quad -1 \leq x \leq 1$$

$$\Leftrightarrow \frac{x^3}{3!} + \frac{x^4}{4!} + \ldots \leq \frac{x^2}{2} \qquad \text{for} \quad -1 \leq x \leq 1$$

Note that $n! \geq 2^{n-1}$ for all $n \geq 3$ (can be proved by induction). Therefore,

$$\begin{aligned}
\frac{x^3}{3!} + \frac{x^4}{4!} + \ldots &\leq \frac{x^3}{2^2} + \frac{x^4}{2^3} + \ldots \\
&= \frac{x^3}{4}\left(1 + \left(\frac{x}{2}\right) + \ldots\right) \\
&= \frac{x^3}{4}\left(\frac{1}{1 - \frac{x}{2}}\right) \qquad \text{is valid since } |x| < 1 \\
&= \frac{x^3}{2(2-x)}
\end{aligned}$$

Hence it is enough to prove,

$$\frac{x^3}{2(2-x)} \leq \frac{x^2}{2} \qquad \text{for} \quad -1 \leq x \leq 1$$

$$\Leftrightarrow x^2(x-1) \leq 0 \qquad \text{for} \quad -1 \leq x \leq 1$$

Leading to $x \leq 1$, hence above inequality is true for $|x| < 1$. Thus completing the proof. □

Lemma 3.3.4 (Mahler-Reuter, 1961[4]). *Let $0 < \varepsilon < 1$ be given and $n \geq 1$; $r_1, r_2, \ldots, r_n > 0$ be integers. Then*

$$\#\left\{(x_1, \ldots, x_n) \in \mathbb{Z}^n_{\geq 0} : \begin{array}{l} 0 \leq x_k \leq r_k \forall k = 1, \ldots, n \\ \left|\sum_{k=1}^n \frac{x_k}{r_k} - \frac{n}{2}\right| \geq \varepsilon n \end{array}\right\} \leq 2\prod_{k=1}^n (r_k+1) e^{-\varepsilon^2 n/4}$$

Proof. In order to prove this lemma we will prove two claims.
Claim 1:*Let $m \geq 2$ be a given integer. Then*

$$\#\left\{\begin{array}{l} (x_{k1}, \ldots, x_{km}) \\ \text{in } \mathbb{Z}^m_{\geq 0} \end{array} : \begin{array}{l} k = 1, 2, \ldots, n \\ x_{k1} + \ldots + x_{km} = r_k \\ \left|\sum_{k=1}^n \frac{x_{k1}}{r_k} - \frac{n}{m}\right| \geq \varepsilon n \end{array}\right\} \leq 2\prod_{k=1}^n \binom{r_k + m - 1}{r_k} e^{\frac{-\varepsilon^2 n}{4}}$$

[4] A slightly weaker version was proved by Schneider in 1936. Roth used a simpler version of Schneider's lemma by Davenport (Lemma 8 in [7])

If we prove this claim, then this lemma follows by taking $m = 2$. Since, for $m = 2$, we get

$$\#\left\{(x_{k1}, x_{k2}) \in \mathbb{Z}^2_{\geq 0} : \begin{array}{l} k = 1, 2, \ldots, n \\ x_{k1} + x_{k2} = r_k \\ \left|\sum_{k=1}^n \frac{x_{k1}}{r_k} - \frac{n}{2}\right| \geq \varepsilon n \end{array}\right\} \leq 2\prod_{k=1}^n (r_k+1)e^{\frac{-\varepsilon^2 n}{4}} \quad (3.6)$$

Since, $x_{k1} + x_{k2} = r_k$ and $x_{ki} \geq 0$ are integers, we can replace this condition by

$$0 \leq x_{k1} \leq r_k \quad \Leftrightarrow \quad \begin{array}{ll} & x_{k1} + x_{k2} = r_k \quad \text{as} \\ & x_{k2} \quad \text{runs through 0 to } r_k \\ \text{and} & x_{k1} = r_k - x_{k2} \end{array}$$

Therefore we can rewrite (3.6) as:

$$\#\left\{(x_1, \ldots, x_n) \in \mathbb{Z}^n_{\geq 0} : \begin{array}{l} 0 \leq x_k \leq r_k \forall k = 1, \ldots, n \\ \left|\sum_{k=1}^n \frac{x_k}{r_k} - \frac{n}{2}\right| \geq \varepsilon n \end{array}\right\} \leq 2\prod_{k=1}^n (r_k+1)e^{-\varepsilon^2 n/4}$$

Thus this lemma follows from Claim 1.

From Claim 1 we shall further deduce the following.

For any tuple $(x_1, \ldots, x_n) \in \mathbb{Z}^n_{\geq 0}$ we have

$$\left|\frac{x_1}{r_1} + \ldots + \frac{x_n}{r_n} - \frac{n}{m}\right| \geq \varepsilon n$$

$$\Leftrightarrow \frac{x_1}{r_1} + \ldots + \frac{x_n}{r_n} - \frac{n}{m} \geq \varepsilon n \quad \text{and} \quad \frac{x_1}{r_1} + \ldots + \frac{x_n}{r_n} - \frac{n}{m} \leq -\varepsilon n$$

$$\Leftrightarrow \frac{x_1}{r_1} + \ldots + \frac{x_n}{r_n} \geq n\left(\frac{1}{m} + \varepsilon\right) \quad \text{and} \quad \frac{x_1}{r_1} + \ldots + \frac{x_n}{r_n} \leq n\left(\frac{1}{m} - \varepsilon\right)$$

We want to estimate the cardinality of set, M, given by

$$M = \#\left\{(x_{k1}, \ldots, x_{km}) \in \mathbb{Z}^m_{\geq 0} : \begin{array}{l} k = 1, 2, \ldots, n \\ x_{k1} + \ldots + x_{km} = r_k \\ \left|\sum_{k=1}^n \frac{x_{k1}}{r_k} - \frac{n}{m}\right| \geq \varepsilon n \end{array}\right\}$$

But, we can write $M = M_+ + M_-$ where

$$M_+ = \#\left\{(x_{k1}, \ldots, x_{km}) \in \mathbb{Z}^m_{\geq 0} : \begin{array}{l} k = 1, 2, \ldots, n \\ x_{k1} + \ldots + x_{km} = r_k \\ \sum_{k=1}^n \frac{x_{k1}}{r_k} \geq n\left(\frac{1}{m} + \varepsilon\right) \end{array}\right\}$$

and

$$M_- = \#\left\{(x_{k1}, \ldots, x_{km}) \in \mathbb{Z}^m_{\geq 0} : \begin{array}{l} k = 1, 2, \ldots, n \\ x_{k1} + \ldots + x_{km} = r_k \\ \sum_{k=1}^n \frac{x_{k1}}{r_k} \leq n\left(\frac{1}{m} - \varepsilon\right) \end{array}\right\}$$

In order to prove Claim 1, we need to prove

$$M \leq 2\prod_{k=1}^{n}\binom{r_k+m-1}{r_k}e^{-\varepsilon^2 n/4}$$

Since, $M = M_+ + M_-$, it is enough to prove

$$M_+, M_- \leq \prod_{k=1}^{n}\binom{r_k+m-1}{r_k}e^{-\varepsilon^2 n/4} \tag{3.7}$$

Claim 2: *For any integer k with $1 \leq k \leq n$ and any integer c_k with $0 \leq c_k \leq r_k$, we define:*

$$F_k(c_k) = \#\{(x_{k2}, \ldots, x_{km}) \in \mathbb{Z}_{\geq 0}^{m-1} : x_{k2} + \ldots + x_{kn} = r_k - c_k\}$$

Then we have,

$$M_+ = \sum_{\substack{c_1,\ldots,c_n \\ 0\leq c_k\leq r_k \\ \sum_{k=1}^{n}\frac{c_k}{r_k}-\frac{n}{m}\geq\varepsilon n}} F_1(c_1)\cdots F_n(c_n)$$

and

$$M_- = \sum_{\substack{c_1,\ldots,c_n \\ 0\leq c_k\leq r_k \\ \sum_{k=1}^{n}\frac{c_k}{r_k}-\frac{n}{m}\leq-\varepsilon n}} F_1(c_1)\cdots F_n(c_n)$$

Note that:

$$\sum_{\substack{c_1,\ldots,c_n \\ 0\leq c_k\leq r_k}} F_1(c_1)\cdots F_n(c_n) = \prod_{k=1}^{n}\left(\sum_{c_k=0}^{r_k} F_k(c_k)\right)$$

By Lemma 3.3.2 and Lemma 3.3.1 we get:

$$\begin{aligned}\prod_{k=1}^{n}\left(\sum_{c_k=0}^{r_k} F_k(c_k)\right) &= \prod_{k=1}^{n} N(m, r_k) \\ &= \prod_{k=1}^{n}\binom{r_k+m-1}{r_k}\end{aligned}$$

Therefore, Claim 2 follows from the definition of M_+, M_- and $F_k(c_k)$ in the above equality.

Now we will prove (3.7) for M_+ (the proof for M_- is similar). Consider

$$\begin{aligned}
M_+ e^{\varepsilon^2 n/2} &= M_+ \exp\left(\frac{\varepsilon^2 n}{2}\right) \\
&= M_+ \exp\left(\frac{\varepsilon}{2}\varepsilon n\right) \\
&= \prod_{k=1}^{n} \left(\sum_{\substack{c_k=0 \\ \sum_{k=1}^{n} \frac{c_k}{r_k} - \frac{n}{m} \geq \varepsilon n}}^{r_k} F_k(c_k) \right) \exp\left(\frac{\varepsilon}{2}\varepsilon n\right) \\
&\leq \prod_{k=1}^{n} \left(\sum_{\substack{c_k=0 \\ \sum_{k=1}^{n} \frac{c_k}{r_k} - \frac{n}{m} \geq \varepsilon n}}^{r_k} F_k(c_k) \right) \exp\left(\frac{\varepsilon}{2}\left(\frac{c_1}{r_1} + \ldots + \frac{c_n}{r_n} - \frac{n}{m}\right)\right) \\
&\leq \prod_{k=1}^{n} \left(\sum_{c_k=0}^{r_k} F_k(c_k) \right) \exp\left(\frac{\varepsilon}{2}\left(\frac{c_1}{r_1} + \ldots + \frac{c_n}{r_n} - \frac{n}{m}\right)\right) \\
&= \prod_{k=1}^{n} \left(\sum_{c_k=0}^{r_k} F_k(c_k) \right) \exp\left(\frac{\varepsilon}{2}\sum_{k=1}^{n}\left(\frac{c_k}{r_k} - \frac{1}{m}\right)\right) \\
&= \prod_{k=1}^{n} \left(\sum_{c_k=0}^{r_k} F_k(c_k) \right) \left(\prod_{k=1}^{n} \exp\left(\frac{\varepsilon}{2}\left(\frac{c_k}{r_k} - \frac{1}{m}\right)\right)\right) \\
&= \prod_{k=1}^{n} \left(\sum_{c_k=0}^{r_k} F_k(c_k) \exp\left(\frac{\varepsilon}{2}\left(\frac{c_k}{r_k} - \frac{1}{m}\right)\right)\right)
\end{aligned}$$

Similarly we will get:

$$M_- e^{\varepsilon^2 n/2} \leq \prod_{k=1}^{n} \left(\sum_{c_k=0}^{r_k} F_k(c_k) \exp\left(-\frac{\varepsilon}{2}\left(\frac{c_k}{r_k} - \frac{1}{m}\right)\right)\right)$$

Put $y = \pm\frac{\varepsilon}{2}\left(\frac{c_k}{r_k} - \frac{1}{m}\right)$

Since, $0 \leq c_k \leq r_k$, we see $0 \leq \frac{c_k}{r_k} \leq 1$ Therefore,

$$\frac{-1}{m} \leq \frac{c_k}{r_k} - \frac{1}{m} \leq 1 - \frac{1}{m} \quad \Leftrightarrow \quad |y| \leq 1 \tag{3.8}$$

By Lemma 3.3.3, we set $1 + y \leq e^y \leq 1 + y + y^2$. Therefore,

$$\exp\left(\frac{\varepsilon}{2}\left(\frac{c_k}{r_k} - \frac{1}{m}\right)\right) \leq 1 + \frac{\varepsilon}{2}\left(\frac{c_k}{r_k} - \frac{1}{m}\right) + \frac{\varepsilon^2}{4}\left(\frac{c_k}{r_k} - \frac{1}{m}\right)^2 \tag{3.9}$$

Interestingly,

$$\begin{aligned}\sum_{c_k=0}^{r_k} F_k(c_k)\left(\frac{\varepsilon}{2}\left(\frac{c_k}{r_k}-\frac{1}{m}\right)\right) &= \sum_{c_k=0}^{r_k} F_k(c_k)\left(\frac{\varepsilon}{2r_k}\left(c_k-\frac{r_k}{m}\right)\right)\\ &= \frac{\varepsilon}{2r_k}\left(\sum_{c_k=0}^{r_k} c_k F_k(c_k)-\frac{r_k}{m}\sum_{c_k=0}^{r_k} F_k(c_k)\right)\\ &= \frac{\varepsilon}{2r_k}\times 0 = 0 \quad \text{(from Lemma 3.3.2)}\end{aligned}$$

Hence,

$$\sum_{c_k=0}^{r_k} F_k(c_k)\left(\frac{\varepsilon}{2}\left(\frac{c_k}{r_k}-\frac{1}{m}\right)\right) = 0 \tag{3.10}$$

Now, using (3.8), (3.9) and (3.10), we get

$$\begin{aligned}\sum_{c_k=0}^{r_k} F_k(c_k)e^{\frac{\varepsilon}{2}\left(\frac{c_k}{r_k}-\frac{1}{m}\right)} &\le \sum_{c_k=0}^{r_k} F_k(c_k)\left[1+\frac{\varepsilon}{2}\left(\frac{c_k}{r_k}-\frac{1}{m}\right)+\frac{\varepsilon^2}{4}\left(\frac{c_k}{r_k}-\frac{1}{m}\right)^2\right]\\ &\le \sum_{c_k=0}^{r_k} F_k(c_k)\left[1+\frac{\varepsilon}{2}\left(\frac{c_k}{r_k}-\frac{1}{m}\right)+\frac{\varepsilon^2}{4}\right]\\ &= \sum_{c_k=0}^{r_k} F_k(c_k)\left(1+\frac{\varepsilon^2}{4}\right)\end{aligned}$$

Thus,

$$\begin{aligned}M_+ e^{\varepsilon^2 n/2} &\le \prod_{k=1}^{n}\left(\sum_{c_k=0}^{r_k} F_k(c_k)\left(1+\frac{\varepsilon^2}{4}\right)\right)\\ &= \prod_{k=1}^{n}\binom{r_k+m-1}{r_k}\left(1+\frac{\varepsilon^2}{4}\right)^n \quad \text{(as in proof of Claim 2)}\\ &\le \prod_{k=1}^{n}\binom{r_k+m-1}{r_k}\left(e^{\frac{\varepsilon^2}{4}}\right)^n \quad \text{(from Lemma 3.3.3)}\end{aligned}$$

Thus, we get:

$$M_+ \le \prod_{k=1}^{n}\binom{r_k+m-1}{r_k}e^{-\frac{\varepsilon^2 n}{4}}$$

Similarly we will get for M_-, hence completing the proof. □

3.4 Auxiliary Polynomial in m-variables

In this section, we will consider polynomials in m variables with rational integer coefficients. Indeed we can write

$$P(x_1, \ldots, x_m) = \sum_{j_1=0}^{r_1} \cdots \sum_{j_m=0}^{r_m} q(j_1, \ldots, j_m) x_1^{j_1} \ldots x_m^{j_m}$$

where, all except finitely many of the coefficients, $q(j_1, \ldots, j_m) \in \mathbb{Z}$, are zero.

A curious question we can ask here is: *Why do we want to study polynomial of several variable when we want to approximate just one algebraic integer*[5] *?*

We saw that Liouville used polynomial in one variable to prove his result. But a Norwegian mathematician Axel Thue accomplished more than Liouville using a polynomial of one variable[6]. Thue's progress (obtaining an approximation exponent of $d/2 + 1 + \varepsilon$) can all be formulated in terms of functions of one variable. It can also be thought of as using an auxiliary polynomial $f(X, Y) \in \mathbb{Z}[X, Y]$ in two variables which is linear in Y. Thus, it was observed that Lioville's Theorem can not be improved, in general, working with a polynomial of one variable. Therefore, Roth's theorem requires an auxiliary polynomial in an arbitrary number of variables but the logical steps remain the same as that of Liouville's Theorem.

We will conclude this section with the theorem regarding the index of auxiliary polynomial in $m-$variables at rational points near the algebraic-integer point (a $m-$tuple).

3.4.1 Partial derivative of a polynomial

As per our earlier notations, we will write $\mathbf{i}$ to represent a $m-$ tuple, $(i_1, i_2, \ldots, i_m)$. For $\mathbf{i} \in \mathbb{Z}_{\geq 0}^m$, we define

$$P_{\mathbf{i}}(x_1, \ldots, x_m) = \frac{1}{i_1! i_2! \ldots i_m!} \frac{\partial^{i_1 + \ldots + i_m}}{\partial x_1^{i_1} \cdots \partial x_m^{i_m}} P(x_1, \ldots, x_m)$$

Lemma 3.4.1. *Let $P(x_1, \ldots, x_m) \in \mathbb{Z}[x_1, \ldots, x_m]$ be a polynomial. For any $\mathbf{i} = (i_1, \ldots, i_m) \in \mathbb{Z}_{\geq 0}^m$ we have:*

$$P_{\mathbf{i}}(x_1, \ldots, x_m) \in \mathbb{Z}[x_1, \ldots, x_m]$$

[5]Better answer to this question is available when we study transcendental numbers, see Burger, E. B. and Tubbs, R., Making Transcendence Transparent (Springer, 2004), 32-34.

[6]For details see §1 of [4], http://www.mast.queensu.ca/~mikeroth/proceedings/Nakamaye-Roth-Method.pdf

Proof. We just need to manipulate definition:

$$\begin{aligned} P_{\mathbf{i}}(x_1,\dots,x_m) &= \frac{1}{i_1!i_2!\dots i_m!}\frac{\partial^{i_1+\dots+i_m}}{\partial x_1^{i_1}\cdots\partial x_m^{i_m}}P(x_1,\dots,x_m) \\ &= \frac{1}{i_1!i_2!\dots i_m!}\sum_{\substack{j_1,\dots,j_m \\ 0\le j_k\le r_k}} q(j_1,\dots,j_m)\frac{\partial^{i_1}x_1^{j_1}}{\partial x_1^{i_1}}\cdots\frac{\partial^{i_m}x_,^{j_m}}{\partial x_m^{i_m}} \\ &= \sum_{\substack{j_1,\dots,j_m \\ 0\le j_k\le r_k}} q(j_1,\dots,j_m)\prod_{\ell=1}^{m}\frac{j_\ell\cdots(j_\ell-(i_\ell-1))}{i_\ell}x_\ell^{j_\ell-i_\ell} \\ &= \sum_{\substack{j_1,\dots,j_m \\ 0\le j_k\le r_k}} q(j_1,\dots,j_m)\prod_{\ell=1}^{m}\binom{j_\ell}{i_\ell}x_\ell^{j_\ell-i_\ell}\in\mathbb{Z}[x_1,\dots,x_m] \end{aligned}$$

(Also, as in combinatorics, $\binom{j_\ell}{i_\ell}=0$ of $j_\ell<i_\ell$.) □

3.4.2 Height of a polynomial and Siegel's Lemma

For any polynomial $P(x_1,\dots,x_m)\in\mathbb{Z}[x_1,\dots,x_m]$, we define the height of the polynomial $P(x_1,\dots,x_m)$, denoted by $[\![P]\!]$ as

$$[\![P]\!] = \max_{\substack{j_1,\dots,j_k \\ 0\le j_k\le r_k}} |q(j_1,\dots,j_m)|$$

and

$$P(x_1,\dots,x_m)=\sum_{\substack{j_1,\dots,j_m \\ 0\le j_k\le r_k}} q(j_1,\dots,j_m)x_1^{j_1}\dots x_m^{j_m}$$

Note that when $m=1$, $[\![P]\!]$ is the maximum of the absolute value of its coefficients which matches with usual definition of height of P (see Section 2.3)

Lemma 3.4.2. *Let $P(x_1,\dots,x_m)\in\mathbb{Z}[x_1,\dots,x_m]$ be a polynomial. For any $\mathbf{i}=(i_1,\dots,i_m)\in\mathbb{Z}_{\ge 0}^m$ we have:*

$$[\![P_{\mathbf{i}}]\!]\le 2^{r_1+r_2+\dots+r_m}[\![P]\!]$$

Proof. From Lemma 3.4.1 we know that:

$$\begin{aligned} P_{\mathbf{i}}(x_1,\dots,x_m) &= \sum_{\substack{j_1,\dots,j_m \\ 0\le j_k\le r_k}} q(j_1,\dots,j_m)\prod_{\ell=1}^{m}\binom{j_\ell}{i_\ell}x_\ell^{j_\ell-i_\ell} \\ &= \sum_{\substack{j_1,\dots,j_m \\ 0\le j_k\le r_k}} A(j_1,\dots,j_m)x_1^{j_1-i_1}\cdots x_m^{j_m-i_m} \end{aligned}$$

where

$$A(j_1,\dots,j_m) = q(j_1,\dots,j_m)\prod_{\ell=1}^{m}\binom{j_\ell}{i_\ell}$$

Therefore,

$$\begin{aligned}
|A(j_1,\dots,j_m)| &= |q(j_1,\dots,j_m)|\binom{j_1}{i_1}\cdots\binom{j_m}{i_m} \\
&\le |q(j_1,\dots,j_m)| \quad 2^{j_1}\cdots 2^{j_m} \\
&\le |q(j_1,\dots,j_m)| \quad 2^{r_1}\cdots 2^{r_m} \qquad (\text{as } j_k \le r_k \forall k) \\
&= |q(j_1,\dots,j_m)| \quad 2^{r_1+\dots+r_m}
\end{aligned}$$

Thus,

$$\begin{aligned}
[\![P_{\mathbf{i}}]\!] &= \max_{\substack{j_1,\dots,j_k \\ 0\le j_k\le r_k}} |A(j_1,\dots,j_m)| \\
&\le 2^{r_1+\dots+r_m} \max_{\substack{j_1,\dots,j_k \\ 0\le j_k\le r_k}} |q(j_1,\dots,j_m)| \\
&= 2^{r_1+\dots+r_m}[\![P]\!]
\end{aligned}$$

□

Lemma 3.4.3 (Siegel)**.** *Let*

$$L_j(\mathbf{z}) = \sum_{k=1}^{N} a_{jk}z_k \qquad (1\le j\le M)$$

be M linear forms with rational integer coefficients. Suppose that $N > M$ and that

$$|a_{jk}| \le Q \qquad (1\le j\le M,\quad 1\le k\le N)$$

where Q is a positive integer. Then there exists an integer point $\mathbf{z} = (z_1,\dots,z_N) \neq \mathbf{0}$ with

$$L_j(\mathbf{z}) = 0 \qquad (1\le j\le M)$$

and

$$[\![\mathbf{z}]\!] \le \left\lfloor (NQ)^{\frac{M}{N-M}} \right\rfloor$$

Proof. Since $N > M$, rational solutions of $L_j(\mathbf{z}) = 0$ for $1 \le j \le M$ with $\mathbf{z} \neq \mathbf{0}$ always exist. But, if $\mathbf{z}$ is a solution of this equation, then so is $\lambda\mathbf{z}$ for any real λ, and therefore integer points $\mathbf{z} \neq \mathbf{0}$ exist, which satisfy this equation.

It remains to show that

$$[\![\mathbf{z}]\!] \le Z \quad \text{where} \quad Z = \left\lfloor (NQ)^{\frac{M}{N-M}} \right\rfloor$$

can also be satisfied. We will follow pigeonhole principle (see Lemma 2.1.1).

Firstly we have $Z+1 > (NQ)^{\frac{M}{N-M}}$, from where $NQ < (Z+1)^{\frac{N-M}{M}}$ and therefore

$$NQZ + 1 \leq NQ(Z+1) < (Z+1)^{N/M} \tag{3.11}$$

Now, for every integer point $\mathbf{z} = (z_1, \ldots, z_N)$ with $0 \leq z_i \leq Z$ for $1 \leq i \leq N$, we have

$$-R_j Z \leq L_j(\mathbf{z}) \leq S_j Z \qquad (1 \leq j \leq M)$$

where $-R_j$ and S_j are the sums of negative and positive coefficients of $L(\mathbf{z})$, respectively. Now $R_j + S_j \leq NQ$, so that each $L_j(\mathbf{z})$ lies in an interval of length less than or equal to NQZ. Therefore each $L_j(\mathbf{z})$ takes at most $NQZ+1$ distinct values. Hence the $M-$tuple, $L_1(\mathbf{z}), \ldots, L_M(\mathbf{z})$ takes at most $(NQZ+1)^M$ values.

The number of possibilities for $\mathbf{z}$ with $0 \leq z_i \leq Z$ for $1 \leq i \leq N$ is $(Z+1)^N$.

But, from (3.11), $(NQZ+1)^M < (Z+1)^N$. Thus there are $N-$tuples $\mathbf{z}^{(1)} \neq \mathbf{z}^{(2)}$ with $0 \leq z_i \leq Z$ for $1 \leq i \leq N$ and $L_j\left(\mathbf{z}^{(1)}\right) = L_j\left(\mathbf{z}^{(2)}\right)$ for $1 \leq j \leq M$.

The integer point $\mathbf{z} = \mathbf{z}^{(1)} - \mathbf{z}^{(2)}$ satisfies the conditions of the lemma. □

Lemma 3.4.4. *Let α be an algebraic number of degree $d \geq 1$ and let $P(x) = x^d + a_{d-1}x^{d-1} + \ldots + a_0$ be the minimal polynomial of α with integer coefficients. Then for any interval $\ell \geq 1$, there exist integers $a_{d-1}^{(\ell)}, a_{d-2}^{(\ell)}, \ldots, a_0^{(\ell)}$ with*

$$\alpha^\ell = a_{d-1}^{(\ell)}\alpha^{d-1} + \ldots + a_0^{(\ell)}$$

and

$$|a_k^{(\ell)}| \leq (\llbracket P \rrbracket + 1)^\ell \qquad \forall k = 0, 1, \ldots, d-1$$

Proof. We will prove this by induction on $\ell \geq 1$.

When $\ell \leq d-1$, we can set $a_\ell^{(\ell)} = 1$ and $a_k^{(\ell)} = 0$ when $k \neq \ell$, this will satisfy given condition.

When $\ell = d$, since $P(\alpha) = 0$, we get

$$\alpha^d + a_{d-1}\alpha^{d-1} + \ldots + a_0 = 0$$

$$\Rightarrow \alpha^d = (-a_{d-1})\alpha^{d-1} + \ldots + (-a_0)$$

with

$$|a_k| \leq \llbracket P \rrbracket \leq (\llbracket P \rrbracket + 1)^d \qquad \forall k = 0, 1, \ldots, d-1$$

Hence, given condition is satisfied for $\ell \leq d$

We can assume that $\ell > d$ and for $\ell - 1$ the result is true. Therefore,

$$\begin{aligned}
\alpha^{\ell} &= \alpha \cdot \alpha^{\ell-1} \\
&= \alpha \left(a_{d-1}^{(\ell-1)} \alpha^{d-1} + \ldots + a_0^{(\ell-1)} \right) \\
&= a_{d-1}^{(\ell-1)} \alpha^{d} + \ldots + a_0^{(\ell-1)} \alpha \\
&= a_{d-1}^{(\ell-1)} \left((-a_{d-1}) \alpha^{d-1} + \ldots + (-a_0) \right) + a_{d-2}^{(\ell-1)} \alpha^{d-1} + \ldots + a_0^{\ell-1} \alpha \\
&= \left(-a_{d-1}^{(\ell-1)} a_{d-1} + a_{d-2}^{(\ell-1)} \right) \alpha^{d-1} + \ldots + \left(-a_{d-1}^{(\ell-1)} a_0 \right)
\end{aligned}$$

Also, for $0 \leq k \leq d-1$ as per triangle inequality and induction hypothesis,

$$\begin{aligned}
\left| -a_{d-1}^{(\ell-1)} a_k + a_{k-1}^{(\ell-1)} \right| &\leq \left| -a_{d-1}^{(\ell-1)} a_k \right| + \left| a_{k-1}^{(\ell-1)} \right| \\
&\leq (\llbracket P \rrbracket + 1)^{\ell-1} \llbracket P \rrbracket + (\llbracket P \rrbracket + 1)^{\ell-1} \\
&= (\llbracket P \rrbracket + 1)^{\ell-1} (\llbracket P \rrbracket + 1) \\
&= (\llbracket P \rrbracket + 1)^{\ell}
\end{aligned}$$

Hence completing the proof. □

3.4.3 Index of a polynomial

Let $P(x_1, x_2, \ldots, x_m)$ be a polynomial with rational integer coefficients. Let $\mathbf{r} = (r_1, \ldots, r_m) \in \mathbb{Z}_{\geq 1}^m$ and $\mathbf{q} = (q_1, \ldots, q_m) \in \mathbb{R}^m$ be given $m-$tuples.

If P is not a zero-polynomial i.e. $P \not\equiv 0$, then *index of P with respect to* $(q_1, \ldots, q_m; r_1, \ldots, r_m) = (\mathbf{q}; \mathbf{r})$ is defined to be

$$\operatorname{ind}_{(\mathbf{q};\mathbf{r})} P = \min_{\substack{\mathbf{i}=(i_1,\ldots,i_m)\in\mathbb{Z}_{\geq 0}^m \\ 0 \leq i_k \leq \deg_P x_i}} \left\{ \frac{i_1}{r_1} + \ldots + \frac{i_m}{r_m} : P_{\mathbf{i}}(q_1, \ldots, q_m) \neq 0 \right\}$$

where, $\deg_P x_i$ = maximum degree of x_i in any monomial of P.

If P is a zero-polynomial i.e. $P \equiv 0$, then index of P is defined to be $+\infty$ for any $(r_1, \ldots, r_m) \in \mathbb{Z}_{\geq 1}^m$ and $(q_1, \ldots, q_m) \in \mathbb{R}^m$ since $P_{\mathbf{i}}(x_1, \ldots, x_m) = 0$ for all $\mathbf{i} \in \mathbb{Z}_{\geq 0}^m$.

Lemma 3.4.5. *If $P \not\equiv 0$, then $\operatorname{ind}_{(\mathbf{q};\mathbf{r})} P$ is a finite number.*

Proof. Let the total degree of $P(x_1, \ldots, x_m)$ be $k = k_1 + \ldots + k_m$, where $x_1^{k_1} \ldots x_m^{k_m}$ is a monomial in P whose degree is maximum of all the other monomials in P and $k_\ell = \deg_P x_\ell$. If $\mathbf{k} = (k_1, \ldots, k_m)$, then $P_{\mathbf{k}}(x_1, \ldots, x_m)$ is a constant polynomial[7] and hence, $P_{\mathbf{k}}(q_1, \ldots, q_m) \neq 0$. Also

$$\operatorname{ind}_{(\mathbf{q};\mathbf{r})} P \leq \frac{k_1}{r_1} + \ldots + \frac{k_m}{r_m} < \infty$$

□

[7] analogous to the case when, $f(x) = \sum_{k=0}^{n} a_r x^r$ is a polynomial, then $f^n(x) = n!$ is a constant polynomial.

Remark. Note that r_ℓ may be smaller that k_ℓ.

Corollary 3.4.1. *If $P(x_1, \ldots, x_m)$ is a non-zero constant polynomial, then $P(q_1, \ldots, q_m) \neq 0$ implies that $\operatorname{ind}_{(\mathbf{q};\mathbf{r})} P = 0$*

Proof. It follows from Lemma 3.4.5, since $\frac{k_1}{r_1} + \ldots + \frac{k_m}{r_m} = 0$. □

Corollary 3.4.2. *If $\operatorname{ind}_{(\mathbf{q};\mathbf{r})} P \neq 0$, then $P(q_1, \ldots, q_m) = 0$ implies that $\mathbf{q} = (q_1, \ldots, q_m)$ is a zero of the polynomial $P(x_1, \ldots, x_m)$.*

Proof. Follows from Corollary 3.4.1 □

Lemma 3.4.6. *Let $P, Q \in \mathbb{Z}[x_1, \ldots, x_m] \backslash \{0\}$ be given polynomials with the given parameters $\mathbf{r} = (r_1, \ldots, r_m) \in \mathbb{Z}^m_{\geq 1}$ and $\mathbf{q} = (q_1, \ldots, q_m) \in \mathbb{R}^m$ from which index of P and Q are calculated. Then,*

1. *For any $\mathbf{i} = (i_1, \ldots, i_k) \in \mathbb{Z}^m_{\geq 0}$ we have*

$$\operatorname{ind}_{(\mathbf{q};\mathbf{r})} P_{\mathbf{i}} \geq \operatorname{ind}_{(\mathbf{q};\mathbf{r})} P - \left(\frac{i_1}{r_1} + \ldots + \frac{i_m}{r_m} \right)$$

2. $\operatorname{ind}_{(\mathbf{q};\mathbf{r})}(P + Q) \geq \min\{\operatorname{ind}_{(\mathbf{q};\mathbf{r})} P, \operatorname{ind}_{(\mathbf{q};\mathbf{r})} Q\}$

3. $\operatorname{ind}_{(\mathbf{q};\mathbf{r})}(PQ) = \operatorname{ind}_{(\mathbf{q};\mathbf{r})} P + \operatorname{ind}_{(\mathbf{q};\mathbf{r})} Q$

Proof. 1. Let $\mathbf{i} = (i_1, \ldots, i_m) \in \mathbb{Z}^m_{\geq 0}$ be a given vector. As seen in Lemma 3.4.1, suppose, $T(x_1, \ldots, x_m) = P_{\mathbf{i}}(x_1, \ldots, x_m) \in \mathbb{Z}[x_1, \ldots, x_m]$.

Now, let $\mathbf{j} = (j_1, \ldots, j_m) \in \mathbb{Z}^m_{\geq 0}$ be the point for which $T_{\mathbf{j}}(q_1, \ldots, q_m) \neq 0$, then

$$\begin{aligned}
T_{\mathbf{j}}(x_1, \ldots, x_m) &= \frac{1}{j_1! \cdots j_m!} \frac{\partial^{j_1 + \ldots + j_m}}{\partial x_1^{j_1} \cdots \partial x_m^{j_m}} T(x_1, \ldots, x_m) \\
&= \frac{1}{j_1! \cdots j_m!} \frac{\partial^{j_1 + \ldots + j_m}}{\partial x_1^{j_1} \cdots \partial x_m^{j_m}} P_{\mathbf{i}}(x_1, \ldots, x_m) \\
&= \frac{1}{j_1! \cdots j_m!} \frac{\partial^{j_1 + \ldots + j_m}}{\partial x_1^{j_1} \cdots \partial x_m^{j_m}} \\
&\quad \left(\frac{1}{i_1! \ldots i_m!} \frac{\partial^{i_1 + \ldots + i_m}}{\partial x_1^{i_1} \cdots \partial x_m^{i_m}} P(x_1, \ldots, x_m) \right) \\
&= \frac{1}{i_1! j_1! \ldots i_m! j_m!} \frac{\partial^{i_1 + j_1}}{\partial x_1^{i_1 + j_1}} \cdots \frac{\partial^{i_m + j_m}}{\partial x_m^{i_m + j_m}} P(x_1, \ldots, x_m)
\end{aligned}$$

But,

$$\begin{aligned}
P_{\mathbf{i}+\mathbf{j}}(x_1, \ldots, x_m) &= \frac{1}{(i_1 + j_1)! \cdots (i_m + j_m)!} \\
&\quad \frac{\partial^{i_1 + j_1}}{\partial x_1^{i_1 + j_1}} \cdots \frac{\partial^{i_m + j_m}}{\partial x_m^{i_m + j_m}} P(x_1, \ldots, x_m) \\
&= c_1(i_1, j_1) \cdots c_m(i_m, j_m) T_{\mathbf{j}}(x_1, \ldots, x_m)
\end{aligned}$$

where $c_1(i_1, j_1), \ldots, c_m(i_m, j_m)$ are non-zero constants.

Since $T_{\mathbf{j}}(q_1, \ldots, q_m) \neq 0$, we have, $P_{\mathbf{i}+\mathbf{j}}(q_1, \ldots, q_m) \neq 0$, thus from definition of $\operatorname{ind}_{(\mathbf{q};\mathbf{r})} P_{\mathbf{i}+\mathbf{j}}$, we have

$$\frac{i_1 + j_1}{r_1} + \ldots + \frac{i_m + j_m}{r_m} \geq \operatorname{ind}_{(\mathbf{q};\mathbf{r})} P$$

$$\Rightarrow \frac{j_1}{r_1} + \ldots + \frac{j_m}{r_m} \geq \operatorname{ind}_{(\mathbf{q};\mathbf{r})} P - \left(\frac{i_1}{r_1} + \ldots + \frac{i_m}{r_m}\right)$$

Since this equation is true for all $\mathbf{j}$ such that $T_{\mathbf{j}}(q_1, \ldots, q_m) \neq 0$, we conclude that

$$\operatorname{ind}_{(\mathbf{q};\mathbf{r})} T \geq \operatorname{ind}_{(\mathbf{q};\mathbf{r})} P - \left(\frac{i_1}{r_1} + \ldots + \frac{i_m}{r_m}\right)$$

$$\Rightarrow \operatorname{ind}_{(\mathbf{q};\mathbf{r})} P_{\mathbf{i}} \geq \operatorname{ind}_{(\mathbf{q};\mathbf{r})} P - \left(\frac{i_1}{r_1} + \ldots + \frac{i_m}{r_m}\right)$$

2. Let $\mathbf{i} = (i_1, \ldots, i_m) \in \mathbb{Z}^m_{\geq 0}$ be a point such that

$$(P + Q)_{\mathbf{i}}(q_1, \ldots, q_m) \neq 0$$

$$\Rightarrow P_{\mathbf{i}}(q_1, \ldots, q_m) + Q_{\mathbf{i}}(q_1, \ldots, q_m) \neq 0$$

$$\Rightarrow P_{\mathbf{i}}(q_1, \ldots, q_m) \neq 0 \quad \text{or} \quad Q_{\mathbf{i}}(q_1, \ldots, q_m) \neq 0$$

$$\Rightarrow \frac{i_1}{r_1} + \ldots + \frac{i_m}{r_m} \geq \operatorname{ind}_{(\mathbf{q};\mathbf{r})} P \quad \text{or} \quad \frac{i_1}{r_1} + \ldots + \frac{i_m}{r_m} \geq \operatorname{ind}_{(\mathbf{q};\mathbf{r})} Q$$

Since, this is true for all $\mathbf{i}$ such that $(P + Q)_{\mathbf{i}}(q_1, \ldots, q_m) \neq 0$, we get

$$\operatorname{ind}_{(\mathbf{q};\mathbf{r})}(P + Q) \geq \operatorname{ind}_{(\mathbf{q};\mathbf{r})} P \quad \text{or} \quad \operatorname{ind}_{(\mathbf{q};\mathbf{r})}(P + Q) \geq \operatorname{ind}_{(\mathbf{q};\mathbf{r})} Q$$

$$\Rightarrow \operatorname{ind}_{(\mathbf{q};\mathbf{r})}(P + Q) \geq \min\{\operatorname{ind}_{(\mathbf{q};\mathbf{r})} P, \operatorname{ind}_{(\mathbf{q};\mathbf{r})} Q\}$$

3. To prove given statement we will prove two statements:

$$\begin{cases} \operatorname{ind}_{(\mathbf{q};\mathbf{r})}(PQ) \geq \operatorname{ind}_{(\mathbf{q};\mathbf{r})} P + \operatorname{ind}_{(\mathbf{q};\mathbf{r})} Q \\ \operatorname{ind}_{(\mathbf{q};\mathbf{r})}(PQ) \leq \operatorname{ind}_{(\mathbf{q};\mathbf{r})} P + \operatorname{ind}_{(\mathbf{q};\mathbf{r})} Q \end{cases}$$

Firstly we will prove: $\operatorname{ind}_{(\mathbf{q};\mathbf{r})}(PQ) \geq \operatorname{ind}_{(\mathbf{q};\mathbf{r})} P + \operatorname{ind}_{(\mathbf{q};\mathbf{r})} Q$
Let, $\mathbf{i} = (i_1, \ldots, i_m) \in \mathbb{Z}^m_{\geq 0}$ be a point such that

$$\frac{i_1}{r_1} + \ldots + \frac{i_m}{r_m} = \operatorname{ind}_{(\mathbf{q};\mathbf{r})}(PQ)$$

$$\Rightarrow (PQ)_{\mathbf{i}}(q_1, \ldots, q_m) \neq 0$$

Now by Leibnitz's rule[8] we have:

$$(PQ)_{\mathbf{i}}(x_1,\ldots,x_m) = \sum_{\substack{\mathbf{j},\mathbf{k} \\ \text{with } \mathbf{j}+\mathbf{k}=\mathbf{i}}} c(\mathbf{j},\mathbf{k}) P_{\mathbf{j}} Q_{\mathbf{k}}(x_1,\ldots,x_m)$$

where $c(\mathbf{j},\mathbf{k})$ is a constant which depends on $\mathbf{j}$ and $\mathbf{k}$.

Since $(PQ)_{\mathbf{i}}(q_1,\ldots,q_m) \neq 0$, we have

$$\sum_{\substack{\mathbf{j},\mathbf{k} \\ \text{with } \mathbf{j}+\mathbf{k}=\mathbf{i}}} c(\mathbf{j},\mathbf{k}) P_{\mathbf{j}}(q_1,\ldots,q_m) Q_{\mathbf{k}}(q_1,\ldots,q_m) \neq 0$$

Thus, there exist $\mathbf{j},\mathbf{k} \in \mathbb{Z}^m_{\geq 0}$ such that $\mathbf{j}+\mathbf{k}=\mathbf{i}$ and both $P_{\mathbf{j}}(q_1,\ldots,q_m)$ and $Q_{\mathbf{k}}(q_1,\ldots,q_m)$ are not zero. Hence,

$$\frac{j_1}{r_1}+\ldots+\frac{j_m}{r_m} \geq \operatorname{ind}_{(\mathbf{q};\mathbf{r})} P \quad \text{and} \quad \frac{k_1}{r_1}+\ldots+\frac{k_m}{r_m} \geq \operatorname{ind}_{(\mathbf{q};\mathbf{r})} Q$$

$$\Rightarrow \frac{j_1+k_1}{r_1}+\ldots+\frac{j_m+k_m}{r_m} \geq \operatorname{ind}_{(\mathbf{q};\mathbf{r})} P + \operatorname{ind}_{(\mathbf{q};\mathbf{r})} Q$$

$$\Rightarrow \frac{i_1}{r_1}+\ldots+\frac{i_m}{r_m} \geq \operatorname{ind}_{(\mathbf{q};\mathbf{r})} P + \operatorname{ind}_{(\mathbf{q};\mathbf{r})} Q$$

for all $\mathbf{i}=(i_1,\ldots,i_m)$ with $(P,Q)_{\mathbf{i}}(q_1,\ldots,q_m) \neq 0$

$$\Rightarrow \operatorname{ind}_{(\mathbf{q};\mathbf{r})}(PQ) \geq \operatorname{ind}_{(\mathbf{q};\mathbf{r})} P + \operatorname{ind}_{(\mathbf{q};\mathbf{r})} Q$$

Now we will prove: $\operatorname{ind}_{(\mathbf{q};\mathbf{r})}(PQ) \leq \operatorname{ind}_{(\mathbf{q};\mathbf{r})} P + \operatorname{ind}_{(\mathbf{q};\mathbf{r})} Q$

Let the points $\mathbf{j}=(j_1,\ldots,j_m) \in \mathbb{Z}^m_{\geq 0}$ and $\mathbf{k}=(k_1,\ldots,k_m) \in \mathbb{Z}^m_{\geq 0}$ be such that

$$\frac{j_1}{r_1}+\ldots+\frac{j_m}{r_m} = \operatorname{ind}_{(\mathbf{q};\mathbf{r})} P \quad \text{and} \quad \frac{k_1}{r_1}+\ldots+\frac{k_m}{r_m} = \operatorname{ind}_{(\mathbf{q};\mathbf{r})} Q$$

$$\Rightarrow P_{\mathbf{j}}(q_1,\ldots,q_m) \neq 0 \quad \text{and} \quad Q_{\mathbf{k}}(q_1,\ldots,q_m) \neq 0$$

Let, $\mathbf{i}=(i_1,\ldots,i_m)$ be such that $i_\ell = j_\ell + k_\ell$ for all $\ell = 1,2,\ldots,m$.

Now, we claim that $(PQ)_{\mathbf{i}}(q_1,\ldots,q_m) \neq 0$

[8] If $f_1,\ldots,f_m$ are differentiable functions, then

$$(f_1 f_2 \cdots f_m)^{(n)} = \sum_{k_1+k_2+\cdots+k_m=n} \binom{n}{k_1,k_2,\ldots,k_m} \prod_{1\leq t\leq m} f_t^{(k_t)}$$

where the sum extends over all m-tuples $(k_1,\ldots,k_m)$ of non-negative integers with $\sum_{t=1}^m k_t = n$ (see: Olver, P. J., Applications of Lie Groups to Differential Equations (Springer-Verlag New York, 1993), pp. 318.)

By definition of $\text{ind}_{(\mathbf{q};\mathbf{r})}\, P$ for any $(j'_1, \ldots, j'_m) \in \mathbb{Z}^m_{\geq 0}$, if we have

$$\frac{j'_1}{r_1} + \ldots + \frac{j'_m}{r_m} < \frac{j_1}{r_1} + \ldots + \frac{j_m}{r_m}$$

then $P_{\mathbf{j}'}(q_1, \ldots, q_m) = 0$ where $\mathbf{j}' = (j'_1, \ldots, j'_m)$.

If

$$\frac{j'_1}{r_1} + \ldots + \frac{j'_m}{r'_m} > \frac{j_1}{r_1} + \ldots + \frac{j_m}{r_m}$$

and

$$(k'_1, \ldots, k'_m) = (i_1 - j'_1, \ldots, i_m - j'_m)$$

then we claim that

$$\frac{k'_1}{r_1} + \ldots + \frac{k'_m}{r_m} < \frac{k_1}{r_1} + \ldots + \frac{k_m}{r_m}$$

But,

$$\begin{aligned}
\frac{k'_1}{r_1} + \ldots + \frac{k'_m}{r_m} &= \frac{i_1 - j'_1}{r_1} + \ldots + \frac{i_m - j'_m}{r_m} \\
&= \frac{j_1 + k_1 - j'_1}{r_1} + \ldots + \frac{j_m + k_m - j'_m}{r_m} \\
&= \frac{k_1}{r_1} + \ldots + \frac{k_m}{r_m} + \underbrace{\left(\frac{j_1 - j'_1}{r_1} + \ldots + \frac{j_m - j'_m}{r_1}\right)}_{\substack{\text{this is negative} \\ \text{due to our assumption}}}
\end{aligned}$$

Thus, our claim was true. Hence, by definition of $\text{ind}_{(\mathbf{q};\mathbf{r})}\, Q$ we have $Q_{\mathbf{k}'}(q_1, \ldots, q_m) = 0$, where $\mathbf{k}' = (k'_1, \ldots, k'_m)$

Thus, either $P_{\mathbf{j}'}(q_1, \ldots, q_m) = 0$ or $Q_{\mathbf{k}'}(q_1, \ldots, q_m) = 0$, leading to :

$$(PQ)_{\mathbf{i}}(q_1, \ldots, q_m) = P_{\mathbf{j}}(q_1, \ldots, q_m) Q_{\mathbf{k}}(q_1, \ldots, q_m) \neq 0$$

Hence proving our claim and completing the proof.

□

Theorem 3.4.1 (Index Theorem)**.** *Suppose that q is an algebraic integer of degree d, $d \geq 2$ and m is an integer satisfying the inequality*

$$m > 16\varepsilon^{-2} \log(4d)$$

where ε is some positive real number. If $r_1, \ldots, r_m$ are positive integers, then there exists a polynomial $P(x_1, \ldots, x_m) \neq 0$ with rational integers coefficients such that

1. $\deg_P x_h \leq r_h$, *where* $1 \leq h \leq m$

2. $\mathrm{ind}_{(\mathbf{q};\mathbf{r})}\, P \geq \dfrac{m}{2}(1-\varepsilon)$, *where* $(\mathbf{q};\mathbf{r}) = (\underbrace{q,\ldots,q}_{m\ times};r_1,\ldots,r_m)$

3. $[\![P]\!] \leq H^{r_1+\ldots+r_m}$, *where* H *depends only on* q *i.e.* $H = H(q)$

Proof. We wish to find a polynomial

$$P(x_1,\ldots,x_m) = \sum_{j_1=0}^{r_1} \cdots \sum_{j_m=0}^{r_m} k(j_1,\ldots,j_m) x_1^{j_1}\ldots x_m^{j_m}$$

with rational integer coefficients $k(j_1,\ldots,j_m)$ such that given conditions *2.* and *3.* hold.

We need to determine all the coefficients, hence we have to determine

$$N = (1+r_1)\cdots(1+r_m)$$

integers.

By *2.* we need

$$P_{\mathbf{i}}(q,\ldots,q) = 0 \qquad \text{when} \qquad \left(\sum_{h=1}^{m} \frac{i_h}{r_h}\right) - \frac{m}{2} < -m\frac{\varepsilon}{2} \tag{3.12}$$

As per Lemma 3.4.1,

$$\Rightarrow \sum_{\substack{j_1,\ldots,j_m \\ 0\leq j_h\leq r_h}} k(j_1,\ldots,j_m)\binom{j_1}{i_1}\cdots\binom{j_m}{i_m} q^{(j_1-i_1)+\ldots+(j_m-i_m)} = 0 \tag{3.13}$$

By replacing ε by $\varepsilon/2$ in Lemma 3.3.4, the number of such $m-$tuples $\mathbf{i}$ is at most

$$M' = (1+r_1)\cdots(1+r_m)\cdot e^{-\varepsilon^2 m/16}$$

But, $m > 16\varepsilon^{-2}\log(4d)$, hence the number of conditions in (3.12) is at most

$$M' = N \times \frac{2}{4d} = \frac{N}{2d}$$

for $m = \lfloor 16\varepsilon^{-2}\log(4d)\rfloor + 1$

Each condition (3.12) is a linear equation in the coefficients $k(j_1,\ldots,j_m)$. The coefficients of these equations will be rational integers times powers of q, hence will be algebraic. But each power of q is a linear combination of $1, q, \ldots, q^{d-1}$ with rational integer coefficients. Hence each condition (3.12) follows from d linear relations in $k(j_1,\ldots,j_m)$ with rational coefficients. Thus, we have the number of linear equations for the $k(j_1,\ldots,j_m)$ with rational coefficients

$$M \leq d \times M' = \frac{N}{2} \tag{3.14}$$

Now we will apply Lemma 3.4.4 to (3.13). Let Q be the maximum of the absolute values of all rational integer coefficients corresponding to linear equations in each condition (3.12), then

$$Q \leq \binom{j_1}{i_1} \cdots \binom{j_m}{i_m} (\llbracket P' \rrbracket + 1)^{(j_1 - i_1) + \ldots + (j_m - i_m)}$$

where P' is the minimal polynomial for q. By combinatorial inequality $\binom{j}{i} \leq 2^j$, we can say

$$\begin{aligned} Q &\leq 2^{j_1 + \ldots + j_m} (\llbracket P' \rrbracket + 1)^{(j_1 - i_1) + \ldots + (j_m - i_m)} \\ &\leq 2^{r_1 + \ldots + r_m} (\llbracket P' \rrbracket + 1)^{r_1 + \ldots + r_m} \qquad \text{(follows from } \textit{1.}\text{)} \\ &= \left(2 \left(\llbracket P' \rrbracket + 1\right)\right)^{r_1 + \ldots + r_m} \end{aligned}$$

Further, by Siegel's Lemma 3.4.3 and (3.14) our system of equations has non-trivial integer solution with

$$|k(j_1, \ldots, j_m)| \leq \lfloor (NQ)^{\frac{M}{N-M}} \rfloor \leq NQ$$

Also, $N \leq 2^{r_1 + \ldots + r_m}$ and $Q \leq \left(2 \left(\llbracket P' \rrbracket + 1\right)\right)^{r_1 + \ldots + r_m}$ we get:

$$|k(j_1, \ldots, j_m)| \leq \left(4 \left(\llbracket P' \rrbracket + 1\right)\right)^{r_1 + \ldots + r_m}$$

for each $m-$tuple $(j_1, \ldots, j_m)$. Hence the height of P satisfies

$$\llbracket P \rrbracket \leq \left(4 \left(\llbracket P' \rrbracket + 1\right)\right)^{r_1 + \ldots + r_m}$$

$$\Rightarrow \llbracket P \rrbracket \leq H^{r_1 + \ldots + r_m}$$

where H is a function of q since it depends on minimal polynomial for q. □

Theorem 3.4.2 (Index of polynomial at rational points near algebraic-integer point)**.** *Consider the real numbers δ and ε such that $0 < \delta < 1$ and $0 < \varepsilon < \frac{\delta}{36}$. Let q be an algebraic integer of degree d, $d \geq 2$ and m is an integer satisfying $m > 16\varepsilon^{-2} \log(4d)$. Also given to us is a $m-$tuple $\mathbf{r} = (r_1, \ldots, r_m) \in \mathbb{Z}^m_{\geq 1}$ and a polynomial*

$$P(x_1, \ldots, x_m) \in \mathbb{Z}[x_1, \ldots, x_m]$$

satisfying the conditions of Theorem 3.4.1.

Suppose there are m distinct rational numbers

$$\left\{ \frac{a_1}{b_1}, \ldots, \frac{a_m}{b_m} \right\} \quad \textit{such that} \quad \left| q - \frac{a_h}{b_h} \right| < \frac{1}{b_h^{2+\delta}} \quad \textit{with } b_h^{\delta} > D$$

for some constant $D = D(q)$ (depends only on q).

If $b_1^{r_1} \leq b_h^{r_h} \leq b_1^{(1+\varepsilon) r_1}$ for all $h = 1, 2, \ldots, m$, then $\operatorname{ind}_{(\mathbf{a};\mathbf{r})} P \geq m\varepsilon$ where $\mathbf{a} = \left(\frac{a_1}{b_1}, \ldots, \frac{a_m}{r_m} \right)$.

Proof. We have to prove

$$\min_{\substack{\mathbf{i}=(i_1,\ldots,i_m)\in\mathbb{Z}^m_{\geq 0}\\ 0\leq i_k\leq \deg_P x_i}} \left\{ \frac{i_1}{r_1}+\ldots+\frac{i_m}{r_m} : P_{\mathbf{i}}\left(\frac{a_1}{b_1},\ldots,\frac{a_m}{b_m}\right)\neq 0 \right\} \geq m\varepsilon$$

where, $\deg_P x_i$ = maximum degree of x_i in some monomial of P.
We will rather prove its contrapositive, i.e. *for any* $\mathbf{i}=(i_1,\ldots,i_m)\in\mathbb{Z}^m_{\geq 0}$, *satisfying* $\frac{i_1}{r_1}+\ldots+\frac{i_m}{r_m}<m\varepsilon$, *we have* $P_{\mathbf{i}}\left(\frac{a_1}{b_1},\ldots,\frac{a_m}{r_m}\right)=0$.

Let, $\mathbf{i}=(i_1,\ldots,i_m)\in\mathbb{Z}^m_{\geq 0}$ be an $m-$tuple satisfying $\frac{i_1}{r_1}+\ldots+\frac{i_m}{r_m}<m\varepsilon$. Also, let $T(x_1,\ldots,x_m)=P_{\mathbf{i}}(x_1,\ldots,x_m)$, now we have to show that

$$T\left(\frac{a_1}{b_1},\ldots,\frac{a_m}{b_m}\right)=0$$

Since from Lemma 3.4.1,

$$P_{\mathbf{i}}(x_1,\ldots,x_m)=\sum_{\substack{j_1,\ldots,j_m\\ 0\leq j_k\leq r_k}} k(j_1,\ldots,j_m)\prod_{h=1}^{m}\binom{j_h}{i_h}x_h^{j_h-i_h}$$

we get,

$$P_{\mathbf{i}}\left(\frac{a_1}{b_1},\ldots,\frac{a_m}{b_m}\right)=\sum_{\substack{j_1,\ldots,j_m\\ 0\leq j_h\leq r_h}} k(j_1,\ldots,j_m)\prod_{h=1}^{m}\binom{j_h}{i_h}\left(\frac{a_h}{b_h}\right)^{j_h-i_h}$$

$$\Rightarrow \left|P_{\mathbf{i}}\left(\frac{a_1}{b_1},\ldots,\frac{a_m}{b_m}\right)\right|=\frac{N'}{b_1^{r_1}\cdots b_m^{r_m}} \tag{3.15}$$

for some integer $N'\geq 0$

Now, if we prove

$$\left|P_{\mathbf{i}}\left(\frac{a_1}{b_1},\ldots,\frac{a_m}{b_m}\right)\right|<\frac{1}{b_1^{r_1}\cdots b_m^{r_m}} \tag{3.16}$$

then from (3.15) and (3.16) we get:

$$\frac{N'}{b_1^{r_1}\cdots b_m^{r_m}}=\left|P_{\mathbf{i}}\left(\frac{a_1}{b_1},\ldots,\frac{a_m}{b_m}\right)\right|<\frac{1}{b_1^{r_1}\cdots b_m^{r_m}}$$

leading to $N'=0$ and hence,

$$P_{\mathbf{i}}\left(\frac{a_1}{b_1},\ldots,\frac{a_m}{b_m}\right)=0$$

Hence it is enough to prove that

$$\left|T\left(\frac{a_1}{b_1},\ldots,\frac{a_m}{b_m}\right)\right|=\left|P_{\mathbf{i}}\left(\frac{a_1}{b_1},\ldots,\frac{a_m}{b_m}\right)\right|<\frac{1}{b_1^{r_1}\cdots b_m^{r_m}}$$

By Lemma 3.4.6(*1.*), with $\mathbf{q} = (q, \ldots, q)$ as in Theorem 3.4.1,

$$\operatorname{ind}_{(\mathbf{q};\mathbf{r})} P_{\mathbf{i}} \geq \operatorname{ind}_{(\mathbf{q};\mathbf{r})} P - \left(\frac{i_1}{r_1} + \ldots + \frac{i_m}{r_m}\right)$$

$$\Rightarrow \operatorname{ind}_{(\mathbf{q};\mathbf{r})} T \geq \operatorname{ind}_{(\mathbf{q};\mathbf{r})} P - \left(\frac{i_1}{r_1} + \ldots + \frac{i_m}{r_m}\right)$$

Also from Theorem 3.4.1 we have:

$$\operatorname{ind}_{(\mathbf{q};\mathbf{r})} P \geq \frac{m}{2}(1 - \varepsilon)$$

and as per our assumption on $\mathbf{i}$, we have:

$$\frac{i_1}{r_1} + \ldots + \frac{i_m}{r_m} < m\varepsilon$$

we get:

$$\operatorname{ind}_{(\mathbf{q};\mathbf{r})} T \geq \frac{m}{2}(1 - \varepsilon) - m\varepsilon$$

$$\Rightarrow \operatorname{ind}_{(\mathbf{q};\mathbf{r})} T \geq \frac{m}{2}(1 - 3\varepsilon) \tag{3.17}$$

The Taylor series expansion (generalizing what we did in Theorem 3.1.1) of $T(x_1, \ldots, x_m)$ about $\mathbf{q} = (q, \ldots, q)$ we get:

$$T(x_1, \ldots, x_m) = \sum_{t_1=0}^{r_1} \cdots \sum_{t_m=0}^{r_m} T_{\mathbf{t}}(q, \ldots, q)(x_1 - q)^{t_1} \cdots (x_m - q)^{t_m}$$

where $\mathbf{t} = (t_1, \ldots, t_m) \in \mathbb{Z}^m_{\geq 0}$. Evaluating value about $\mathbf{a} = \left(\frac{a_1}{b_1}, \ldots, \frac{a_m}{b_m}\right)$ we get:

$$T\left(\frac{a_1}{b_1}, \ldots, \frac{a_m}{b_m}\right) = \sum_{t_1=0}^{r_1} \cdots \sum_{t_m=0}^{r_m} T_{\mathbf{t}}(q, \ldots, q) \left(\frac{a_1}{b_1} - q\right)^{t_1} \cdots \left(\frac{a_m}{b_m} - q\right)^{t_m} \tag{3.18}$$

Now, we want to estimate right hand side of this equation. Therefore we get:

$$\left|T\left(\frac{a_1}{b_1}, \ldots, \frac{a_m}{b_m}\right)\right| \leq \sum_{\substack{t_1,\ldots,t_m \\ 0 \leq t_h \leq r_h}} |T_{\mathbf{t}}(q, \ldots, q)| \prod_{h=1}^{m} \left|\frac{a_h}{b_h} - q\right|^{t_h}$$

Now, to estimate $|T_{\mathbf{t}}(q, \ldots, q)|$ we need to know the estimate of $[\![T_{\mathbf{t}}]\!]$, number of terms in $T_{\mathbf{t}}$ and highest power of $|q|$.

But, from Lemma 3.4.2 we know that

$$[\![P_{\mathbf{i}}]\!] \leq 2^{r_1+\ldots+r_m} [\![P]\!]$$

$$\Rightarrow [\![T]\!] \leq 2^{r_1+\ldots+r_m} [\![P]\!] \quad \text{and} \quad [\![T_{\mathbf{t}}]\!] \leq 2^{r_1+\ldots+r_m} [\![T]\!]$$

leading to

$$[\![T_{\mathbf{t}}]\!] \leq 4^{r_1+\ldots+r_m}[\![P]\!] \tag{3.19}$$

Also from simple combinatorics we know that

$$\#(\text{terms in } T_{\mathbf{t}}) \ \leq (r_1+1)\cdots(r_m+1) \leq 2^{r_1+\ldots+r_m} \tag{3.20}$$

Since, $|q| \geq 1$ or $|q| < 1$, we can take the estimate $\max\{1,|q|\}^{r_1+\ldots+r_m}$ for highest power of $|q|$. By using this along with (3.19) and (3.20) get

$$\begin{aligned} &|T_{\mathbf{t}}(q,\ldots,q)| \leq \left(4^{r_1+\ldots+r_m}[\![P]\!]\right)\left(2^{r_1+\ldots+r_m}\right)\max\{1,|q|\}^{r_1+\ldots+r_m} \\ &\Rightarrow |T_{\mathbf{t}}(q,\ldots,q)| \leq C^{r_1+\ldots+r_m} \quad \text{where} \quad C = 8\max\{1,|q|\}[\![P]\!]^{\frac{1}{r_1+\ldots+r_m}} \end{aligned} \tag{3.21}$$

But, we are given in statement of theorem that

$$\begin{aligned} &\left|\frac{a_h}{b_h} - q\right|^{t_h} < \left(\frac{1}{b_h^{2+\delta}}\right)^{t_h} \quad \forall h = 1,2,\ldots,m \\ &\Rightarrow \left|\frac{a_h}{b_h} - q\right|^{t_h} < \left(\frac{1}{b_h^{t_h}}\right)^{2+\delta} \quad \forall h = 1,2,\ldots,m \end{aligned} \tag{3.22}$$

Also, (3.17) implies that

$$\operatorname{ind}_{(\mathbf{q};\mathbf{r})} T \geq m\left(\frac{1}{2} - 2\varepsilon\right)$$

which further implies that any $\mathbf{t} = (t_1,\ldots,t_m) \in \mathbb{Z}^m_{\geq 0}$ with $\frac{t_1}{r_1} + \ldots + \frac{t_m}{r_m} \leq m\left(\frac{1}{2} - 2\varepsilon\right)$ we have $T_{\mathbf{t}}(q,\ldots,q) = 0$. Using this along with (3.21) and (3.22) in (3.18) we get:

$$\left|T\left(\frac{a_1}{b_1},\ldots,\frac{a_m}{b_m}\right)\right| \leq \sum_{\substack{t_1,\ldots,t_m \\ 0\leq t_h\leq r_h \\ \frac{t_1}{r_1}+\ldots+\frac{t_m}{r_m} > m\left(\frac{1}{2}-2\varepsilon\right)}} C^{r_1+\ldots+r_m}\frac{1}{\left(b_1^{t_1}\cdots b_m^{t_m}\right)^{2+\delta}} \tag{3.23}$$

Further for $\frac{t_1}{r_1}+\ldots+\frac{t_m}{r_m} > m\left(\frac{1}{2}-2\varepsilon\right)$ we can write,

$$\begin{aligned}
b_1^{t_1}\cdots b_m^{t_m} &= b_1^{r_1\left(\frac{t_1}{r_1}\right)} b_2^{r_2\left(\frac{t_2}{r_2}\right)}\cdots b_m^{r_m\left(\frac{t_m}{r_m}\right)} \\
&\geq b_1^{r_1\left(\frac{t_1}{r_1}\right)} b_1^{r_1\left(\frac{t_2}{r_2}\right)}\cdots b_1^{r_1\left(\frac{t_m}{r_m}\right)} \quad \text{(given: } b_1^{r_1}\leq b_h^{r_h}\text{)} \\
&= b_1^{r_1\left(\frac{t_1}{r_1}+\ldots+\frac{t_m}{r_m}\right)} \\
&\geq b_1^{r_1 m\left(\frac{1}{2}-2\varepsilon\right)} \\
&= \underbrace{\left(b_1^{r_1}\cdots b_1^{r_1}\right)}_{\text{m times}}{}^{\left(\frac{1}{2}-2\varepsilon\right)} \\
&\geq \left(b_1^{\frac{r_1}{1+\varepsilon}}\cdots b_m^{\frac{r_m}{1+\varepsilon}}\right)^{\left(\frac{1}{2}-2\varepsilon\right)} \quad \text{(given: } b_h^{r_h}\leq b_1^{(1+\varepsilon)r_1}\text{)} \\
&= \left(b_1^{r_1}\cdots b_m^{r_m}\right)^{\left(\frac{\frac{1}{2}-2\varepsilon}{1+\varepsilon}\right)}
\end{aligned}$$

Further, we have

$$\frac{\frac{1}{2}-2\varepsilon}{1+\varepsilon} = \frac{1}{2}\left(\frac{1-4\varepsilon}{1+\varepsilon}\right) = \frac{1}{2}\left(1-\frac{5\varepsilon}{1+\varepsilon}\right) \geq \frac{1}{2}(1-6\varepsilon)$$

Thus for all $\mathbf{t}$ with $\frac{t_1}{r_1}+\ldots+\frac{t_m}{r_m} > m\left(\frac{1}{2}-2\varepsilon\right)$ we have

$$b_1^{t_1}\cdots b_m^{t_m} \geq \left(b_1^{r_1}\cdots b_m^{r_m}\right)^{\frac{1}{2}(1-6\varepsilon)} \tag{3.24}$$

From (3.23) and (3.24) we get

$$\begin{aligned}
\left|T\left(\frac{a_1}{b_1},\ldots,\frac{a_m}{b_m}\right)\right| &\leq (2C)^{r_1+\ldots+r_m}\left(b_1^{r_1}\cdots b_m^{r_m}\right)^{-\frac{1}{2}(1-6\varepsilon)(2+\delta)} \\
&= \prod_{h=1}^{m}\left(2Cb_h^{-\frac{1}{2}(1-6\varepsilon)(2+\delta)}\right)^{r_h}
\end{aligned}$$

Note that we are given $0<\delta<1$ and $0<\varepsilon<\frac{\delta}{36}$, so

$$\frac{1}{2}(1-6\varepsilon)(2+\delta) = \frac{2+\delta-12\varepsilon-6\delta\varepsilon}{2} > 1+\frac{\delta-\delta/3-\delta^2/6}{2}$$

$$\Rightarrow \frac{1}{2}(1-6\varepsilon)(2+\delta) > 1+\delta\left(\frac{4-\delta}{12}\right) > 1+\delta\left(\frac{4-1}{12}\right)$$

$$\Rightarrow \frac{1}{2}(1-6\varepsilon)(2+\delta) > 1+\frac{\delta}{4}$$

Hence,

$$\left|T\left(\frac{a_1}{b_1},\ldots,\frac{a_m}{b_m}\right)\right| \leq \prod_{h=1}^{m}\left(2Cb_h^{-\left(1+\frac{\delta}{4}\right)}\right)^{r_h}$$

Now,

$$2Cb_h^{-\left(1+\frac{\delta}{4}\right)} < b_h^{-1}$$
$$\Leftrightarrow (2C)^4 < b_h^{\delta}$$
$$\Leftrightarrow D < b_h^{\delta} \quad \text{given in statement of theorem}$$

where $D = (2C)^4 = 2^4 \left(8 \max\{1, |q|\}[\![P]\!]^{\frac{1}{r_1+\ldots+r_m}}\right)^4$, hence $D = D(q)$ and we get as desired:

$$\left| T\left(\frac{a_1}{b_1}, \ldots, \frac{a_m}{b_m}\right) \right| \leq \prod_{h=1}^{m} b_h^{-r_h}$$

□

3.5 Wrońskians and Linear Independence of Polynomials

Wrońskian is a determinant introduced by Polish mathematician Józef Hoene-Wroński (1812) and named by Scottish mathematician Thomas Muir (1882). It is used in the study of ordinary differential equations, where it can sometimes show linear independence in a set of solutions.

Firstly let's see "Why the Wrońskian work?"[9]

For illustration, let's work with 3×3 system. Consider functions f, g, h. Then they are linearly dependent on some set of real numbers I if we can find $a, b, c \in \mathbb{R}$ (not all zero) such that $af(t) + bg(t) + ch(t) = 0$ for all t in I. If we differentiate this again and again, we'll get other equations:

$$\begin{aligned} af(t) + bg(t) + ch(t) &= 0 \\ af'(t) + bg'(t) + ch'(t) &= 0 \\ af''(t) + bg''(t) + ch''(t) &= 0 \end{aligned}$$

Let

$$\mathbf{f}_1(t) = \begin{bmatrix} f(t) \\ f'(t) \\ f''(t) \end{bmatrix}, \qquad \mathbf{f}_2(t) = \begin{bmatrix} g(t) \\ g'(t) \\ g''(t) \end{bmatrix}, \qquad \text{and} \qquad \mathbf{f}_3(t) = \begin{bmatrix} h(t) \\ h'(t) \\ h''(t) \end{bmatrix}$$

be vectors of functions (i.e. functions from $\mathbb{R}$ to $\mathbb{R}^3$).

This leads to the discussion about linear independence in reference to the set:

$$\left\{ \begin{bmatrix} f(t) \\ f'(t) \\ f''(t) \end{bmatrix}, \begin{bmatrix} g(t) \\ g'(t) \\ g''(t) \end{bmatrix}, \begin{bmatrix} h(t) \\ h'(t) \\ h''(t) \end{bmatrix} \right\}$$

[9] Bill Cook (http://math.stackexchange.com/users/16423/bill-cook), Linear independence of function vectors and Wronskians, URL (version: 2012-01-07): http://math.stackexchange.com/q/97094

We say the set $\{\mathbf{f}_1(t), \mathbf{f}_2(t), \mathbf{f}_3(t)\}$ is linearly dependent on $I \subseteq \mathbb{R}$, if there exist $c_1, c_2, c_3 \in \mathbb{R}$ (not all zero) such that $c_1\mathbf{f}_1(t) + c_2\mathbf{f}_2(t) + c_3\mathbf{f}_3(t) = \mathbf{0}$ for all $t \in I$.

This equation can be restated in terms of matrices. We have linear dependence if and only if there exists some constant vector $\mathbf{c} \neq \mathbf{0}$ such that $\mathbf{F}(t)\mathbf{c} = \mathbf{0}$ for all $t \in I$. This is where $\mathbf{F}(t) = [\mathbf{f}_1(t)\ \mathbf{f}_2(t)\ \mathbf{f}_3(t)]$. Or writing it out in a more expanded form:

$$\mathbf{F}(t)\mathbf{c} = \begin{bmatrix} f(t) & g(t) & h(t) \\ f'(t) & g'(t) & h'(t) \\ f''(t) & g''(t) & h''(t) \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

Now the determinant of $\mathbf{F}(t)$ is known as the Wronskian of the functions $\mathbf{f}_1, \mathbf{f}_2, \mathbf{f}_3$. That is $W(t) = \det(\mathbf{F})(t)$.

To show the columns of $\mathbf{F}$ are linearly dependent[10] we need there to be a non-zero solution for all t in I. So only the following can be said:

If the columns of $\mathbf{F}(t)$ are linearly dependent on I, then there is a non-zero solution for $\mathbf{F}(t)\mathbf{c} = \mathbf{0}$ which works for all t in I. Thus $W(t) = \det(\mathbf{F})(t) = 0$ for all t in I.

The converse does not hold in general, but it holds for polynomials.

3.5.1 Ordinary Wrońskian

Let $g_0(z), g_1(z), \ldots, g_{\ell-1}(z) \in K[z]$ where K is a sub-field of $\mathbb{C}$, be a collection of polynomials. Then Wrońskian of $g_0(z), g_1(z), \ldots, g_{\ell-1}(z)$ is defined as[11]

$$W(z) = \det\left(\frac{1}{\mu!}\frac{d^\mu}{dz^\mu}g_\nu(z)\right) \qquad \text{where } 0 \leq \mu, \nu \leq \ell - 1$$

Theorem 3.5.1. *Let $g_0(z), g_1(z), \ldots, g_{\ell-1}(z) \in K[z]$ be given non-zero polynomials. Then they are linearly independent if and only if Wrońskian of $g_0, g_1, \ldots, g_{\ell-1}$ is a non-zero polynomial in $K[z]$.*

Proof. We will divide proof in two parts.

.

Part 1: *$W(z)$ is a non-zero polynomial $\Rightarrow$ they are linearly independent over K.*

[10] For a system of constants (not functions), the columns of an $n \times n$ matrix A are linearly dependent if and only if there is a non-trivial (i.e. non-zero) solution of $A\mathbf{x} = \mathbf{0}$. This is true if and only if $\det(A) = 0$.

[11] this definition differs from the standard definition encountered when we study ordinary differential equations only in the presence of the non-zero constant factor $\frac{1}{0!1!\cdots(\ell-1)!}$

Let, $c_0, c_1, \ldots, c_{\ell-1} \in K$ be given elements, consider system of equations.

$$\begin{array}{ccccccc} c_0 g_0(z) & + & \ldots & + & c_{\ell-1} g_{\ell-1}(z) & = & 0 \\ c_0 g_0^{(1)}(z) & + & \ldots & + & c_{\ell-1} g_{\ell-1}^{(1)}(z) & = & 0 \\ \vdots & & \vdots & & \vdots & & \vdots \\ c_0 g_0^{(\ell-1)}(z) & + & \ldots & + & c_{\ell-1} g_{\ell-1}^{(\ell-1)}(z) & = & 0 \end{array}$$

which can we written as:

$$\begin{bmatrix} g_0(z) & \ldots & g_{\ell-1}(z) \\ g_0^{(1)}(z) & \ldots & g_{\ell-1}^{(1)}(z) \\ \vdots & \ddots & \vdots \\ g_0^{(\ell-1)}(z) & \ldots & g_{\ell-1}^{(\ell-1)}(z) \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{\ell-1} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

Since, as per our assumption

$$W(z) = \frac{1}{0!1!\ldots(\ell-1)!} \begin{vmatrix} g_0(z) & \ldots & g_{\ell-1}(z) \\ g_0^{(1)}(z) & \ldots & g_{\ell-1}^{(1)}(z) \\ \vdots & \ddots & \vdots \\ g_0^{(\ell-1)}(z) & \ldots & g_{\ell-1}^{(\ell-1)}(z) \end{vmatrix}$$

is a non-zero polynomial. Hence there exist $z_0 \in K$ such that $W(z_0) \neq 0$. Therefore, we have

$$A = \begin{bmatrix} g_0(z_0) & \ldots & g_{\ell-1}(z_0) \\ g_0^{(1)}(z_0) & \ldots & g_{\ell-1}^{(1)}(z_0) \\ \vdots & \ddots & \vdots \\ g_0^{(\ell-1)}(z_0) & \ldots & g_{\ell-1}^{(\ell-1)}(z_0) \end{bmatrix}$$

such that $\det(A) \neq 0$, then

$$\begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{\ell-1} \end{bmatrix} = A^{-1} \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

$$\Rightarrow c_0 = c_1 = \ldots = c_{\ell-1} = 0$$

Thus, the polynomials $g_0, \ldots g_{\ell-1}$ are linearly independent over K

.

Part 2: *$g_0, g_1, \ldots, g_{\ell-1}$ are linearly independent $\Rightarrow$ $W(z)$ is a non-zero polynomial over K.*

We will prove contrapositive of this statement[12], i.e., *if $W(z)$ is a zero polynomial then $g_0, \ldots g_{\ell-1}$ are linearly dependent over K.*

[12]Hence I will follow the proof given for Theorem 4-7(a) in [3]

We will prove this statement by induction on ℓ.

If $\ell = 1$ and $W(z) = g_0(z) \equiv 0$ and hence our statement is true for base case.

Take $\ell > 1$ and suppose that the theorem is true for every set of $\ell - 1$ polynomials, $g_0, g_1, \ldots, g_{\ell-2}$ over K. Also, let the Wrońskian, W_ℓ of $g_0, g_1, \ldots, g_{\ell-1}$ vanishes identically.

If $g_0, \ldots, g_{\ell-2}$ are linearly dependent, so are $g_0, \ldots, g_{\ell-1}$ and the assertion is proved.

So, we just need to consider the case when $g_0, \ldots, g_{\ell-2}$ are linearly independent, so that their Wrońskian $W_{\ell-1}$ is not identically zero.

Now $W_{\ell-1}$, being a polynomial, has only finitely many roots. Let I be an interval in which it doesn't vanish and take $z \in I$. For such z, the system of equations

$$\begin{array}{ccccccc} g_0(z)f_0(z) & + & \ldots & + & g_{\ell-2}(z)f_{\ell-2}(z) & = & g_{\ell-1}(z) \\ g_0^{(1)}(z)f_0(z) & + & \ldots & + & g_{\ell-2}^{(1)}(z)f_{\ell-2}(z) & = & g_{\ell-1}^{(1)}(z) \\ \vdots & & \vdots & & \vdots & & \vdots \\ g_0^{(\ell-2)}(z)f_0(z) & + & \ldots & + & g_{\ell-2}^{(\ell-2)}(z)f_{\ell-2}(z) & = & g_{\ell-1}^{(\ell-2)}(z) \end{array}$$

which can be re-written as

$$\sum_{k=0}^{\ell-2} g_k^{(j)}(z) f_k(z) = g_{\ell-1}^{(j)}(z) \qquad \text{where} \quad j = 0, 1, \ldots, \ell - 2 \tag{3.25}$$

can be solved for f_k's as rational functions of z. But then by subtracting appropriate multiples of each column of W_ℓ, from its last column, we obtain

$$\begin{aligned} 0 &= 0!1!\cdots(\ell-1)!W_\ell(z) \\ &= \begin{vmatrix} g_0(z) & g_1(z) & \ldots & 0 \\ g_0^{(1)}(z) & g_1^{(1)}(z) & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ g_0^{(\ell-1)}(z) & g_1^{(\ell-1)}(z) & \vdots & g_{\ell-1}^{(\ell-1)}(z) - \sum_{k=0}^{\ell-2} g_k^{(\ell-1)}(z) f_k(z) \end{vmatrix} \\ &= 0!1!\cdots(\ell-2)! \left(g_{\ell-1}^{(\ell-1)}(z) - \sum_{k=0}^{\ell-2} g_k^{(\ell-1)}(z) f_k(z) \right) W_{\ell-1}(z) \end{aligned}$$

Now, since $W_{\ell-1}(z) \neq 0$ for $z \in I$, we have

$$\sum_{k=0}^{\ell-2} g_k^{(\ell-1)}(z) f_k(z) = g_{\ell-1}^{(\ell-1)}(z) \tag{3.26}$$

Differentiating (3.25) gives (by chain rule):

$$\sum_{k=0}^{\ell-2} g_k^{(j+1)}(z) f_k(z) + \sum_{k=0}^{\ell-2} g_k^{(j)}(z) f_k'(z) = g_{\ell-1}^{(j+1)}(z) \quad \forall j = 0, 1, \ldots, \ell - 2$$

and comparing this with (3.25) for $j = 0, \ldots, \ell - 3$ and with (3.26) for $j = \ell - 2$ we get:

$$\sum_{k=0}^{\ell-2} g_k^{(j)}(z) f_k'(z) = 0 \quad \forall j = 0, 1, \ldots, \ell - 2$$

But, since $W_{\ell-1} \neq 0$, it must be that

$$f_0'(z) = \ldots = f_{\ell-2}'(z) = 0 \quad \forall z \in I$$

So, we can say that $f_k(z) = c_k$ is some constant in K. But then the polynomial[13]

$$\sum_{k=0}^{\ell-2} c_k g_k(z) - g_{\ell-1}(z) = 0 \quad \forall z \in I$$

Therefore, the polynomials $g_0, \ldots, g_{\ell-1}$ are linearly dependent. □

3.5.2 Generalized Wrońskian

The concept of generalized Wronskians was introduced by Alexander Ostrowski in 1919. For functions of several variables, the situation is not quite so simple, since there are then several partial derivatives to consider. Let $\Delta_0, \Delta_1, \ldots, \Delta_\mu, \ldots, \Delta_{\ell-1}$ be differential operators of form

$$\Delta_\mu = \frac{1}{j_1! j_2! \cdots j_h!} \quad \frac{\partial^{j_1}}{\partial z_1^{j_1}} \cdots \frac{\partial^{j_h}}{\partial z_h^{j_h}}$$

such that the order $j_1 + \ldots + j_h$ of Δ_μ does not exceed μ, for $0 \leq \mu \leq \ell - 1$. Then the function

$$G(z_1, \ldots, z_h) = \begin{vmatrix} \Delta_0 g_0 & \Delta_0 g_1 & \ldots & \Delta_0 g_{\ell-1} \\ \Delta_1 g_0 & \Delta_1 g_1 & \ldots & \Delta_1 g_{\ell-1} \\ \vdots & \vdots & \ddots & \vdots \\ \Delta_{\ell-1} g_0 & \Delta_{\ell-1} g_1 & \ldots & \Delta_{\ell-1} g_{\ell-1} \end{vmatrix}$$

is called a generalized Wrońskian of $g_0, \ldots, g_{\ell-1}$. Except in the trivial case $h = \ell = 1$, there are several Δ_μ's for each μ and hence more than one generalized Wrońskian.

In the case of functions of one variable, the ordinary Wrońskian is that generalized Wrońskian for which the order of Δ_μ is exactly μ, for $0 \leq \mu \leq \ell - 1$

Lemma 3.5.1. *If $f(t, t^k, \ldots, t^{k^{h-1}})$ is a polynomial, then*[14]

$$\frac{d^\mu}{dt^\mu} f = \varphi_1(t) \Delta_\mu^{(1)} f + \ldots + \varphi_r(t) \Delta_\mu^{(r)} f$$

[13] since $g_0, \ldots, g_{\ell-2}$ are assumed to be linearly independent, $c_k = 0$ will work.

[14] Note that for this operator $\frac{d^\mu}{dt^\mu} \equiv \left(\frac{d}{dt}\right)^\mu$

where $\Delta^{(1)}, \ldots, \Delta^{(r)}$ are differential operators of orders not exceeding μ and $\varphi_1, \ldots, \varphi_r$ are polynomials with rational coefficients. Moreover, r depends only on μ and h.

Proof. Firstly note that, by a standard differentiation formula,

$$\frac{d}{dt}f(t,\ldots,t^{k^{h-1}}) = \sum_{j=1}^{h} \frac{\partial}{\partial z_j} f(z_1,\ldots,z_h)\bigg|_{(t,\ldots,t^{k^{h-1}})} \frac{d}{dt}t^{k^{j-1}}$$

We will prove the given statement by induction on μ.

If, $\mu = 1$, let $h = 2$ then

$$\begin{aligned}\frac{d}{dt}f(t,t^k) &= \frac{\partial}{\partial z_1}f(z_1,z_2)\bigg|_{(t,t^k)}\frac{d}{dt}t + \frac{\partial}{\partial z_2}f(z_1,z_2)\bigg|_{(t,t^k)}\frac{d}{dt}t^k \\ &= \frac{\partial}{\partial z_1}f(z_1,z_2)\bigg|_{(t,t^k)} + \frac{\partial}{\partial z_2}f(z_1,z_2)\bigg|_{(t,t^k)} kt^{k-1}\end{aligned}$$

where $\varphi_1(t) = 1$, $\varphi_2(t) = kt^{k-1}$, $\Delta_1^{(1)} = \frac{1}{1!}\frac{\partial}{\partial z_1}$ and $\Delta_1^{(2)} = \frac{1}{1!}\frac{\partial}{\partial z_2}$. Hence given statement is true for base case.

Fix h and assume $\mu > 1$. Let the result be true for $\mu - 1$. Then,

$$\frac{d^{\mu-1}}{dt^{\mu-1}}f(t,t^k,\ldots,t^{k^{h-1}}) = \varphi_1(t)\Delta_{\mu-1}^{(1)}f + \ldots + \varphi_r(t)\Delta_{\mu-1}^{(r)}f$$

Now differentiate this

$$\begin{aligned}\frac{d}{dt}\left(\frac{d^{\mu-1}}{dt^{\mu-1}}\right)f = \frac{d^{\mu}}{dt^{\mu}}f &= \frac{d}{dt}\left(\varphi_1(t)\Delta_{\mu-1}^{(1)}f + \ldots + \varphi_r(t)\Delta_{\mu-1}^{(r)}f\right) \\ &= \frac{d}{dt}\left(\varphi_1(t)\Delta_{\mu-1}^{(1)}f\right) + \ldots + \frac{d}{dt}\left(\varphi_r(t)\Delta_{\mu-1}^{(r)}f\right) \\ &= \left(\frac{d}{dt}\left(\varphi_1(t)\right)\Delta_{\mu-1}^{(1)}f + \varphi_1(t)\frac{d}{dt}\left(\Delta_{\mu-1}^{(1)}f\right)\right) + \ldots \\ &\quad + \left(\frac{d}{dt}\left(\varphi_r(t)\right)\Delta_{\mu-1}^{(r)}f + \varphi_r(t)\frac{d}{dt}\left(\Delta_{\mu-1}^{(r)}f\right)\right)\end{aligned}$$

Note that,

$$\Delta_{\mu-1}^{(j)}f = \frac{1}{j_1!j_2!\cdots j_h!}\quad \frac{\partial^{j_1}}{\partial z_1^{j_1}}\cdots\frac{\partial^{j_h}}{\partial z_h^{j_h}}f$$

where $j_1 + \ldots + j_h \leq \mu - 1$. Hence,

$$\begin{aligned}
\frac{d}{dt}\left(\Delta_{\mu-1}^{(j)} f\right) &= \frac{d}{dt}\Delta_{\mu-1}^{(j)} f\left(z_1, \ldots, z_h\right)\Big|_{(t,\ldots,t^{k^{h-1}})} \\
&= \sum_{m=1}^{h} \frac{\partial}{\partial z_m}\left(\frac{\partial^{j_1}}{\partial z_1^{j_1}} \cdots \frac{\partial^{j_h}}{\partial z_h^{j_h}} f\right) \\
&= \sum_{m=1}^{h} \frac{\partial^{j_1}}{\partial z_1^{j_1}} \cdots \frac{\partial^{j_m+1}}{\partial z_m^{j_m+1}} \cdots \frac{\partial^{j_h}}{\partial z_h^{j_h}} f\Big|_{(t,\ldots,t^{k^{h-1}})} \\
&= \Delta_{\mu}^{(j)} f
\end{aligned}$$

where $\Delta_{\mu}^{(j)}$ is of order $\leq (\mu - 1) + 1 = \mu$.

Also, since $\frac{d}{dt}(\phi_j(t)) \in \mathbb{Q}[t]$, so we conclude that,

$$\frac{d^{\mu}}{dt^{\mu}} f = \lambda_1(t)\Delta_{\mu}^{(1)} f + \ldots + \lambda_s(t)\Delta_{\mu}^{(s)} f$$

where $\lambda_j(t) \in \mathbb{Q}[t]$ since sum of rational functions is a rational function and s depends on μ and h only. □

Theorem 3.5.2. *Let $g_0(z_1, \ldots, z_h), \ldots, g_{\ell-1}(z_1, \ldots, z_h) \in K[z_1, \ldots, z_h]$ be given non-zero polynomials. If they are linearly independent over K then at least one of the generalized Wrońskian does not vanish.*

Proof. Let, for each ν, g_ν be of degree less than k in each of its arguments, so that we can write

$$g_\nu(z_1, \ldots, z_h) = \sum_{\substack{k_1=0 \\ 0 \leq \nu \leq \ell-1}}^{k-1} \cdots \sum_{k_h=0}^{k-1} b_\nu(k_1, \ldots, k_h) z_1^{k_1} \cdots z_h^{k_h}$$

We claim that *the polynomials $g_\nu(t, t^k \ldots, t^{k^{h-1}})$ are linearly independent.*

For otherwise there would be an identity in t of the form:

$$\sum_{\nu=0}^{\ell-1} c_\nu \sum_{k_1=0}^{k-1} \cdots \sum_{k_h=0}^{k-1} b_\nu(k_1, \ldots, k_h) t^{k_1 + k_2 k + \ldots + k_h k^{h-1}} = 0$$

$$\Rightarrow \sum_{k_1=0}^{k-1} \cdots \sum_{k_h=0}^{k-1} \left(\sum_{\nu=0}^{\ell-1} c_\nu b_\nu(k_1, \ldots, k_h) t^{k_1 + k_2 k + \ldots + k_h k^{h-1}}\right) = 0$$

and it would follow from uniqueness of the representation of an integer to the base k that for each exponents $k_1, \ldots, k_h$

$$\sum_{\nu=0}^{\ell-1} c_\nu b_\nu(k_1, \ldots, k_h) = 0$$

from where we get

$$\sum_{\nu=0}^{\ell-1} c_\nu g_\nu(z_1,\ldots,z_h) = 0$$

contradiction the given condition that $g_\nu(z_1,\ldots,z_h)$ are linearly independent, hence proving our claim.

From Theorem 3.5.1 we know that the Wrońskian

$$W(t) = \det\left(\frac{1}{\mu!}\frac{d^\mu}{dt^\mu} f(t)\right)_{\mu,\nu=0,\ldots,\ell-1} = \det\left(\frac{1}{\mu!}\frac{d^\mu}{dt^\mu} g_\nu\left(t, t^k, \ldots, t^{k^{h-1}}\right)\right)_{\mu,\nu=0,\ldots,\ell-1}$$

does not vanish identically.

Using Lemma 3.5.1 in the above expression for $W(t)$ and writing the resulting determinant as sum of other determinants, an expression for $W(t)$ of the form

$$W(t) = \psi_1(t) G_1\left(t,\ldots,t^{k^{h-1}}\right) + \ldots + \psi_r(t) G_r\left(t,\ldots,t^{k^{h-1}}\right)$$

results, in which $\psi_1,\ldots,\psi_r$ are polynomials and $G_1,\ldots,G_r$ are generalized Wrońskians of $g_0,\ldots,g_{\ell-1}$. Since $W(t)$ does not vanish identically, there is an i for which $G_i(t,\ldots,t^{k^{h-1}})$ is not identically zero and therefore $G_i(z_1,\ldots,z_h)$ is not identically zero. □

3.6 Proof of Roth's Theorem

Lemma 3.6.1 (Roth, 1955)**.** *Let ε be given real number satisfying $0 < \varepsilon < \frac{1}{12}$. Let m be given positive integer. Define the real number $\omega = \omega(m,\varepsilon)$ to be*

$$\omega = \frac{24}{2^m}\left(\frac{\varepsilon}{12}\right)^{2^{m-1}}$$

Let $r_1,\ldots,r_m$ be any positive integers satisfying $\omega r_h \geq r_{h+1}$ for $h = 1,2,\ldots,m-1$.

Suppose γ with $0 \leq \gamma \leq 1$ be a real number and $(a_1,b_1),\ldots,(a_m,b_m)$ are pairs of coprime integers satisfying

1. *$b_h > 0$ for $h = 1,2,\ldots,m$*
2. *$b_h^{r_h} \geq b_1^{\gamma r_1}$ for $h = 1,2,\ldots,m$*
3. *$b_h^{\omega\gamma} \geq 2^{3m}$ for $h = 1,2,\ldots,m$*

Let $P(x_1,\ldots,x_m) \in \mathbb{Z}[x_1,\ldots,x_m]$ be given polynomial of degree $r_1 + \ldots + r_m \leq m r_1$ with $[\![P]\!] \leq b_1^{\omega\gamma r_1}$. Then, $\operatorname{ind}_{(\mathbf{a};\mathbf{r})} P \leq \varepsilon$ where $\mathbf{a} = \left(\frac{a_1}{b_1},\ldots,\frac{a_m}{b_m}\right)$

Proof. We will prove this lemma by induction on m.

When $m = 1$ we have, $P(x) \in \mathbb{Z}[x]$ and

$$\omega = \omega(1, \epsilon) = \frac{24}{2}\left(\frac{\varepsilon}{12}\right)^{2^0} = \varepsilon$$

Let, $r_1 \geq 1$ be given integer and $0 < \gamma \leq 1$ be a given real number. Let a_1, b_1 be two coprime integers such that b_1 satisfies

$$b_1^{\omega\gamma} = b_1^{\varepsilon\gamma} \geq 2^3$$

Since we want to estimate $\operatorname{ind}_{(\mathbf{a};\mathbf{r})} P$ where $\mathbf{a} = (a_1/b_1)$ and $\mathbf{r} = (r_1)$ we need to find if $P^{(\ell)}(a_1/b_1)$ vanishes or not.

If $P(a_1/b_1) \neq 0$ then $\operatorname{ind}_{(\mathbf{a};\mathbf{r})} P = 0$ and hence $\operatorname{ind}_{(\mathbf{a};\mathbf{r})} P < \varepsilon$.

So we can assume that $P(a_1/b_1) = 0$. Let,

$$P(x) = \left(x - \frac{a_1}{b_1}\right)^{\ell} M(x) \tag{3.27}$$

where $M(x) \in \mathbb{Q}[x]$ with $M(a_1/b_1) \neq 0$ and $\ell \geq 1$ is a positive integer. Therefore

$$\begin{aligned} P(x) &= (b_1 x - a_1)^{\ell} b_1^{-\ell} M(x) \\ &= (b_1 x - a_1)^{\ell} R(x) \end{aligned}$$

where $R(x) \in \mathbb{Q}[x]$. Therefore by clearing the denominators on the right hand side of equation, we conclude that the leading coefficient of $P(x)$ is divisible by b_1^{ℓ}. If q is the leading coefficient of $P(x)$ then we have

$$|q| \leq [\![P]\!] \leq b_1^{\varepsilon r_1}$$

since b_1^{ℓ} divides $|q|$, we conclude that

$$b_1^{\ell} \leq [\![P]\!] \leq b_1^{\varepsilon r_1} \quad \Rightarrow \ell \log b_1 \leq \varepsilon r_1 \log b_1 \quad \Rightarrow \frac{\ell}{r_1} \leq \varepsilon$$

Also, as per (3.27), $P^{(\ell)}(a_1/b_1) \neq 0$, therefore

$$\operatorname{ind}_{(\mathbf{a};\mathbf{r})} P \leq \frac{\ell}{r_1} \leq \varepsilon$$

Hence, given statement is true for base case.

We assume that the result is true for $m - 1$ and will prove it for $m > 1$.

It is given that $P(x_1, \ldots, x_m) \in \mathbb{Z}[x_1, \ldots, x_m]$. Let $k \geq 1$ be the minimal integer such that

$$P(x_1, \ldots, x_m) = \sum_{j=1}^{k} \phi_j(x_1, \ldots, x_{m-1}) \psi_j(x_m) \tag{3.28}$$

where $\phi_j(x_1, \ldots, x_{m-1}) \in \mathbb{Q}[x_1, \ldots, x_{m-1}]$ and $\psi_j(x_m) \in \mathbb{Q}[x_m]$ for all $j = 1, 2, \ldots, k$. Now we shall divide our proof in 4 parts.

Claim 1: *The polynomial $\phi_1, \ldots, \phi_k$ are linearly independent over $\mathbb{Q}$.*

Suppose the contrary. Thus there exist $c_1, \ldots, c_k \in \mathbb{Q}$ not all zero such that $c_1\phi_1 + \ldots + c_k\phi_k = 0$. By clearing the denominators, we can also assume that $c_1, \ldots, c_k$ are integers and $c_k \neq 0$. Therefore

$$\phi_k = -\frac{1}{c_k}(c_1\phi_1 + \ldots + c_{k-1}\phi_{k-1})$$

Then

$$\begin{aligned} P(x_1, \ldots, x_m) &= \sum_{j=1}^{k-1} \phi_j(x_1, \ldots, x_{m-1})\psi_j(x_m) + \phi_k(x_1 + \ldots + x_{m-1})\psi_k(x_m) \\ &= \sum_{j=1}^{k-1} \phi_j(x_1, \ldots, x_{m-1})\psi_j(x_m) - \frac{1}{c_k}\Big(c_1\phi_1(x_1, \ldots, x_{m-1}) + \\ &\quad \ldots + c_{k-1}\phi_{k-1}(x_1, \ldots, x_{m-1})\Big)\psi_k(x_m) \\ &= \sum_{j=1}^{k-1} \phi_j(x_1, \ldots, x_{m-1}) \left(\psi_j(x_m) - \frac{c_j}{c_k}\psi_k(x_m)\right) \\ &= \sum_{j=1}^{k-1} \phi_j(x_1, \ldots, x_{m-1})\Psi_j(x_m) \end{aligned}$$

contradicts the minimality of k. Therefore $\phi_1, \ldots, \phi_k$ are linearly independent over $\mathbb{Q}$.

From Theorem 3.5.2, we conclude that

$$G(x_1, \ldots, x_{m-1}) = \det\left(\Delta_i\phi_j(x_1, \ldots, x_{m-1})\right)_{1 \leq i,j \leq k} \tag{3.29}$$

is not a zero polynomial.

Claim 2: *$\psi_1, \psi_2, \ldots, \psi_k$ are linearly independent over $\mathbb{Q}$*

This claim can be proved just like Claim 1.

Now from Theorem 3.5.1, it follows that

$$W(x_m) = \det\left(\frac{1}{(i-1)!}\frac{\partial^{i-1}}{\partial x_m^{i-1}}\psi_j(x_m)\right) \qquad \text{where } 1 \leq i, j \leq k \tag{3.30}$$

is not a zero polynomial. Since $P(x_1, \ldots, x_m)$ is a given polynomial, we define

$$U(x_1, \ldots, x_m) = \det\left(\frac{1}{(j-1)!}\frac{\partial^{j-1}}{\partial x_m^{j-1}}\left(\Delta_i P\right)\right)_{1 \leq i,j \leq k} \tag{3.31}$$

But, from (3.28) we observe that for any integer $i \geq 1$,

$$\begin{aligned}\Delta_i P(x_1, \ldots, x_m) &= \Delta_i \left(\sum_{r=1}^{k} \phi_r(x_1, \ldots, x_{m-1}) \psi_r(x_m) \right) \\ &= \sum_{r=1}^{k} \psi_r(x_m) \Delta_i \left(\phi_r(x_1, \ldots, x_{m-1}) \right)\end{aligned}$$

since Δ_i is an operator on $x_1, \ldots, x_{m-1}$ variables. Hence we can rewrite (3.31) as

$$\begin{aligned}U(x_1, \ldots, x_m) = \det &\left(\frac{1}{(j-1)!} \frac{\partial^{j-1}}{\partial x_m^{j-1}} \psi_r(x_m) \right)_{\substack{1 \leq j \leq k \\ 1 \leq r \leq k}} \\ &\det \left(\Delta_i \phi_r(x_1, \ldots, x_{m-1}) \right)_{\substack{1 \leq j \leq k \\ 1 \leq r \leq k}}\end{aligned}$$

By (3.29) and (3.30) we get

$$U(x_1, \ldots, x_m) = W(x_m) G(x_1, \ldots, x_{m-1}) \tag{3.32}$$

Note that $P(x_1, \ldots, x_m) \in \mathbb{Z}[x_1, \ldots, x_m]$, therefore

$$\begin{aligned}&\Delta_i P(x_1, \ldots, x_m) \in \mathbb{Z}[x_1, \ldots, x_m] \\ \Rightarrow &\frac{1}{(j-1)!} \frac{\partial^{j-1}}{\partial x_m^{j-1}} (\Delta_i P) \in \mathbb{Z}[x_1, \ldots, x_m] \\ &\Rightarrow U(x_1, \ldots, x_m) \in \mathbb{Z}[x_1, \ldots, x_m]\end{aligned}$$

Since, $\phi_1, \ldots, \phi_k$ and $\psi_1, \ldots, \psi_k$ are polynomials with integer coefficients, $W(x_m)$ and $G(x_1, \ldots, x_{m-1})$ are also polynomials with integer coefficients. Thus, $U(x_1, \ldots, x_m) = W(x_m) G(x_1, \ldots, x_{m-1}) \in \mathbb{Z}[x_1, \ldots, x_{m-1}]$

To be able to calculate $\text{ind}_{(\mathbf{a};\mathbf{r})} P$ we will first find the lower and upper bound for $\text{ind}_{(\mathbf{a};\mathbf{r})} U$ involving $\text{ind}_{(\mathbf{a};\mathbf{r})} P$.

Claim 3: *Let $\theta = \text{ind}_{(\mathbf{a};\mathbf{r})} P$, then we have*

$$-\frac{k\varepsilon^2}{24} + \sum_{j=1}^{k} \max_j \left(\theta - \frac{j-1}{r_m}, 0 \right) \leq \text{ind}_{(\mathbf{a};\mathbf{r})} U \leq \frac{k\varepsilon^2}{6}$$

Firstly we will prove the upper bound, that

$$\text{ind}_{(\mathbf{a};\mathbf{r})} U \leq \frac{k\varepsilon^2}{6}$$

Using Lemma 3.4.6*(3.)* on (3.32) we get:

$$\text{ind}_{(\mathbf{a};\mathbf{r})} U = \text{ind}_{(\mathbf{a};\mathbf{r})} W + \text{ind}_{(\mathbf{a};\mathbf{r})} G$$

Hence it is enough to prove that $\text{ind}_{(\mathbf{a};\mathbf{r})} W \leq k\varepsilon^2/12$ and $\text{ind}_{(\mathbf{a};\mathbf{r})} G \leq k\varepsilon^2/12$

To estimate the $\text{ind}_{(\mathbf{a};\mathbf{r})} W$ and $\text{ind}_{(\mathbf{a};\mathbf{r})} G$ we will use induction hypothesis of lemma. Replace m by $m-1$ in the hypotheis of the lemma and set parameters as follows

$$\varepsilon' = \frac{\varepsilon^2}{12} \quad \text{and} \quad \omega' = \omega'(m-1, \varepsilon') = \frac{24}{2^{m-1}} \left(\frac{\varepsilon'}{12}\right)^{2^{(m-1)-1}} = 2\omega(m, \varepsilon)$$

Take $kr_1, \ldots, kr_{m-1}$ as given positive integers. Since it is given that $\omega r_h \geq r_{h+1}$, we get

$$\omega' k r_h = 2\omega k r_h \geq 2kr_{h+1} \geq kr_{h+1}$$

Therefore, $\omega' r_h \geq r'_{h+1}$ where $r' = kr_h$ for $h = 1, \ldots, m-1$. Also,

$$b_h^{\omega'\gamma} = b_h^{2\omega\gamma} = \left(b_h^{\omega\gamma}\right)^2 \geq \left(2^{3m}\right)^2 \geq 2^{3(m-1)}$$

We need to check that

$$[\![G]\!] \leq b_1^{\omega'\gamma k r_1}$$

Since, $U = WG$, product of integer coefficient polynomials,

$$[\![U]\!] \geq [\![W]\!] \quad \text{and} \quad [\![U]\!] \geq [\![G]\!]$$

So it is enough to compute the heights of $[\![U]\!]$.

Note that $W(x_1, \ldots, x_m)$ is a determinant of those polynomials of the form $P_{\mathbf{i}}(x_1, \ldots, x_m)$ with $i_1 + \ldots + i_{m-1} \leq r_m$ and $i_m \leq r_m$. Since determinant is a sum of those terms, each of which is product of at most k number of elements of the form $P_{\mathbf{i}}(x_1, \ldots, x_m)$ we see that

$$[\![U]\!] \leq [\![P_{\mathbf{i}}]\!]^k$$

for some $\mathbf{i} = (i_1, \ldots, i_m)$ with $i_1 + \ldots + i_{m-1} \leq r_m$ and $i_m \leq r_m$. Also, from Lemma 3.4.2, we get

$$[\![P_{\mathbf{i}}]\!] \leq 2^{r_1 + \ldots + r_m} [\![P]\!]$$

$$\Rightarrow [\![U]\!] \leq \left(2^{r_1 + \ldots + r_m} [\![P]\!]\right)^k$$

By given hypothesis we know that $r_1 + \ldots + r_m \leq mr_1 \leq 3mr_1$ with $[\![P]\!] \leq b_1^{\omega\gamma r_1}$, hence

$$[\![U]\!] \leq 2^{3mr_1 k} b_1^{\omega k r_1 \gamma}$$

Moreover since, $b_1^{\omega\gamma} \geq 2^{3m}$, we get

$$[\![U]\!] \leq b_1^{\omega k r_1 \gamma} \cdot b_1^{\omega k r_1 \gamma} = b_1^{2\omega k r_1 \gamma}$$

$$\Rightarrow [\![W]\!] \leq b_1^{2\omega k r_1 \gamma} = b_1^{\omega' r'_1 \gamma} \quad \text{and} \quad [\![G]\!] \leq b_1^{2\omega k r_1 \gamma} = b_1^{\omega' r'_1 \gamma}$$

Hence we see that for ε', ω', $r'_1, \ldots, r'_{m-1}$ we have $b_h^{r'_h} = b_h^{kr_h} \geq (b_1^{r_1})^k = b_1^{r'_1}$ and $b_h^{\omega\gamma} \geq 2^{3m}$ for $h = 1, \ldots, m$ together with $[\![G]\!] \leq b_1^{\omega' r'_1 \gamma}$. Thus by induction hypothesis we get

$$\operatorname{ind}_{(\mathbf{a};\mathbf{r}')} G \leq \varepsilon'$$

$$\Rightarrow \operatorname{ind}_{(\mathbf{a};k\mathbf{r})} G \leq \frac{\varepsilon^2}{12}$$

$$\Rightarrow \operatorname{ind}_{(\mathbf{a};\mathbf{r})} G \leq \frac{k\varepsilon^2}{12}$$

Now we will apply induction on $W(x_m)$. Choose $m'' = 1$, $\varepsilon'' = \frac{\varepsilon^2}{12}$, kr_m for $r_1, \ldots, r_m$ and $\omega'' \geq \omega(1, \varepsilon'') \geq 2\omega(m, \varepsilon)$. Also we know that

$$[\![W]\!] \leq b_1^{2\omega k r_1 \gamma} \leq b_1^{\omega'' r''_1 \gamma} < b_1^{\omega'' r''_1}$$

Hence,

$$\operatorname{ind}_{(\mathbf{a};k\mathbf{r})} W \leq \varepsilon'' = \frac{\varepsilon^2}{12}$$

$$\Rightarrow \operatorname{ind}_{(\mathbf{a};\mathbf{r})} W \leq \frac{k\varepsilon^2}{12}$$

Therefore, as desired

$$\operatorname{ind}_{(\mathbf{a};\mathbf{r})} U \leq \frac{k\varepsilon^2}{6}$$

Now we will prove the lower bound

$$-\frac{k\varepsilon^2}{24} + \sum_{j=1}^{k} \max_j \left(\theta - \frac{j-1}{r_m}, 0\right) \leq \operatorname{ind}_{(\mathbf{a};\mathbf{r})} U$$

Let $(p_1, p_2, \ldots, p_{m-1}) \in \mathbb{Z}_{\geq 0}^{m-1}$ be such that $p_1 + \ldots + p_{m-1} \leq k-1 \leq r_m$ and $q \geq 0$ is an integer such that $q - 1 \leq k - 1 \leq r_m$. Then by Lemma 3.4.6*(1.)* we know that if $\mathbf{q} = (p_1, p_2, \ldots, p_{m-1}, q-1)$, then

$$\begin{aligned}\operatorname{ind}_{(\mathbf{a};\mathbf{r})} P_{\mathbf{q}} &\geq \operatorname{ind}_{(\mathbf{a};\mathbf{r})} P - \left(\frac{p_1}{r_1} + \ldots + \frac{p_{m-1}}{r_{m-1}} + \frac{q-1}{r_m}\right) \\ &= \theta - \left(\frac{p_1}{r_1} + \ldots + \frac{p_{m-1}}{r_{m-1}}\right) - \frac{q-1}{r_m}\end{aligned}$$

As per given statement we have, $r_1 \geq \ldots \geq r_m$, therefore

$$\begin{aligned}\operatorname{ind}_{(\mathbf{a};\mathbf{r})} P_{\mathbf{q}} &\geq \theta - \left(\frac{p_1}{r_{m-1}} + \ldots + \frac{p_{m-1}}{r_{m-1}}\right) - \frac{q-1}{r_m} \\ &= \theta - \left(\frac{p_1 + \ldots + p_{m-1}}{r_{m-1}}\right) - \frac{q-1}{r_m} \\ &\geq \theta - \left(\frac{r_m}{r_{m-1}}\right) - \frac{q-1}{r_m}\end{aligned}$$

Also, it is given that $\omega r_{m-1} \geq r_m$, we get

$$\omega \geq \frac{r_m}{r_{m-1}}$$

Therefore,

$$\text{ind}_{(\mathbf{a};\mathbf{r})}\, P_{\mathbf{q}} \geq \theta - \omega - \frac{q-1}{r_m}$$

Note that this lower bound is independent of the chosen $p_1, \ldots, p_{m-1}$. Moreover,

$$\omega = \frac{24}{2^m}\left(\frac{\varepsilon}{12}\right)^{2^{m-1}} \qquad \forall m \geq 2$$
$$\Rightarrow \omega \leq \frac{24}{2^2}\left(\frac{\varepsilon}{12}\right)^{2^{2-1}}$$
$$\Rightarrow \omega \leq \frac{\varepsilon^2}{24}$$

Therefore,

$$\text{ind}_{(\mathbf{a};\mathbf{r})}\, P_{\mathbf{q}} \geq \theta - \frac{\varepsilon^2}{24} - \frac{q-1}{r_m}$$

But since index is always positive,

$$\text{ind}_{(\mathbf{a};\mathbf{r})}\, P_{\mathbf{q}} \geq \max\left\{\theta - \frac{\varepsilon^2}{24} \ - \frac{q-1}{r_m}, 0\right\}$$

Observe that each entry in column q of the determinant defining U is of type $P_{(p_1,\ldots,p_{m-1},q-1)}$ Also using Lemma 3.4.6*(2.),(3.)* we get

$$\begin{aligned}
\text{ind}_{(\mathbf{a};\mathbf{r})}\, U &\geq \sum_{q=1}^{k} \text{ind}_{(\mathbf{a};\mathbf{r})}\, P_{\mathbf{q}} \\
&\geq \sum_{q=1}^{k} \max\left\{\theta - \frac{\varepsilon^2}{24} - \frac{q-1}{r_m}, 0\right\} \\
&\geq \sum_{q=1}^{k} \left(-\frac{\varepsilon^2}{24} + \max\left\{\theta - \frac{q-1}{r_m}, 0\right\}\right) \\
&= -\frac{k\varepsilon^2}{24} + \sum_{q=1}^{k} \max\left\{\theta - \frac{q-1}{r_m}, 0\right\}
\end{aligned}$$

Hence completing proof of Claim 3.

Claim 4: *Proof of this lemma directly follows from* Claim 3

By Claim 3 we get:

$$\sum_{j=1}^{k} \max_{j}\left(\theta - \frac{j-1}{r_m}, 0\right) \leq \frac{k\varepsilon^2}{6} + \frac{k\varepsilon^2}{24} = \frac{5k\varepsilon^2}{24} \leq \frac{k\varepsilon^2}{4} \tag{3.33}$$

Now by using this we will prove our lemma.

Case 1: $\theta > \dfrac{k-1}{r_m}$

$$\begin{aligned}
\sum_{j=1}^{k} \max_j \left\{ \theta - \frac{j-1}{r_m}, 0 \right\} &= \sum_{j=1}^{k} \left(\theta - \frac{j-1}{r_m} \right) \\
&= k\theta - \frac{1}{r_m} \sum_{j=1}^{k} (j-1) \\
&= k\theta - \frac{1}{r_m} \frac{(k-1)k}{2} \\
&= \frac{k}{2} \left(2\theta - \frac{k-1}{r_m} \right) \\
&= \frac{k}{2} \left(\theta + \left(\theta - \frac{k-1}{r_m} \right) \right)
\end{aligned}$$

By (3.33),

$$\begin{aligned}
&\frac{k}{2} \left(\theta + \left(\theta - \frac{k-1}{r_m} \right) \right) \leq \frac{k\varepsilon^2}{4} \\
\Rightarrow &\frac{k\theta}{2} < \frac{k}{2} \left(\theta + \left(\theta - \frac{k-1}{r_m} \right) \right) \leq \frac{k\varepsilon^2}{4} \\
&\Rightarrow \theta \leq \frac{\varepsilon^2}{2} \leq \varepsilon
\end{aligned}$$

Case 2: $\theta \leq \dfrac{k-1}{r_m}$

In this case,

$$\begin{aligned}
\sum_{j=1}^{k} \max_j \left\{ \theta - \frac{j-1}{r_m}, 0 \right\} &= \sum_{j=0}^{\lfloor \theta r_m \rfloor} \left(\theta - \frac{j}{r_m} \right) \\
&= \left(\lfloor \theta r_m \rfloor + 1 \right) \theta - \frac{1}{r_m} \frac{\lfloor \theta r_m \rfloor \left(\lfloor \theta r_m \rfloor + 1 \right)}{2} \\
&= \frac{\lfloor \theta r_m \rfloor + 1}{2} \left(2\theta - \frac{\lfloor \theta r_m \rfloor}{r_m} \right) \\
&= \frac{\lfloor \theta r_m \rfloor + 1}{2} \left(\theta + \left(\theta - \frac{\lfloor \theta r_m \rfloor}{r_m} \right) \right)
\end{aligned}$$

Again by (3.33) we get:

$$\Rightarrow \frac{\lfloor \theta r_m \rfloor + 1}{2} \theta \leq \sum_{j=1}^{k} \max_j \left\{ \theta - \frac{j-1}{r_m}, 0 \right\} \leq \frac{k\varepsilon^2}{4}$$

Since, $\lfloor \theta r_m \rfloor + 1 \geq \theta r_m$, we observe that from above inequality,

$$\frac{\theta r_m}{2}\theta \leq \frac{k\varepsilon^2}{4}$$

$$\Rightarrow r_m\theta^2 \leq \frac{k\varepsilon^2}{4}$$

Note that $k \leq r_m + 1 \leq 2r_m$ because $\deg_P x_m \leq r_m$ and hence $k \leq \deg_P x_m + 1$

$$\Rightarrow r_m\theta^2 \leq \frac{2r_m\varepsilon^2}{4}$$

$$\Rightarrow \theta^2 \leq \frac{\varepsilon^2}{2}$$

$$\Rightarrow \theta \leq \frac{\varepsilon}{\sqrt{2}} \leq \varepsilon$$

□

Proof of Theorem 3.2.1. Claim : *For a given algebraic integer α of degree $d \geq 2$ and $0 < \delta < 1$ real number, the inequality*

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b^{2+\delta}} \tag{3.34}$$

has finitely many solutions in rational numbers.

Suppose, on the contrary, that there exist infinitely many rational solutions a/b satisfying given inequality. Then the denominators of a/b are unbounded. Now we proceed as follows:

1. Choose a real number $\varepsilon > 0$, such that $0 < \varepsilon < \frac{\delta}{36}$. Since $\delta < 1$, we see that $0 < \varepsilon < \frac{1}{36} < \frac{1}{12}$.

2. Choose an integer m with $m \geq 16\varepsilon^{-2}\log(4d)$. Define $\omega = \omega(m, \varepsilon) = \frac{24}{2^m}\left(\frac{\varepsilon}{12}\right)^{2^{m-1}}$

3. Let a_1/b_1 be a solution of (3.34) with $(a_1, b_1) = 1$, $b_1 > 0$ such that $b_1^\omega > H^m$ (H from Theorem 3.4.1), and $b_1^\delta > D$ (put $h = 1$ in Theorem 3.4.2) and $b_1^\omega \geq 2^{3m}$ (put $\gamma = 1$ in Lemma 3.6.1)

4. Choose $\frac{a_2}{b_2}, \ldots, \frac{a_m}{b_m}$ satisfying (3.34), with $(a_h, b_h) = 1$, $b_h > 0$ for $h = 2, \ldots, m$, so that

$$\omega \log b_{h+1} \geq 2 \log b_h$$

for $h = 1, \ldots, m-1$. This implies that $b_1 < b_2 < \ldots < b_m$, and hence $b_h^\delta > D$ (as in Theorem 3.4.2) and $b_h^\omega \geq 2^{3m}$ (put $\gamma = 1$ in Lemma 3.6.1) hold for $h = 1, 2, \ldots, m$

5. Let r_1 be an integer so large that $\varepsilon r_1 \log b_1 \geq \log b_m$

6. For $2 \leq h \leq m$, put
$$r_h = \left\lfloor \frac{r_1 \log b_1}{\log b_h} \right\rfloor + 1$$

Then for $2 \leq h \leq m$ we have

$$\begin{aligned} r_1 \log b_1 &< r_h \log b_h && \text{(by 6.)} \\ &\leq r_1 \log b_1 + \log b_h && \text{(by 6.)} \\ &\leq (1+\varepsilon) r_1 \log b_1 && \text{(by 5.)} \end{aligned}$$

This gives $b_1^{r_1} \leq b_h^{r_h} \leq b_1^{(1+\varepsilon)r_1}$ (as in Theorem 3.4.2) and $b_h^{r_h} \geq b_1^{r_1}$ (with $\gamma = 1$ in Lemma 3.6.1)

From the above sequence of inequalities it follows that

$$r_{h+1} \log b_{h+1} \leq (1+\varepsilon) r_h \log b_h$$

where $h = 1, \ldots, m-1$. Therefore, for $h = 1, \ldots, m-1$, we have

$$\begin{aligned} \omega r_h &\geq \omega \frac{r_{h+1} \log b_{h+1}}{(1+\varepsilon) \log b_h} \\ &\geq \frac{2}{1+\varepsilon} r_{h+1} && \text{(by 4.)} \end{aligned}$$

Thus leading to $\omega r_h \geq r_{h+1}$ (as in Lemma 3.6.1).

The conditions of Theorem 3.4.1 (Index Theorem) are satisfied, since $m \geq 16\varepsilon^{-2} \log(4d)$ holds. Let $P(x_1, \ldots, x_m)$ be a polynomial satisfying the conclusions of Theorem 3.4.1. The hypothesis of Theorem 3.4.2,

I. $0 < \varepsilon < \frac{\delta}{36}$

II. $|\alpha - a_h/b_h| < b_h^{-2-\delta}$ for $h = 1, 2, \ldots, m$

III. $b_h^{\delta} > D$ for $h = 1, 2, \ldots, m$

IV. $b_1^{r_1} \leq b_h^{r_h} \leq b_1^{(1+\varepsilon)r_1}$ for $h = 1, 2, \ldots, m$

also hold. Hence,

$$\operatorname{ind}_{(\mathbf{a};\mathbf{r})} P \geq \varepsilon m \tag{3.35}$$

where $\mathbf{a} = \left(\frac{a_1}{b_1}, \ldots, \frac{a_m}{b_m}\right)$ and $\mathbf{r} = (r_1, \ldots, r_m) \in \mathbb{Z}^m_{\geq 1}$.

On the other hand, the hypothesis of Lemma 3.6.1 hold with $\gamma = 1$,

I. $0 < \varepsilon < \frac{1}{12}$

II. $\omega = \omega(m, \varepsilon) = \frac{24}{2^m} \left(\frac{\varepsilon}{12}\right)^{2^{m-1}}$

III. $\omega r_h \geq r_{h+1}$ for $h = 1, \ldots, m$

IV. $b_h^{r_h} \geq b_1^{r_1}$ for $h = 1, \ldots, m$

V. $q_h^{\omega} \geq 2^{3m}$ for $h = 1, \ldots, m$

VI. $[\![P]\!] \leq b_1^{\omega r_1}$, since

$$\begin{aligned} [\![P]\!] &\leq H^{r_1+\ldots+r_m} && \text{(by Theorem 3.4.1)} \\ &\leq H^{mr_1} && \text{(by 6.)} \\ &\leq b_1^{\omega r_1} && \text{(by 3.)} \end{aligned}$$

Hence,

$$\operatorname{ind}_{(\mathbf{a};\mathbf{r})} P \leq \varepsilon \tag{3.36}$$

where $\mathbf{a} = \left(\frac{a_1}{b_1}, \ldots, \frac{a_m}{b_m}\right)$ and $\mathbf{r} = (r_1, \ldots, r_m) \in \mathbb{Z}_{\geq 1}^m$.

We observe that, the two conclusions drawn from our assumption of infinite solutions, (3.35) and (3.36), contradict each other. Hence our assumption was wrong and (3.34) has only finitely many solutions. □

3.7 Solutions to Diophantine Equations

As indicated in Introduction of this report, Diophantine approximation can be used to determine the number of solutions of Diophantine equations.

Example 3.7.1. *Prove that there are finitely many integer solutions of*

$$x^3 - 2y^3 = 11$$

Solution. If (x, y) is a solution, then x/y must be close to $\sqrt[3]{2}$ (assuming $|x|$ or $|y|$ is large, which would imply both are large):

$$\left|\frac{x}{y} - \sqrt[3]{2}\right| = \left|\frac{11}{y(x^2 + xy\sqrt[3]{2} + y^2\sqrt[3]{4})}\right| \ll \frac{1}{|y|^3}$$

Thus Roth's theorem implies that given equation has only finitely many solutions.

But we have more general results, some of which we will discuss in this section.

Definition (Thue Equation[15])**.** Suppose $f(x, y)$ is a binary form with rational coefficients, and with at least 3 distinct linear factors (with algebraic coefficients). Then if m is non-zero real number, the diophantine equation $f(x, y) = m$, is known as *Thue equation.*

[15]Historically, Thue equation was the driving force behind the development of Roth's theorem.

Theorem 3.7.1 (Finite Solutions of Thue Equations)**.** *Let* $f(x,y) = a_0x^d + a_1x^{d-1}y + \ldots + a_dy^d$ *with* $a_i \in \mathbb{Z}$ *be a form of degree* $d \leq 3$ *which is irreducible*[16] *over* $\mathbb{Q}$ *and* m *be given. The equation,* $f(x,y) = m$ *has only finitely many integer solutions* (x,y)*.*

Proof. Factoring $f(x,y)$ over $\mathbb{C}$, we can write

$$a_0(x - \alpha_1 y)\cdots(x - \alpha_d y) = m$$

where $\alpha_1, \ldots, \alpha_d$ are algebraic numbers of degree d and conjugates of one another. Then dividing by y^d and taking absolute values gives

$$|a_0| \left|\alpha_1 - \frac{x}{y}\right| \cdots \left|\alpha_d - \frac{x}{y}\right| = \left|\frac{m}{y^d}\right| \tag{3.37}$$

Without loss of generality, we have

$$|x - \alpha_1 y| = \min_{1\leq i\leq d} |x - \alpha_i y|$$

which is the same as

$$\left|\alpha_1 \frac{x}{y}\right| = \min_{1\leq i\leq d} \left|\alpha_i - \frac{x}{y}\right|$$

Also, let

$$\gamma = \frac{1}{2} \min_{i\neq j} |\alpha_i - \alpha_j| > 0$$

If y is large, then both sides of (3.37) will be small. In particular, $|\alpha_1 - x/y|$ will be small. But, for $i \neq j$ we observe that

$$\left|\alpha_i - \frac{x}{y}\right| \geq |\alpha_i - \alpha_1| - \left|\alpha_1 - \frac{x}{y}\right| \geq 2\gamma - \gamma = \gamma \tag{3.38}$$

Then we have

$$\begin{aligned} \left|\alpha_1 - \frac{x}{y}\right| &= \prod_{i=2}^{d} \left|\alpha_i - \frac{x}{y}\right|^{-1} \quad \left|\frac{m}{a_0 y^d}\right| && \text{(from (3.37))} \\ &\leq \left|\frac{m}{a_0\gamma^{d-1}}\right| \quad \frac{1}{|y|^d} && \text{(from (3.38))} \end{aligned}$$

Now, since $d \geq 3$, Roth's theorem implies that there is only finite number of solutions (x,y). □

Theorem 3.7.2 (Siegel's Theorem[17])**.** *If* α *is an algebraic number of degree* d*, then there is an* $c(\alpha)$*, depending only on* α*, such that*

$$\left|\alpha - \frac{a}{b}\right| > \frac{c(\alpha)}{b^{2\sqrt{d}}}$$

[16] A polynomial is said to be irreducible if it cannot be factored into nontrivial polynomials over the same field. Also, such a form f can never be irreducible over $\mathbb{C}$.

[17] This theorem lead to Siegel's Conjecture, hence is a predecessor of Roth's Theorem

Theorem 3.7.3 (Pillai[18]). *Let a, b, m and n be natural numbers and $\delta > 0$. Then for any integral x and y if we have $am^x - bn^y \neq 0$, then we have*

$$|am^x - bn^y| > m^{(1-\delta)x}$$

for all $x > x(\delta)$ where $x(\delta)$ depends on m, n, a, b and δ.

Proof. Suppose that u and v are positive integers, such that a/b is not a perfect r^{th} power and $\frac{1}{2}au^r < bv^r < au^r$. If

$$w = \left(\frac{a}{b}\right)^{\frac{1}{r}} u = \alpha u$$

then α is an algebraic number of degree r at most, and

$$\begin{aligned}
au^r - bv^r &= b(w^r - v^r) \\
&= b(w^{r-1} + w^{r-2}v + \ldots + v^{r-1})(w - v) \\
&> brv^{r-1}(w - v) && \left(\because w^r = \frac{a}{b}u^r > v^r\right) \\
&= br\left(\frac{v}{u}\right)^{r-1} u^{r-1}(w - v) \\
&> br\left(\frac{a}{2b}\right)^{\frac{r-1}{r}} u^r\left(\alpha - \frac{v}{u}\right) && \left(\because \frac{a}{2b} < \frac{v^r}{u^r} < \frac{a}{b}\right) \\
&> br\left(\frac{a}{2b}\right)^{\frac{r-1}{r}} c(\alpha)u^{r-2\sqrt{r}} && \text{(Siegel's Theorem)}
\end{aligned}$$

This is also true if $0 < bv^r \leq \frac{1}{2}au^r < au^r$, so that it holds whenever $au^r - bv^r$ is positive.

Similarly, whenever $bv^r - au^r$ is positive, $\frac{1}{2}bv^r < au^r < bv^r$, we get

$$\begin{aligned}
bv^r - au^r &> b\frac{2^{1/r}}{2(2^{1/r} - 1)}\frac{u}{v}v^r\left(\frac{v}{u} - \alpha\right) \\
&> \frac{b2^{1/r}}{2(2^{1/r} - 1)}\left(\frac{b}{2a}\right)^{1/r} v^r\left(\frac{v}{u} - \alpha\right) \\
&> \frac{b2^{1/r}}{2(2^{1/r} - 1)}\left(\frac{b}{2a}\right)^{1/r} c(\alpha)v^{r-2\sqrt{r}}
\end{aligned}$$

Hence in general,

$$|au^r - bv^r| > Kz^{r-2\sqrt{r}} \tag{3.39}$$

where u and v are any positive integers, and z being u or v. Also, K depends on a, b and r.

[18] Neither Liouville's nor Thue's theorems would be strong enough for Pillai's application. It is essential to have an exponent of lower order of magnitude than r.

Let r be any positive integer and x and y are very large as compared to r. For natural numbers s, t we can write

$$\begin{cases} x = sr + h & (0 \leq h < r) \\ y = tr + l & (0 \leq l < r) \end{cases}$$

Then,

$$|am^x - bn^y| = |am^h \cdot m^{rs} - bn^l \cdot n^{tr}|$$

Let, $m^s = u$ and $n^t = v$ to get

$$|am^x - bn^y| = |am^h \cdot u^r - bn^l \cdot v^r|$$

Then by (3.39) we get

$$|am^x - bn^y| > Ku^{r-2\sqrt{r}}$$

where K depends on a, b, h, l and r. Since the number of values of h and l concerned depends only on r, let K_0 be the minimum of all K's, hence

$$\begin{aligned} |am^x - bn^y| &> K_0 u^{r-2\sqrt{r}} \\ &= K_0 u^{(1-\frac{2}{\sqrt{r}})r} \\ &> u^{\left(1-\frac{2}{\sqrt{r}}-\frac{\varepsilon}{r}\right)r} \end{aligned}$$

where $x > x(\varepsilon)$ and $\varepsilon \to 0$, which depends only on K_0 and x.

But, $u^r = m^{sr} = m^{x-h}$, and accounting the dependency of x, r and h we get,

$$\begin{aligned} |am^x - bn^y| &> m^{\left(1-\frac{2}{\sqrt{r}}-\frac{\varepsilon}{r}\right)(x-h)} \\ &> m^{\left(1-\frac{2}{\sqrt{r}}-\frac{\varepsilon}{r}\right)x} \end{aligned}$$

Now for given δ, we can choose $x(\delta)$ and r so that $\frac{2}{\sqrt{r}} + \frac{\varepsilon}{r} < \delta$ for all $x > x(\delta)$, leading to

$$|am^x - bn^y| > m^{(1-\delta)x}$$

□

Definition (Pillai Equation[19])**.** Given positive integers a, b, c, m, n with $a \geq 2$ and $b \geq 2$, the equation

$$am^x - bn^y = c$$

where the unknown x, y are nonnegative integers, is known as Pillai Equation or Pillai's Diophantine Equation.

Corollary 3.7.1. *Let a, b, c, m and n be natural numbers, then the equation*

$$am^x - bn^y = c$$

has only finite number of solutions.

[19]It is a subclass of exponential diophantine equations.

Conclusion

Roth's theorem can be restated as

Theorem. *Let α be an irrational algebraic number. Then for any $\varepsilon > 0$ there is a quantity $c_{\alpha,\varepsilon}$ such that*

$$\left|\alpha - \frac{a}{b}\right| > \frac{c_{\alpha,\varepsilon}}{b^{2+\varepsilon}}$$

As stated by Terence Tao in Roth's obituary[20],

> An important point is that the constant $c_{\alpha,\varepsilon}$ is ineffective - it is a major open problem in Diophantine approximation to produce any bound significantly stronger than Liouville's theorem with effective constants. This is because the proof of Roth's theorem does not exclude any single rational a/b from being close to α, but instead very ingeniously shows that one cannot have two different rationals a/b, a'/b' that are unusually close to α, even when the denominators b, b' are very different in size.

All results obtained by the method of Thue, Siegel and Roth share the disadvantage that they are non-effective. Effective bounds, which however don't imply Roth's, Thue's or Siegel's Theorem unless α is of a special type, were given by Alan Baker.[21]

The method of proof of Roth's Theorem can easily be used to prove some other modifications, for example, consider following theorem by Ridout[22]

Theorem. Let α be any algebraic number other than 0; let $P_1, \ldots, P_s$, $Q_1, \ldots, Q_t$ be distinct primes; and let μ, ν, c be real numbers satisfying

$$0 \le \mu \le 1, \quad 0 \le \nu \le 1, \quad c > 0$$

[20] K. F. Roth died about a month before start of this project, on 10 November 2015, aged 90. https://terrytao.wordpress.com/2015/11/12/klaus-roth/

[21] see: Baker, A., 'Rational Approximations to certain algebraic numbers', Proc. London Math. Soc., (3) 14 (1964), 385-398.

[22] Ridout, D., 'Rational approximations to algebraic numbers', Mathematika, 4 (1957), 125-131, doi:10.1112/S0025579300001182

Let p, q be restricted to integers of form

$$p = p^* P_1^{\rho_1} \cdots P_s^{\rho_s}, \quad q = q^* Q_1^{\sigma_1} \ldots Q_t^{\sigma_t}$$

where $\rho_1, \ldots, \rho_s, \sigma_1, \ldots, \sigma_t$ are non-negative integers and p^*, q^* are integers satisfying

$$0 < |p^*| \leq cp^{\mu}, \quad 0 < q^* \leq cq^{\nu}$$

Then if $\kappa > \mu + \nu$, the inequality

$$0 < \left| \alpha - \frac{p}{q} \right| < \frac{1}{q^{\kappa}}$$

has only finite number of solutions in p, q.

An important point to note here is that unlike Roth's Theorem, this theorem does not become trivial if α is rational.

The Subspace Theorem of W.M. Schmidt (Theorem 1B in Chapter VI of [8]), is a powerful generalisation of the Roth's Theorem. It deals with the approximation of algebraic numbers and says that tuples of algebraic numbers do behave like almost all tuples. Another point of view is the metrical one, dealing with almost all numbers. The metric theory of Diophantine approximation provides statements which are valid for almost all (real or complex) numbers, that means for all numbers outside a set of Lebesgue measure 0. (see §1.2 of [11]).

I will conclude my report with two famous conjectures in Diophantine Approximation:

- *Littlewood's Conjecture*[23] *(1930):* For all pairs of real numbers α and β, we have that

  $$\liminf_{n \to \infty} n \|n\alpha\| \|n\beta\| = 0$$

  where $\|x\|$ denote distance of x from the nearest integer.

- *Zaremba's Conjecture*[24] *(1971):* For a fixed finite set $\mathcal{A} \subset \mathbb{N}$, let $\mathfrak{R}_A$ be the set of all finite continued fractions with all partial denominators bounded by an integer $A := \max \mathcal{A}$

  $$\mathfrak{R}_A = \left\{ \frac{b}{d} = [0; a_1, \ldots, a_k] : 0 < b < d, \gcd(b, d) = 1, \text{and} \forall j, a_j \in \mathcal{A} \right\}$$

  and let $\mathfrak{D}_A \subset \mathbb{N}$ be the set of denominators of fractions in $\mathfrak{R}_A$,

  $$\mathfrak{D}_A = \left\{ d \in \mathbb{N} : \exists \gcd(b, d) = 1 \text{with} \frac{b}{d} \in \mathfrak{R}_A \right\}$$

  Then for sufficiently large A, $\mathfrak{D}_A = \mathbb{N}$ holds.

[23] see: Haynes, A. and Munday, S., 'Diophantine Approximation and Coloring', The American Mathematical Monthly, Vol. 122, No. 6 (June-July 2015), 567-580

[24] see: Borwein, J.,et al., Neverending Fractions. An Introduction to Continued Fractions, Australian Mathematical Society Lecture Series 23 (Cambridge University Press, Cambridge, 2014) pp. 117.

Bibliography

[1] Beskin, N. M., Fascinating Fractions, English translation, Little Mathematics Library (Mir Publishers, Moscow, 1986).

[2] Hardy, G. H. and Wright, E. M., An Introduction to the Theory of Numbers, 6th edn (Oxford University Press, Oxford, 2008)

[3] LeVeque, W. J., Topics in Number Theory. Volume II (Addison-Wesley Publishing Company, 1956)

[4] Nakamaye, M., 'Roths Theorem: an introduction to diophantine approximation', in: Rational Points, Rational Curves and Entire Holomorphic Curves on Projective Varieties (Conference at Centre de recherches mathématiques, Université de Montréal, June 3 - 28, 2013)

[5] Niven, I., Zuckerman, H. M. and Montgomery, H. L., An Introduction to the Theory of Numbers, 5th edn (John Wiley & Sons Inc, New York, 1991).

[6] Pillai, S. S., 'On the inequality $0 < a^x - b^y \leq n$', Journal of Indian Mathematical Society, XIX (1931), 1-11.

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

[8] Schmidt, W. M., Diophantine Approximation, Lecture Notes in Mathematics 785 (Springer-Verlag, Berlin Heidelberg, 1980).

[9] Thangadurai, R., Notes on Roth's Theorem (Harish-Chandra Research Institute, Allahabad, 2015).

[10] Waldschmidt, M., 'Perfect Powers: Pillai's Works and their Developments', in: Collected Works of S. Sivasankaranarayana Pillai. Volume I (Ramanujan Mathematical Society, India, 2010), xxii-xlvii.

[11] Waldschmidt, M., 'Recent advances in Diophantine approximation', in: Number Theory, Analysis and Geometry. In Memory of Serge Lang (Springer, New York, 2012), 659-704.

Prepared in LaTeX 2_ε by *Gaurish Korpal*