An elementary approach to Roth's theorem

Aleksa Milojevic

January 2022

Abstract

In 1955, Roth proved his famous theorem on Diophantine approximation, which states that for any algebraic number $\alpha \in \mathbb{R}$ and any $\varepsilon > 0$, there are only finitely many rational numbers $\frac{p}{q} \in \mathbb{Q}$ for which $|\alpha - \frac{p}{q}| \leq \frac{1}{q^{2+\varepsilon}}$. This theorem extended previous work of Liouville, Thue, Siegel and Dyson, and bridged the gap between previously known results and Dirichlet's theorem which shows that above theorem no longer holds if the exponent $2 + \varepsilon$ is replaced by 2. The intent of this note is to present the proof of Roth's theorem in a self-contained way and give the motivation for certain steps of the proof.

1 Introduction

A basic question in the area of Diophantine approximation is how well can a real number $\alpha \in \mathbb{R}$ be approximated by rationals of small denominator. Starting in 19th century, much work has been put into this field, using techniques of continued fractions and the polynomial method. One of the first results in the field was the famous Liouville's theorem.

Theorem 1.1. *(Liouville, 1844) Let $\alpha \in \mathbb{R}$ be an irrational algebraic number of degree d. Then, there exist a constant $C = C(\alpha) > 0$ such that for all rationals $\frac{p}{q} \in \mathbb{Q}$:*

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

Remark. The original motivation behind this result comes from an attempt to construct explicitly a transcendental number, by constructing a number which can be approximated "too well" by the rationals.

We postpone the proof of Liouville's theorem, and present it at the end of this section. Although this result is considerably weaker than Roth's theorem, its proof will serve as a blueprint for understanding Roth's proof. A natural way to improve the above theorem is to obtain a lower exponent of q on the right-hand side. This motivates the following definition.

Definition 1.A. Let $\alpha \in \mathbb{R}$. The *approximation degree* of α is the smallest real number $\tau(\alpha)$ with the following property: for all exponents $\kappa > \tau(\alpha)$ there are only finitely many rationals $\frac{p}{q} \in \mathbb{Q}$ with

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^\kappa}.$$

In light of this definition, Liouville's theorem states $\tau(\alpha) \leq d$ for algebraic numbers α of degree d. An natural question is whether we can determine exactly what $\tau(\alpha)$. If α is rational, it is not hard to get $\tau(\alpha) = 1$. However, the case when α is irrational and algebraic calls for much subtler techniques. Using the polynomial method, Roth showed $\tau(\alpha) \leq 2$ for all algebraic numbers α.

Theorem 1.2. *(Roth, 1955) Let $\alpha \in \mathbb{R}$ be an algebraic number. For any $\varepsilon > 0$, there exist only finitely many rationals $\frac{p}{q} \in \mathbb{Q}$ for which:*

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

The goal of this note is to present the proof of Roth's theorem in an elementary way, assuming no more than standard linear algebra. Even though the theorem can be vastly generalized, in many directions, it is valuable to see the main ideas of the proof stripped of all technicalities coming from working in higher generality. The proof given here is essentially a rewriting of the proof given in [1], using slightly different terminology and notation. Additionally, [2] was used as a source of motivation and for providing a high-level overview of the proof.

Roth's theorem comes as a final improvement, building on the work of Thue, who showed $\tau(\alpha) \leq \frac{1}{2}d + 1$, Siegel, who showed $\tau(\alpha) \leq 2\sqrt{d}$ and Dyson, who showed $\tau(\alpha) \leq \sqrt{2d}$, where d is the degree of α. Moreover, in conjunction with the following simple result of Dirichlet, Roth's theorem proves $\tau(\alpha) = 2$ for all irrational algebraic $\alpha \in \mathbb{R}$.

Theorem 1.3. *(Dirichlet) Let $\alpha \in \mathbb{R}$ be an irrational real number. Then, there exist infinitely many rational numbers $\frac{p}{q} \in \mathbb{Q}$ for which:*

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

Proof. Before proceeding to show the above result, we need to show that for any $n \in \mathbb{Z}_{>0}$ there exists a rational number $\frac{p}{q} \in \mathbb{Q}$ with $q \leq n$ and $\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{nq}$.

For a positive integer n, consider the set $S_n = \Big\{\{k\alpha\} | k = 0, \ldots, n\Big\}$, where $\{k\alpha\}$ denotes the fractional part of $k\alpha$. Let us partition the interval $[0, 1)$ into n subintervals of the form $\left[\frac{k}{n}, \frac{k+1}{n}\right)$, for $k = 0, \ldots, n-1$. As all $n+1$ elements of S_n lie in $[0, 1)$, Pigeonhole principle implies there are two elements of S_n within the same subinterval, say $\{k_1\alpha\}$ and $\{k_2\alpha\}$.

Assuming $k_1 < k_2$, we subtract these two elements to get $\{(k_2 - k_1)\alpha\} \in (-\frac{1}{n}, \frac{1}{n})$. Recalling the definition of the fractional part, we have an integer p for which $(k_2 - k_1)\alpha \in (p - \frac{1}{n}, p + \frac{1}{n})$. Setting $q = k_2 - k_1 \leq n$ and manipulating the above expression gives:

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

Assume now the inequality (2) has only finitely many rationals $\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m} \in \mathbb{Q}$ satisfying it. It suffices to pick $n > \max_i\{\frac{1}{|\alpha - p/q|}\}$ and find the corresponding approximation $\frac{p}{q} \in \mathbb{Q}$ using the above argument. The rational $\frac{p}{q}$ does not coincide with any of the previous solutions by the definition of n. Moreover, it is also a solution to inequality (2), implying a contradiction to the fact $\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}$ were all solutions. This completes the proof. □

Before passing to the proof of the main theorem, we will present Liouville's proof.

Proof of Liouville's theorem. It does not reduce generality to assume α is an algebraic integer of degree d. Let $\frac{p}{q} \in \mathbb{Q}$ with $|\frac{p}{q} - \alpha| \leq 1$ be an arbitrary rational and let f be the minimal polynomial of α with $\deg f = d$. The idea of the proof is to evaluate $f(\frac{p}{q})$ and obtain upper and lower bounds which will give us information about $|\alpha - \frac{p}{q}|$.

To bound $f(\frac{p}{q})$ from below is easy. We know f does not vanish at $\frac{p}{q}$ because it is irreducible of degree $d > 1$. Therefore, $f(\frac{p}{q})$ can be written as a nonzero rational number of denominator q^d, implying $|f(\frac{p}{q})| \geq \frac{1}{q^d}$.

On the other hand, f has a Taylor expansion around α of the form $f(x) = f(\alpha) + (x - \alpha)f'(\alpha) + \cdots$. As $\deg f = d$, this expansion has d terms. The first term of the expansion vanishes, and all others can be bounded by $C_0|x - \alpha|$, where the constant C_0 depends only on α (and the derivatives of its minimal polynomial). Therefore, we have the upper bound on $f(\frac{p}{q})$:

$$f(\frac{p}{q}) \leq C_0 d\left|\frac{p}{q} - \alpha\right|.$$

Combining the upper and lower bounds, we get a lower bound on $|\frac{p}{q} - \alpha|$:

$$C_0 d\left|\frac{p}{q} - \alpha\right| \geq f(\frac{p}{q}) \geq \frac{1}{q^d},$$

which directly implies the Liouville's theorem with $C = (C_0 d)^{-1}$. □

This note will be organized into 6 sections. Section 2 serves to present a high-level sketch of the proof, where we identify the areas where Liouville's proof can be improved and which kind of difficulties arise in doing so. In section 3, notation and terminology to be used throughout the paper is introduced, and several elementary lemmas are proved. In section 4, we show a way to construct the auxiliary polynomial, which replaces the minimal polynomial from Liouville's proof. Section 5 contains the essence of the proof, Roth's lemma, which shows that the auxiliary polynomial cannot vanish to high order at a rational point near α, under certain assumptions. Finally, section 6 combines the previous parts and proves Roth's theorem.

2 Sketch of the proof

When proving Roth's theorem, we will follow the strategy outlined in Liouville's proof. However, in order to gain an improvement on the exponent, we need to use a different polynomial. The main idea will be to find an integer polynomial P which vanishes at α and does not vanish at rational points $\frac{p}{q}$ near α in order to obtain a contradictory bounds on $P(\frac{p}{q})$.

In order to apply this idea, there is a significant difficulty we need to solve. If $P \in \mathbb{Z}[x]$ vanishes at α to order n, we expect $P(\frac{p}{q})$ to behave like $\left|\alpha - \frac{p}{q}\right|^n$ for $\frac{p}{q}$ close to α. At the same time, the lower bound on $P(\frac{p}{q})$ will be $\frac{1}{q^{\deg P}}$, where $\deg P$ is the degree of the P. Taking n-th roots, we would obtain a lower bound $\left|\alpha - \frac{p}{q}\right| \geq \frac{1}{q^{\deg P/n}}$. Therefore, in order to improve upon Liouville's result and obtain an exponent lower than $d = \deg \alpha$, we would need $\deg P < nd$. Unfortunately, it is not possible to construct a polynomial P of degree less than nd vanishing at α to order n because vanishing constraints imply $f^n | P$, where f is the minimal polynomial of α. Hence, $\deg P \geq n \deg f = nd$.

In order to go around this difficulty, we consider polynomials in more than one variable, $P \in \mathbb{Z}[x_1, \ldots, x_m]$. we construct these so that they vanish $(\alpha, \ldots, \alpha) \in \mathbb{R}^m$ to high enough order, which serves to establish upper bounds on the value of P at a rational point. Then, under reasonable assumptions we will be able to prove that P does not vanish to high order at the rational point near $(\alpha, \ldots, \alpha)$, which will provide us with lower bounds. More precisely, the proof can be divided into four main steps.

- Choose m and a sequence of rational approximations for α, denoted by $\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}$ whose denominators increase rapidly. Also, construct a polynomial P vanishing at $(\alpha, \ldots, \alpha)$ to high order.
- Show that P does not vanish at the point $\left(\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}\right)$.
- From the vanishing of P at $(\alpha, \ldots, \alpha)$ and closeness of approximations $\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}$, derive an upper bound for $P\left(\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}\right)$.
- Choose the parameters in order to obtain a contradictions by combining upper and lower bounds.

We proceed to perform the above steps mostly in order - after covering the preliminaries in section 3, section 4 constructs the polynomial P and section 5 argues why it does not vanish to high order. Finally, section 6 completes the last two steps and presents the complete proof. Let us make three additional short remarks before introducing formal definitions and statements.

In order to obtain useful upper bounds, we must construct P carefully so that it does not have too large coefficients. This will be accomplished using Siegel's lemma, which talks about existence of small integer solutions to the system of these linear equations with bounded coefficients.

On the other hand, it turns out that P will have very unbalanced degrees in different variables. Therefore, it is not very useful to measure the standard vanishing order at a certain point. Rather, we need to introduce a more refined notion of the *index* at a point which will behave as a scaled version of the vanishing order. With this new definition, each variable will contribute equally to the index, even with unbalanced degrees.

Finally, before developing the whole machinery we reduce the theorem to the case of algebraic integers. This makes the constructions somewhat simpler, as we only care about integer coefficient polynomials.

Claim 2.1. *It suffices to prove Roth's theorem in case α is an algebraic integer.*

Proof. Assume Roth theorem holds in case α is an algebraic integer and let D be an integer for which $D\alpha$ is an algebraic integer. In case there are infinitely many $\frac{p}{q} \in \mathbb{Q}$ satisfying equation (1), we also have infinitely many solutions to:

$$\left|D\alpha - D\frac{p}{q}\right| < \frac{D}{q^{2+\varepsilon}}.$$

For all except finitely many of these we have $q^{\varepsilon/2} > D$, and therefore we also have infinitely many solutions to $\left|D\alpha - \frac{p'}{q'}\right| \leq \frac{1}{q'^{2+\varepsilon/2}}$. However, this contradicts Roth's theorem for algebraic integers and completes the reduction. □

3 Preliminaries

Throughout this note, multivariate polynomials will be ubiquitous. Therefore, we start by introducing the basic terminology, most notably the concept of the *index*, and proceed to prove a couple of elementary facts which will be used in the subsequent sections.

The set of polynomials in variables $x_1, \ldots, x_m$ with integer coefficients is denoted $\mathbb{Z}[x_1, \ldots, x_m]$. For a polynomial $P \in \mathbb{Z}[x_1, \ldots, x_m]$ of the form $P = \sum_{i_1,\ldots,i_m} c_{i_1,\ldots,i_m} x_1^{i_1} \cdots x_m^{i_m}$, we use the shorthand notation $P = \sum_I c_I \boldsymbol{x}^I$, where $I = (i_1, \ldots, i_m)$ and $\boldsymbol{x}^I = x_1^{i_1} \cdots x_m^{i_m}$. We also define the *partial degree* of P in variable x_k as the maximal degree of x_k appearing in P, and denote it by $\deg_k P$. It is also worth noting that the base of all logarithms is 2, although this is only an ad-hoc convention and has no real impact on the proof.

For a multi-index $\boldsymbol{\mu} \in \mathbb{Z}^m_{\geq 0}$, the differential operator ∂_μ is defined in the following unusual way:

$$\partial_{\boldsymbol{\mu}} P(x_1, \ldots, x_m) = \frac{1}{\mu_1! \cdots \mu_m!} \Big(\frac{\partial}{\partial x_1}\Big)^{\mu_1} \cdots \Big(\frac{\partial}{\partial x_m}\Big)^{\mu_m} P(x_1, \ldots, x_m)$$

Moreover, for $\boldsymbol{\mu} \in \mathbb{Z}^m_{\geq 0}$, its *size* is defined as $|\boldsymbol{\mu}| = \mu_1 + \cdots + \mu_m$.

Finally, as a scaled measure of vanishing order at a given point, the definition of the index proves to be very useful. The *index* of a polynomial P at a point $\boldsymbol{\xi} = (\xi_1, \ldots, \xi_m)$ with respect to a degree sequence $\boldsymbol{d} = (d_1, \ldots, d_m)$ is defined as:

$$\operatorname{ind}(P; \boldsymbol{d}, \boldsymbol{\xi}) = \min \Big\{ \sum_{i=1}^{m} \frac{\mu_i}{d_i} \big| \partial_{\boldsymbol{\mu}} P \neq 0 \Big\}$$

It is also common to talk about the index of the monomial $\boldsymbol{x}^I$, which is simply $\sum_{k=1}^m \frac{i_k}{d_k}$. Index of the polynomial behaves in many ways similar to the vanishing order, as shown by the following claim.

Claim 3.1. *For arbitrary polynomials $P, Q \in \mathbb{Z}[x_1, \ldots, x_m]$ and $\boldsymbol{d} \in \mathbb{Z}^m_{>0}$, $\boldsymbol{\mu} \in \mathbb{Z}^m_{\geq 0}$, $\boldsymbol{\xi} \in \mathbb{R}^m$, the index defined as above has the following properties:*

- $\operatorname{ind}(P + Q; \boldsymbol{d}, \boldsymbol{\xi}) \geq \min\big(\operatorname{ind}(P; \boldsymbol{d}, \boldsymbol{\xi}), \operatorname{ind}(Q; \boldsymbol{d}, \boldsymbol{\xi})\big)$
- $\operatorname{ind}(PQ; \boldsymbol{d}, \boldsymbol{\xi}) = \operatorname{ind}(P; \boldsymbol{d}, \boldsymbol{\xi}) + \operatorname{ind}(Q; \boldsymbol{d}, \boldsymbol{\xi})$
- $\operatorname{ind}(\partial_{\boldsymbol{\mu}} P; \boldsymbol{d}, \boldsymbol{\xi}) \geq \operatorname{ind}(P; \boldsymbol{d}, \boldsymbol{\xi}) - \sum_{i=1}^m \frac{\mu_i}{d_i}$

Proof. Generally, a good way to understand the index is to work with the Taylor polynomial. We may assume that $\xi = (0, \ldots, 0)$, and in this case Taylor polynomial coincides with the notation $P = \sum_I c_I \boldsymbol{x}^I, Q = \sum_J d_J \boldsymbol{x}^J$.

We start by showing the first property. Note that all monomials in either of the sums have index $\geq \min\big(\operatorname{ind}(P; \boldsymbol{d}, \boldsymbol{\xi}), \operatorname{ind}(Q; \boldsymbol{d}, \boldsymbol{\xi})\big)$. Therefore, the polynomial $P + Q$ cannot contain any monomial of smaller index.

The second property is similar: we start from $PQ = \sum_{I,J} c_I d_J \boldsymbol{x}^{I+J}$, where $\sum_k \frac{i_k}{d_k} \geq \operatorname{ind}(P; \boldsymbol{d}, \boldsymbol{\xi})$, $\sum_k \frac{j_k}{d_k} \geq \operatorname{ind}(Q; \boldsymbol{d}, \boldsymbol{\xi})$ for all terms. Summing the constrains gives $\sum_k \frac{i_k+j_k}{d_k} \geq \operatorname{ind}(P; \boldsymbol{d}, \boldsymbol{\xi}) + \operatorname{ind}(Q; \boldsymbol{d}, \boldsymbol{\xi})$, which means $\operatorname{ind}(PQ; \boldsymbol{d}, \boldsymbol{\xi}) \geq \operatorname{ind}(P; \boldsymbol{d}, \boldsymbol{\xi}) + \operatorname{ind}(Q; \boldsymbol{d}, \boldsymbol{\xi})$. Showing the other inequality is straightforward as well: pick minimal index monomials $\boldsymbol{x}^I$ in P and $\boldsymbol{x}^J$ in Q (if there are several choices, pick the minimal one in lexicographic order on I, J). It is not hard to see that this monomial cannot be cancelled, which shows the exact equality.

Finally, the third property is also direct. The monomials of $\partial_{\boldsymbol{\mu}} P$ are of the form $\boldsymbol{x}^{I-\boldsymbol{\mu}}$, and therefore $\sum_k \frac{i_k-\mu_k}{d_k} = \sum_k \frac{i_k}{d_k} - \sum_k \frac{\mu_k}{d_k} \geq \operatorname{ind}(P; \boldsymbol{d}, \boldsymbol{\xi}) - \sum_k \frac{\mu_k}{d_k}$. □

For a polynomial $P \in \mathbb{Z}[x_1, \ldots, x_m]$, we define its *height*, or *norm*, as the maximum absolute value of its coefficients. In other words, if $P = \sum_I c_I \boldsymbol{x}^I$ we have $\|P\| = \max_I |c_I|$. The following two claims will be very useful when estimating the height of various polynomials in section 5.

Claim 3.2. *Let $P \in \mathbb{Z}[x_1, \ldots, x_m], Q \in \mathbb{Z}[x_{m+1}, \ldots, x_n]$ have independent variables. Then, one has $\|PQ\| = \|P\| \cdot \|Q\|$.*

Proof. Coefficients of PQ correspond to products of coefficients of P and Q as there is no cancellations. Hence, the conclusion follow immediately. □

Claim 3.3. *(Gelfond's lemma) Let $P_1, \ldots, P_n \in \mathbb{Z}[x_1, \ldots, x_m]$ be any polynomials, and let $P = \prod_{j=1}^n P_j$. Then, $\|P\| \leq 2^d \prod_{j=1}^n \|P_j\|$, where d is the sum of partial degrees of P.*

Proof. Let us introduce the notation $P_j = \sum_{\boldsymbol{\mu}} c_{\boldsymbol{\mu}}^{(j)} \boldsymbol{x}^{\boldsymbol{\mu}}$. Then,

$$P = \prod_{j=1}^n \sum_{\boldsymbol{\mu}} c_{\boldsymbol{\mu}}^{(j)} \boldsymbol{x}^{\boldsymbol{\mu}} = \sum_{\boldsymbol{\mu}_1, \ldots, \boldsymbol{\mu}_n} \Big(\prod_{j=1}^n c_{\boldsymbol{\mu}}^{(j)} \Big) \boldsymbol{x}^{\boldsymbol{\mu}_1 + \cdots + \boldsymbol{\mu}_n}.$$

Each of the products $\Big(\prod_{j=1}^n c_{\boldsymbol{\mu}}^{(j)} \Big)$ is bounded by $\prod_{j=1}^n \|P_j\|$. The number of n-tuples $(\boldsymbol{\mu}_1, \ldots, \boldsymbol{\mu}_n)$ with the same $\boldsymbol{\mu}_1 + \cdots + \boldsymbol{\mu}_n$ is at most the number of all monomials in the full expansion of $\prod_j P_j$, which is $\prod_{j=1}^n \prod_{i=1}^m (1 + \deg_i P_j) < 2^d$. Therefore, the coefficients of the resulting polynomial are bounded by $2^d \prod_{j=1}^n \|P_j\|$, which completes the proof. □

4 Constructing the auxiliary polynomial

The goal for this section is to construct a polynomial $P \in \mathbb{Z}[x_1, \ldots, x_m]$ which has bounded degree, high index at $(\alpha, \ldots, \alpha)$ and relatively small coefficients.

Lemma 4.1. *Let $\alpha \in \mathbb{R}$ be an algebraic integer of degree r and let $\varepsilon > 0, m > r\varepsilon^{-2}$. Set $t = \Big(\frac{1}{2} - \epsilon\Big)m$, and let $d_1, \ldots, d_m$ be big enough. Then, there exists a nontrivial polynomial $P \in \mathbb{Z}[x_1, \ldots, x_m]$ and a constant $C = C(\alpha) > 0$ such that $\deg_i P \leq d_i$ for $i = 1, \ldots, m$, $\operatorname{ind}\big(P; (d_1, \ldots, d_m), (\alpha, \ldots, \alpha)\big) \geq t$, and $\|P\| \leq 2^{C \sum_{i=1}^m d_i}$.*

Proof. The idea of the proof is to first write P as a polynomial with undetermined coefficients, and to impose a set of linear equations on the coefficients which will ensure that the index of P at $(\alpha, \ldots, \alpha)$ is big enough. Using Siegel's lemma to find a small solution to the resulting set of equations, we will be able to show P can be chosen to have small coefficients.

Let us write $P(x_1, \ldots, x_m) = \sum_I c_I \boldsymbol{x}^I$, where $c_I \in \mathbb{Z}$ are coefficients to be determined. In order to ensure the index of P at $(\alpha, \ldots, \alpha)$ is high, P must satisfy $\partial_{\boldsymbol{\mu}} P(\alpha, \ldots, \alpha) = 0$ for all multi-indices $\boldsymbol{\mu}$ of index $\leq t$. Expanded in terms of the coefficients, these equations take the form $\sum_I c_I \binom{i_1}{\mu_1} \cdots \binom{i_m}{\mu_m} \alpha^{(i_1-\mu_1)+\cdots+(i_m-\mu_m)} = 0$.

If the goal is to find small integer solution c_I to the above system, there are three issues we need to take care of. First, the coefficients of linear equations are not rational numbers, and therefore we need to justify why non-trivial integer solutions exist. Second, we need to compare the number of variables c_I and equations, and finally we need to bound the size of the coefficients in the equations.

To address the first point, note that α is an algebraic integer of degree r. This means α^r is a integer linear combination of $\alpha^{r-1}, \dots, \alpha, 1$. Moreover, the size of the coefficients of this integer combination is at most $\|f\|$, where f is the minimal polynomial of α. Therefore, one can replace the highest power of α in every equation by the lower powers of α until only $\alpha^{r-1}, \dots, \alpha, 1$ are left in the equation. After replacing a single power of α by smaller ones, the coefficients of the equation increase at most $\|f\|$ times. Hence, after forming the new equations, the coefficients have increased at most $\|f\|^{d_1+\dots+d_m}$ times, as $\alpha^{d_1+\dots+d_m}$ is the highest power of α appearing in the equations.

After being left only with r lowest powers of α, the idea is to group the terms of every equation into r brackets, depending on which power of α the terms contain. As the first r powers of α are linearly independent, it is natural to split every equation into r new ones, setting every bracket of every equation to 0. Now, all coefficients of the new equations are integers, and thus we proceed to count how many equations there are.

As the last step only multiplies the number of equations by r, we need to count how many equations we originally had. This is precisely equal to the number of multi-indices $\boldsymbol{\mu}$ of index $\leq t$. The following lemma counts how many such indices there are.

Lemma 4.2. *Let $d_1, \dots, d_m \in \mathbb{Z}$ be integers and let $\epsilon > 0$. Let $T(\epsilon)$ be the number of m-tuples $(\mu_1, \dots, \mu_m) \in \mathbb{Z}^m$ with $0 \leq \mu_i \leq d_i$ and $\sum_{i=1}^m \frac{\mu_i}{d_i} \leq m\big(\frac{1}{2} - \epsilon\big)$. Then,*

$$T(\varepsilon) \leq \frac{1}{24m\epsilon^2} \prod_{i=1}^m (d_i + 1).$$

Proof. The idea is to think of μ_i as random variables uniformly distributed on $\{0, \dots, d_i\}$. From this perspective $\frac{T(\epsilon)}{\prod_{i=1}^m (1+d_i)}$ corresponds to the probability $\sum_{i=1}^m \frac{\mu_i}{d_i} \leq m\big(\frac{1}{2} - \epsilon\big)$. To bound this probability, we use standard probability theory techniques.

The expectation of $\sum_{i=1}^m \frac{\mu_i}{d_i}$ is $\mathbb{E}[\sum_{i=1}^m \frac{\mu_i}{d_i}] = \sum_{i=1}^m \frac{\mathbb{E}[\mu_i]}{d_i} = \frac{m}{2}$. On the other hand, the variance of this variable is:

$$\mathbb{V}[\sum_{i=1}^m \frac{\mu_i}{d_i}] = \sum_{i=1}^m \frac{\mathbb{V}[\mu_i]}{d_i^2} = \sum_{i=1}^m \frac{d_i^2 - 1}{12 d_i^2} \leq \frac{m}{12}.$$

Therefore, Chebyshev's inequality completes the proof:

$$\mathbb{P}\left[\sum_{i=1}^m \frac{\mu_i}{d_i} \leq m\Big(\frac{1}{2} - \epsilon\Big)\right] = \frac{1}{2}\mathbb{P}\left[\Big|\sum_{i=1}^m \frac{\mu_i}{d_i} - \frac{m}{2}\Big| \geq m\epsilon\right] \leq \frac{1}{2}\frac{\mathbb{V}\big[\sum_{i=1}^m \frac{\mu_i}{d_i}\big]}{m^2\epsilon^2} \leq \frac{1}{24m\epsilon^2}.$$

□

Remark. The bounds from this lemma can be significantly improved by using Chernoff bounds instead of Chebyshev inequality. However, the key takeaway from this lemma is that by increasing m, one can make $\frac{T(\epsilon)}{\prod_{i=1}^m (1+d_i)}$ arbitrarily small. Thus, the exact bounds themselves bear no significance, we opt for a more elementary proof.

The above lemma now allows us to conclude there are $M \leq \frac{r}{24m\epsilon^2} \prod_{i=1}^m (d_i + 1) \leq \frac{1}{24} \prod_{i=1}^m (d_i + 1)$ equations. On the other hand, there are $N = \prod_{i=1}^m (d_i + 1)$ undetermined coefficients c_I. Finally, the coefficients of original equations had size at most $2^{\sum_{i=1}^m d_i}$, and they were increased at most $\|f\|^{\sum_{i=1}^m d_i}$ times, implying the size of the final coefficients can be bounded by $T = (2\|f\|)^{\sum_{i=1}^m d_i}$. Having all these prerequisites, the final ingredient of the proof is Siegel's lemma, which ensures that we can find small c_I solving the above system.

Lemma 4.3. *(Siegel's lemma) Consider a linear system of M equations of the form $\sum_{j=1}^N A_{i,j} x_j = 0$, for $i = 1, \dots, M$. If $A_{i,j}$ are integers of norm bounded by T, then there exists an integer solution $\boldsymbol{x} \in \mathbb{Z}^n$ with $\max_i |x_i| \leq 2(3NT)^{\frac{M}{N-M}}$.*

Proof. The proof relies on the Pigeonhole principle. The idea of the proof is to find a vector $\boldsymbol{x}$ in a box $[-K, K]^N \subset \mathbb{R}^N$ such that $A\boldsymbol{x} = 0^M$. We do this by finding two vectors with the same image and subtracting them.

More precisely, let $K = (3NT)^{\frac{M}{N-M}}$ and define the boxes $B_1 = \{\boldsymbol{x} \in \mathbb{R}^n | -K \leq |x_i| \leq K\}$, $B_2 = \{\boldsymbol{y} \in \mathbb{R}^M | -NTK \leq |y_i| \leq NTK\}$. First, note that $A\boldsymbol{x} \in B_2$ for $\boldsymbol{x} \in B_1$, because:

$$|(Ax)_j| = |\sum_{i=1}^{N} A_{ij}x_i| \leq N \max_i |A_{ij}| \max_i |x_i| \leq NTK.$$

The definition of K and an easy computation shows B_2 has less integer points than B_1. Hence, by Pigeonhole principle, there are vectors $\boldsymbol{x}_1, \boldsymbol{x}_2 \in B_1$ with $A\boldsymbol{x}_1 = A\boldsymbol{x}_2$. If we let $\boldsymbol{x} = \boldsymbol{x}_1 - \boldsymbol{x}_2$, it is clear that $A\boldsymbol{x} = 0^M$ and $\max_i |x_i| \leq 2K = 2(3NT)^{\frac{N}{N-M}}$, completing the proof. □

The above lemma directly applies to the problem at hand, and thus there exist the coefficients c_I solving the constructed system and having size at most

$$|c_I| \leq 2\Big(3\prod_{i=1}^{m}(1+d_i)(2\|f\|)^{\sum_{i=1}^m d_i}\Big)^{\frac{M}{N-M}} \leq 2^{C\sum_{i=1}^m d_i},$$

because $M \leq \frac{1}{24}N$. This completes the proof and constructs the auxiliary polynomial. □

5 Roth's lemma

The main ingredient of the proof is Roth's lemma, which serves to bound the the index of a polynomial at a rational point of large height near $(\alpha, \ldots, \alpha)$. More precisely, we have the following statement:

Lemma 5.1. *(Roth's lemma) Let $P \in \mathbb{Z}[x_1, \ldots, x_m]$ be the auxiliary polynomial for which $\deg_i P \leq d_i$, with $d_1, \ldots, d_m \in \mathbb{Z}_{>0}$. Also, let $0 < \sigma \leq \frac{1}{2}$ and $(\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}) \in \mathbb{Q}^m$ such that the following assumptions are satisfied:*

- *for $i = 1, \ldots, m-1$, we have $\sigma d_i \geq d_{i+1}$, and*
- *for $i = 1, \ldots, m$ we have $q_i^{d_i} \geq 2^{4md_1\sigma^{-1}}\|P\|^{\sigma^{-1}}$.*

Then, $\operatorname{ind}(P; \boldsymbol{d}, (\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m})) \leq 2m\sigma^{\frac{1}{2^{m-1}}}$.

Before passing to the proof of this lemma, we show an auxiliary claim about linearly independent polynomials and their Wronskians. This lemma is classical and our proof is based on [3].

Lemma 5.2. *Let $h_1, \ldots, h_n \in \mathbb{Z}[x_1, \ldots, x_m]$ be arbitrary polynomials. These polynomials are linearly independent over $\mathbb{Q}$ if and only if there exist multi-indices $\boldsymbol{\mu}_1, \ldots, \boldsymbol{\mu}_n$ such that $|\boldsymbol{\mu}_i| \leq i-1$ and the Wronskian $W_{\boldsymbol{\mu}_1,\ldots,\boldsymbol{\mu}_n} = \det\left(\partial_{\boldsymbol{\mu}_i} h_j\right)_{i,j=1,\ldots,n}$ is not identically zero.*

Proof. Suppose first that $h_1, \ldots, h_n$ are linearly dependent, i.e. that there exist scalars $c_1, \ldots, c_n \in \mathbb{Q}$, not all zero, for which $\sum_{i=1}^n c_i h_i = 0$. The goal is to show that any Wronskian $W_{\boldsymbol{\mu}_1,\ldots,\boldsymbol{\mu}_n}$ vanishes identically. Then, applying $\boldsymbol{\mu}_j$ derivative to the above equation gives $\sum_{i=1}^n c_i \partial_{\boldsymbol{\mu}_j} h_i = 0$. This shows that the columns of the matrix defining $W_{\boldsymbol{\mu}_1,\ldots,\boldsymbol{\mu}_n}$ are linearly dependent, which means $W_{\boldsymbol{\mu}_1,\ldots,\boldsymbol{\mu}_n}$ vanishes identically.

Next, consider the case when h_j are linearly independent. The first step is to reduce the multivariate case to the univariate one. To this end, we have the following claim:

Claim 5.1. *Choose an integer $d \in \mathbb{Z}_{>0}$ bigger than the partial degrees of h_j, $d > \max_{i,j} \deg_i h_j$. Then, the polynomials $H_j(t) = h_j(t, t^d, \ldots, t^{d^{m-1}}) \in \mathbb{Z}[t]$ for $j = 1, \ldots, n$ are linearly independent if $h_j(x_1, \ldots, x_m) \in \mathbb{Z}[x_1, \ldots, x_m]$ are linearly independent.*

Proof. First, note that the mapping $x_1^{k_1} \ldots x_m^{k_m} \mapsto t^{\sum_{i=1}^m k_i d^{i-1}}$ is injective by the assumption on d. Therefore, the monomials appearing in $h_j(x_1, \ldots, x_m)$ and $H_j(t)$ are in one-to-one correspondence.

Suppose polynomials H_j are not independent, i.e. there exists scalars $c_1, \ldots, c_n \in \mathbb{Q}$, not all zero, such that $\sum_{j=1}^n c_j H_j(t) = 0$. Then, for every exponent $k = \sum_{i=1}^m k_i d^{i-1}$ we have $\sum_{j=1}^n c_j [t^k] H_j = 0$,

where $[t^k]H_j$ stands for the coefficient of t^k in H_j. Using the one-to-one correspondence established above we have $\sum_{j=1}^{n} c_j[x_1^{k_1}\dots x_m^{k_m}]h_j = 0$. Summing over all monomials $x_1^{k_1}\dots x_m^{k_m}$ now gives the linear dependency of polynomials h_j, implying a contradiction.[1] □

In case of univariate polynomials, a simple criterion checks linear independence.

Claim 5.2. *If the polynomials $H_1, \dots, H_n \in \mathbb{Q}[t]$ are linearly independent, the Wronskian defined by $W(t) = \det\left(\left(\frac{d}{dt}\right)^{i-1} H_j(t)\right)_{i,j=1,\dots,n}$ is not identically zero.*

Proof. Before computing the Wronskian, we will alter the polynomials H_j slightly. The idea is that adding to one of the polynomials H_j a linear combination of H_i with $i \neq j$ does not change the Wronskian. More precisely, for any choice of scalars $c_i \in \mathbb{Q}$, replacing $H_j \mapsto H_j + \sum_{i\neq j} c_i H_i$ will not change the Wronskian. Therefore, by performing appropriate operations, we may assume that the lowest order terms of all H_j are of different degree.

Linear independence guarantees that the polynomials will remain non-zero throughout this process, meaning every $H_j(t)$ will have a well defined lowest order term. In other words, we may write $H_j(t) = a_j t^{b_j}(1 + tF_j(t))$, for some polynomials $F_j \in \mathbb{Q}[t]$. Their derivatives will now have the form

$$\left(\frac{d}{dt}\right)^i H_j(t) = a_j (b_j)_i t^{b_j - i}(1 + tG_{i,j}(t)),$$

where $(b_j)_i = b_j(b_j - 1)\cdots(b_j - i + 1)$ denotes the falling factorial and $G_{i,j}(t) \in \mathbb{Q}[t]$. Using this, one can get an expression for the Wronskian determinant as:

$$\begin{aligned} W(t) &= \det\left(a_j (b_j)_{i-1} t^{b_j - i + 1}(1 + tG_{i-1,j}(t))\right)_{i,j=1,\dots,n} \\ &= \left(\prod_{j=1}^{n} a_j\right) t^{b_1 + \dots + b_n - \binom{n}{2}} \det\left((b_j)_{i-1}(1 + tG_{i-1,j}(t))\right)_{i,j=1,\dots,n}. \end{aligned} \tag{3}$$

The identity (3) follows directly from the permutation expansion, by noting that every term contains exactly $b_1 + \dots + b_n - \binom{n}{2}$ power of t.

As our goal showing that Wronskian is not zero, note that first two factors are clearly nonzero, while the final determinant modulo t corresponds to the determinant $D = \det\left((b_j)_{i-1}\right)_{i,j=1,\dots,n}$.

To see why this determinant is nonzero for pairwise distinct b_j, it is useful to define the polynomials $p_i(x) = (x)_i = x(x-1)\dots(x-i+1)$ and note $D = \det\left(p_{i-1}(b_j)\right)_{i,j=1,\dots,n}$. Note that polynomials $p_0, \dots, p_{n-1}$ all have different degrees and therefore are linearly independent. As they all belong to a space of dimension n, they form a basis for it. Elementary linear algebra now shows that the basis $1, x, \dots, x^{n-1}$ of this space can be obtained from $p_0, \dots, p_{n-1}$ through elementary operations. In other words, the determinant D can be transformed into the Vandermonde determinant using elementary operations, and the Vandermonde determinant is clearly nonzero as the integers b_j are distinct.

Therefore, the determinant $D \neq 0$, which implies $\det\left((b_j)_{i-1}(1 + tP_{i-1,j}(t))\right)_{i,j=1,\dots,n}$ is nonzero modulo t and therefore nonzero in general. Finally, using equation (3), we conclude $W(t)$ is also not identically zero, which completes the proof of the claim. □

To complete the proof of the lemma 5.2 is now relatively straightforward. The idea is to express the Wronskian of $H_1, \dots, H_n$ using the Wronskians $W_{\boldsymbol{\mu}_1,\dots,\boldsymbol{\mu}_n}$ of $h_1, \dots, h_n$. To do that, note first that the derivatives $\left(\frac{d}{dt}\right)^{i-1} H_j(t)$ can be expressed as a linear combination of $\partial_{\boldsymbol{\mu}} h_j$ for $|\boldsymbol{\mu}| \leq i-1$. In other words, a simple induction and chain rule show there exist polynomials $p_{i,\boldsymbol{\mu}}(t)$ depending on d, m but not on $h_1, \dots, h_n$ such that:

$$\left(\frac{d}{dt}\right)^{i-1} H_j(t) = \sum_{|\boldsymbol{\mu}| \leq i-1} p_{i,\boldsymbol{\mu}}(t) \partial_{\boldsymbol{\mu}} h_j(t, \dots, t^{d^{m-1}}). \tag{4}$$

[1] It is not hard to see that this proof actually shows that linear independence of H_j implies linear independence of h_j, but we skip this because it is not necessary for the main proof.

Using (4), it is easy to express the Wronskian $W(t)$ as:

$$\begin{aligned} W(t) &= \det\Big(\big(\frac{d}{dt}\big)^{i-1} H_j(t)\Big)_{i,j=1,\ldots,n} = \det\big(\sum_{|\boldsymbol{\mu}|\le i-1} p_{i,\boldsymbol{\mu}}(t)\partial_{\boldsymbol{\mu}} h_j(t,\ldots,t^{d^{m-1}})\big)_{i,j=1,\ldots,n} \\ &= \sum_{\substack{\boldsymbol{\mu}_1,\ldots,\boldsymbol{\mu}_n \\ |\boldsymbol{\mu}_i|\le i-1}} p_{1,\boldsymbol{\mu}_1}(t)\cdots p_{n,\boldsymbol{\mu}_n}(t)\det\big(\partial_{\boldsymbol{\mu}_i} h_j(t,\ldots,t^{d^{m-1}})\big)_{i,j=1,\ldots,n} \\ &= \sum_{\substack{\boldsymbol{\mu}_1,\ldots,\boldsymbol{\mu}_n \\ |\boldsymbol{\mu}_i|\le i-1}} p_{1,\boldsymbol{\mu}_1}(t)\cdots p_{n,\boldsymbol{\mu}_n}(t) W_{\mu_1,\ldots,\mu_n}(t,t^d,\ldots,t^{d^{m-1}}) \end{aligned}$$

If the Wronskian $W(t)$ is not identically zero, it must be that one of the terms of the right hand side is also nonzero. This shows the existence of multi-indices $\boldsymbol{\mu}_1,\ldots,\boldsymbol{\mu}_n$ for which $W_{\boldsymbol{\mu}_1,\ldots,\boldsymbol{\mu}_n}(x_1,\ldots,x_m)$ is nonzero, which completes the proof of the lemma. □

Proof of Roth's lemma. The proof proceeds by induction on the number of variables. First, we deal with case $m = 1$.

If $t = \operatorname{ind}(P;\boldsymbol{d},\frac{p_1}{q_1})$, we have $\left(x_1 - \frac{p_1}{q_1}\right)^{td_1} | P(x_1)$, and therefore Gauss' lemma gives $(q_1x_1 - p_1)^{t_1 d} | P(x_1)$. Looking at the highest order coefficient in P implies $\|P\| \ge q_1^{td_1}$. Combining this with the assumption $q_1^{d_1} \ge 2^{4d_1\sigma^{-1}}\|P\|^{\sigma^{-1}}$, we infer $q_1 \ge 2^{2\sigma^{-1}} q_1^{t\sigma^{-1}}$, i.e. $t \le \sigma$. This provides a slightly better bound, $\operatorname{ind}(P;\boldsymbol{d},\frac{p_1}{q_1}) \le \sigma$, the improvement which we will use later.

In case $m > 1$, we represent P as a linear combination $P = \sum_{j=0}^{s} f_j(x_1,\ldots,x_{m-1})g_j(x_m)$, with minimal s. Note that minimality of s implies that $\{f_j\},\{g_j\}$ are linearly independent. Therefore, by the preliminary lemma, there exist multi-indices $\boldsymbol{\mu}_0,\ldots,\boldsymbol{\mu}_s$ with $|\boldsymbol{\mu}_i| \le i$ and the following nonzero Wronskians:

$$U(x_1,\ldots,x_{m-1}) = \det\big(\partial_{\boldsymbol{\mu}_i} f_j\big)_{i,j=0,\ldots,s} \ne 0, \qquad V(x_m) = \det\big(\partial_\nu g_j\big)_{\nu,j=0,\ldots,s} \ne 0.$$

Note that multiplying U and V yields a nonzero polynomial W of the form

$$W(x_1,\ldots,x_m) = U(x_1,\ldots,x_{m-1})V(x_m) = \det\big(\partial_{\boldsymbol{\mu}_i,\nu} P\big)_{i,\nu=0,\ldots,s}. \tag{5}$$

The polynomial W turns out to be very useful in upper bounding the index of P. Therefore, after showing the relation between these two indices, we turn to bounding the index of W from above by inductively applying Roth's lemma to U and V. Combining these two bounds will complete the inductive step.

In what is to follow, we will fix the degree sequence $\boldsymbol{d}$ and the point $\left(\frac{p_1}{q_1},\ldots,\frac{p_m}{q_m}\right)$ and denote $\operatorname{ind}(f;\boldsymbol{d},\left(\frac{p_1}{q_1},\ldots,\frac{p_m}{q_m}\right))$ simply by $\operatorname{ind}(f)$, for a polynomial $f \in \mathbb{Z}[x_1,\ldots,x_m]$.

Claim 5.3. *For W defined as above,* $\operatorname{ind}(W) \ge (s+1)\big(\frac{1}{2}\min(\operatorname{ind}(P),\operatorname{ind}(P)^2) - \sigma\big)$.

Proof. By the properties given in claim 3.1, if $j \in \{0,\ldots,s\}$:

$$\operatorname{ind}(\partial_{\boldsymbol{\mu}_j,\nu} P) \ge \operatorname{ind}(P) - \sum_{i=1}^{m-1}\frac{\mu_{ji}}{d_i} - \frac{\nu}{d_m} \ge \operatorname{ind}(P) - \frac{|\boldsymbol{\mu}_j|}{d_{m-1}} - \frac{\nu}{d_m}$$

Note that $|\boldsymbol{\mu}_j| \le s$ by definition of the Wronskian and $s \le d_m$ as $\{g_j\}$ is a family of $s+1$ linearly independent polynomials of degree $\le d_m$. Therefore,

$$\operatorname{ind}(\partial_{\boldsymbol{\mu}_j,\nu} P) \ge \operatorname{ind}(P) - \frac{|\boldsymbol{\mu}_j|}{d_{m-1}} - \frac{\nu}{d_m} \ge \operatorname{ind}(P) - \frac{\nu}{d_m} - \frac{d_m}{d_{m-1}} \ge \max\big(\operatorname{ind}(P) - \frac{\nu}{d_m}, 0\big) - \sigma,$$

where the last inequality follows from the fact index must always be nonnegative. The last bound can be used to control the indices of W and P using claim 3.1 and the permutation expansion of the

determinant from (5):

$$\operatorname{ind}(W) \geq \min_{\pi \in S_{s+1}} \sum_{i=0}^{s} \operatorname{ind}(\partial_{\boldsymbol{\mu}_i, \pi(i)} P) \geq \min_{\pi \in S_{s+1}} \sum_{i=0}^{s} \Big[\max\big(\operatorname{ind}(P) - \frac{\pi(i)}{d_m}, 0\big) - \sigma \Big]$$

$$\operatorname{ind}(W) \geq \sum_{i=0}^{s} \max\big(\operatorname{ind}(P) - \frac{i}{s}, 0\big) - \sigma(s+1)$$

Finally, we want to bound $\sum_{i=0}^{s} \max\big(\operatorname{ind}(P) - \frac{i}{s}, 0\big)$. In case $\operatorname{ind}(P) \geq 1$, we have:

$$\sum_{i=0}^{s} \max\big(\operatorname{ind}(P) - \frac{i}{s}, 0\big) = (s+1)\operatorname{ind}(P) - \frac{s(s+1)}{2s} \geq (s+1)\frac{\operatorname{ind}(P)}{2}.$$

In case $\operatorname{ind}(P) < 1$, we can write $\operatorname{ind}(P) = \frac{k}{s} + \lambda$, for $k \leq s-1, 0 \leq \lambda < \frac{1}{n}$. Then,

$$\sum_{i=0}^{s} \max\big(\operatorname{ind}(P) - \frac{i}{s}, 0\big) = (s+1)\lambda + \frac{k(k+1)}{2s} \geq \frac{s+1}{2}\Big(\frac{k}{s} + \lambda\Big)^2,$$

where the last inequality follows by expanding the square and cancelling the remaining terms. Combining the previous three equations, we finally get:

$$\operatorname{ind}(W) \geq \frac{s+1}{2} \min\big(\operatorname{ind}(P), \operatorname{ind}(P)^2\big),$$

which completes the proof of this claim. □

On the other hand, one can bound $\operatorname{ind}(W)$ from above using the induction hypothesis, which is shown in the following claim.

Claim 5.4. *For W defined as above,* $\operatorname{ind}(W) \leq 2(m-1)(s+1)\sigma^{1/2^{m-2}} + (s+1)\sigma$.

Proof. As $W = U \cdot V$, claim 3.1 implies

$$\operatorname{ind}(W; \boldsymbol{d}, \Big(\frac{p_1}{q_1}, \ldots, \frac{p_m}{q_m}\Big)) = \operatorname{ind}(U; (d_1, \ldots, d_{m-1}), \Big(\frac{p_1}{q_1}, \ldots, \frac{p_{m-1}}{q_{m-1}}\Big)) + \operatorname{ind}(V; d_m, \frac{p_m}{q_m}).$$

Our goal is now to analyze the indices of U, V as given above. Before applying Roth's lemma, we need to bound the norms of U, V. To this end, we recall claim 3.2 gives $\|U\|\|V\| = \|W\|$. One can also show $\|W\| \leq 2^{4d_1(s+1)}\|P\|^{s+1}$ as follows.

If we let $d = \sum_{i=1}^{m} \deg_i P$, Gelfond's lemma (claim 3.3) implies:

$$\|W\| = \|\sum_{\pi \in S_{s+1}} \prod_{j=0}^{s} \partial_{\boldsymbol{\mu}_i, \pi(i)} P\| \leq (s+1)! \max_{\pi \in S_{s+1}} \|\prod_{j=0}^{s} \partial_{\boldsymbol{\mu}_i, \pi(i)} P\| \leq (s+1)! \max_{\pi \in S_{s+1}} 2^d \prod_{j=0}^{s} \|\partial_{\boldsymbol{\mu}_i, \pi(i)} P\|$$

As $\partial_{\boldsymbol{\mu}_i, \pi(i)} \boldsymbol{x}^I = \binom{i_1}{\mu_1} \cdots \binom{i_m}{\pi(i)} \boldsymbol{x}^{I - \boldsymbol{\mu}}$, we have the bound $\|\partial_{\boldsymbol{\mu}_i, \pi(i)} P\| \leq 2^d \|P\|$. Using that $\sigma \leq \frac{1}{2}$ implies $d \leq 2d_1$, we now have the bound on $\|W\|$:

$$\|W\| \leq (s+1)! \max_{\pi \in S_{s+1}} 2^d \prod_{j=0}^{s} \|\partial_{\boldsymbol{\mu}_i, \pi(i)} P\| \leq 2^{2s^2} 2^{2d_1} 2^{2d_1(s+1)} \|P\|^{s+1} \leq 2^{4d_1(s+1)} \|P\|^{s+1}. \tag{6}$$

As $\|U\|\|V\| = \|W\|$, we have $\|U\| \leq \|W\|, \|V\| \leq \|W\|$, and therefore the bound (6) suffices to to apply the induction hypothesis on U, V. First, let us define a new degree sequence with respect to which their indices will be calculated. Let $d'_i = (s+1)d_i$ and let $\boldsymbol{d}' = (d'_1, \ldots, d'_{m-1})$. Then, one can apply Roth's lemma to U, with the new degree sequence $\boldsymbol{d}'$, same σ and at the same point $(\frac{p_1}{q_1}, \ldots, \frac{p_{m-1}}{q_{m-1}})$. The degrees d'_i obviously still satisfy the assumptions, and we have $\deg_i U \leq d'_i, \deg_m V \leq d'_m$ because

U is a determinant of a $(s+1)\times(s+1)$ matrix with entries of partial degrees bounded by d_i. The second assumption is also satisfied because:

$$q_i^{(s+1)d_i} \geq 2^{4m(s+1)d_1\sigma^{-1}}\|P\|^{(s+1)\sigma^{-1}} \geq 2^{4(m-1)(s+1)d_1\sigma^{-1}}\|U\|^{\sigma^{-1}}.$$

Therefore, the conclusion of the lemma is:

$$\operatorname{ind}(U;\boldsymbol{d}',\left(\frac{p_1}{q_1},\ldots,\frac{p_{m-1}}{q_{m-1}}\right)) \leq 2(m-1)\sigma^{1/2^{m-2}}.$$

One can also check the improved version of the lemma in case $m=1$ applies to V, and hence $\operatorname{ind}(V;d'_m,\frac{p_m}{q_m})\leq\sigma$.

Relating these indices to the original degree sequence amounts to scaling the bounds by $s+1$, and therefore:

$$\operatorname{ind}(W;\boldsymbol{d},\left(\frac{p_1}{q_1},\ldots,\frac{p_m}{q_m}\right)) \leq 2(m-1)(s+1)\sigma^{1/2^{m-2}}+(s+1)\sigma,$$

which completes the proof of the claim. □

Combining the bounds for $\operatorname{ind}(W)$ from the previous two claims, we get:

$$\frac{s+1}{2}\left[\min\left(\operatorname{ind}(P),\operatorname{ind}(P)^2\right)-\sigma\right] \leq 2(m-1)(s+1)\sigma^{1/2^{m-2}}+(s+1)\sigma$$
$$\frac{1}{2}\min\left(\operatorname{ind}(P),\operatorname{ind}(P)^2\right) \leq 2(m-1)\sigma^{1/2^{m-2}}+2\sigma$$

The last equation gives $\min\left(\operatorname{ind}(P),\operatorname{ind}(P)^2\right)\leq 4m\sigma^{1/2^{m-2}}$. From the definition of the index, it is clear $\operatorname{ind}(P)\leq m$ and therefore $\operatorname{ind}(P)^2\leq 4m^2\sigma^{1/2^{m-2}}$. Taking the square root of the last bound finally completes the proof of Roth's lemma. □

6 Completing the proof

Having constructed the auxiliary polynomial and proven Roth's lemma, we are now ready to put together all the pieces and prove Roth's theorem.

Proof. The idea of the proof is to assume the contrary, i.e. that there are infinitely many good approximations $\frac{p}{q}$, and choose a sequence of m rationals $\frac{p_1}{q_1},\ldots,\frac{p_m}{q_m}$ with increasing denominators. Then, we will construct the auxiliary polynomial having high index at α, using the arguments from section 4. The goal will be to show that this auxiliary polynomial P does not have high index at the point $\left(\frac{p_1}{q_1},\ldots,\frac{p_m}{q_m}\right)$, which will ultimately provide a contradiction.

Before using the lemma we proved earlier, we will first fix their parameters based on ε. First, pick $\epsilon>0$ such that $(2+\varepsilon)(\frac{1}{2}-3\epsilon)>1$, $m>r\epsilon^{-2}$ and fix $\sigma=\epsilon^{2^{m-1}}$. Then, choose two parameters $M=\sigma^{-1}$ and $L\geq(4m+2C)\sigma^{-1}$, where $C=C(\alpha)>0$ is the constant produced by lemma 4.1. We will have one more condition on L, but we postpone the precise bound because it would be unnatural to state it now. Using these parameters and the assumption there are infinitely many rational solutions to equation (1), we can find a sequence of m solutions $\frac{p_1}{q_1},\ldots,\frac{p_m}{q_m}$ satisfying $q_1\geq 2^L, q_{i+1}\geq q_i^M$. With these q_i fixed, we choose the degrees sequence of our auxiliary polynomial to be $d_i=\frac{D}{\log q_i}$, where D is a very big integer we will let go to infinity at the end of the proof. It may be that d_i defined in this way are not integers, but this is only a technical point which does not alter the essence of the proof - one may round them to the nearest integer.

Having fixed the above parameters, use lemma 4.1 to construct a polynomial P with $\deg_i P\leq d_i$, $\operatorname{ind}\left(P;(d_1,\ldots,d_m),(\alpha,\ldots,\alpha)\right)\geq\left(\frac{1}{2}-\epsilon\right)m$, and coefficients of controlled size, $\|P\|\leq 2^{C\sum_{i=1}^m d_i}$.

Before applying Roth's lemma, we need to check its assumptions. The first one, $\sigma d_i\geq d_{i+1}$ directly follows from $\log q_{i+1}>M\log q_i=\sigma^{-1}\log q_i$. On the other hand, to verify the second assumption we need to check that $2^{4md_1\sigma^{-1}}\|P\|^{\sigma^{-1}}\leq q_i^{d_i}$. Recalling the bounds on $\|P\|$, this reduces to $2^{4md_1\sigma^{-1}}\|P\|^{\sigma^{-1}}\leq 2^{4md_1\sigma^{-1}}2^{C\sigma^{-1}\sum_{i=1}^m d_i}$. As $d_i=D/\log q_i$, and $\log q_i\geq LM^{i-1}$, we further

have the inequality $2^{4md_1\sigma^{-1}}2^{C\sigma^{-1}\sum_{i=1}^m d_i} \leq 2^{\frac{D}{L}\sigma^{-1}\left(4m+C\frac{M}{M-1}\right)}$. Finally, from the choice of L, as $L > (4m+2C)\sigma^{-1}$, we have $2^{\frac{D}{L}\sigma^{-1}\left(4m+C\frac{M}{M-1}\right)} \leq 2^D = q_i^{d_i}$, which checks the second condition.

Applying Roth's lemma now ensures $\operatorname{ind}(P; \boldsymbol{d}, (\frac{p_1}{q_1}, \dots, \frac{p_m}{q_m})) \leq 2m\sigma^{\frac{1}{2^{m-1}}}$. This means there exists a multi-index $\boldsymbol{\mu}$ of index $\leq 2m\sigma^{1/2^{m-1}} = 2m\epsilon$ and $\partial_{\boldsymbol{\mu}} P(\frac{p_1}{q_1}, \dots, \frac{p_m}{q_m}) \neq 0$.

Therefore, we set $Q = \partial_{\boldsymbol{\mu}} P$ and note that the index of Q at $(\alpha, \dots, \alpha)$ remain high, $\geq \left(\frac{1}{2} - 3\epsilon\right)m$, and Q does not vanish at $(\frac{p_1}{q_1}, \dots, \frac{p_m}{q_m})$. Moreover, Q has coefficients $\leq 2^{(C+1)\sum_{i=1}^m d_i}$. Giving lower and upper bounds on $Q(\frac{p_1}{q_1}, \dots, \frac{p_m}{q_m})$ now gives a contradiction.

First, note that the lower bound trivially follows from the non-vanishing property and the fact $\deg_i Q \leq d_i$:

$$Q\Big(\frac{p_1}{q_1}, \dots, \frac{p_m}{q_m}\Big) \geq \prod_{i=1}^m \frac{1}{q_i^{d_i}} \geq \frac{1}{2^{Dm}}$$

For the upper bound, we first write the Taylor expansion of Q around $(\alpha, \dots, \alpha)$. Note that all sums in the Taylor expansion are finite as Q is a polynomial:

$$\begin{aligned}
\Big|Q\Big(\frac{p_1}{q_1}, \dots, \frac{p_m}{q_m}\Big)\Big| &\leq \Big|\sum_{\boldsymbol{\mu}} \partial_{\boldsymbol{\mu}} Q(\alpha, \dots, \alpha)\Big(\frac{p_1}{q_1} - \alpha\Big)^{\mu_1} \cdots \Big(\frac{p_m}{q_m} - \alpha\Big)^{\mu_m}\Big| \\
&\leq \prod_{i=1}^m (d_i+1) \max_{\boldsymbol{\mu}: \sum_{i=1}^m \frac{\mu_i}{d_i} \geq (\frac{1}{2}-3\epsilon)m} |\partial_{\boldsymbol{\mu}} Q(\alpha, \dots, \alpha)| \prod_{i=1}^m \frac{1}{q_i^{(2+\varepsilon)\mu_i}} \\
&\leq 2^{\sum_{i=1}^m d_i} \max_{\boldsymbol{\mu}: \sum_{i=1}^m \frac{\mu_i}{d_i} \geq (\frac{1}{2}-3\epsilon)m} |\partial_{\boldsymbol{\mu}} Q(\alpha, \dots, \alpha)| \prod_{i=1}^m \frac{1}{q_i^{d_i(2+\varepsilon)\frac{\mu_i}{d_i}}} \\
&\leq 2^{\sum_{i=1}^m d_i} \frac{1}{2^{D(2+\varepsilon)\left(\frac{1}{2}-3\epsilon\right)m}} \max_{\boldsymbol{\mu}} |\partial_{\boldsymbol{\mu}} Q(\alpha, \dots, \alpha)|
\end{aligned}$$

The only term we still need to estimate is $\max_{\boldsymbol{\mu}} |\partial_{\boldsymbol{\mu}} Q(\alpha, \dots, \alpha)|$. To do this, we write $Q = \sum_{i_1, \dots, i_m} c_I \boldsymbol{x}^I$. Then,

$$\begin{aligned}
|\partial_{\boldsymbol{\mu}} Q(\alpha, \dots, \alpha)| &= \Big|\sum_I c_I \binom{i_1}{\mu_1} \cdots \binom{i_m}{\mu_m} \alpha^{(i_1-\mu_1)+\cdots+(i_m-\mu_m)}\Big| \\
&\leq \sum_I |c_I| \cdot 2^{\sum_{k=1}^m i_k} |\alpha|^{i_1+\cdots+i_m-|\boldsymbol{\mu}|} \\
&\leq \prod_{i=1}^m (1+d_i) \cdot 2^{(C+2)\sum_{i=1}^m d_i} \cdot \max\{|\alpha|, 1\}^{\sum_{i=1}^m d_i} \leq 2^{C'\sum_{i=1}^m d_i},
\end{aligned}$$

where $C' > 0$ is a constant depending solely on α. Combining the upper and lower bounds now gives:

$$\frac{1}{2^{Dm}} \leq Q\Big(\frac{p_1}{q_1}, \dots, \frac{p_m}{q_m}\Big) \leq \frac{2^{C''\sum_{i=1}^m d_i}}{2^{D(2+\varepsilon)\left(\frac{1}{2}-3\epsilon\right)m}}.$$

Bounding $\sum_{i=1}^m d_i \leq 2\frac{D}{L}$ and letting $D \to \infty$ now gives $m \geq (2+\varepsilon)(\frac{1}{2} - 3\epsilon)m - \frac{2C''}{L}$. However, we may choose $L \geq L(\varepsilon, \epsilon, m)$ so that this inequality is not satisfied, because $(2+\varepsilon)(\frac{1}{2} - 3\epsilon) < 1$. Therefore, we have a contradiction and this finishes the proof of Roth's theorem.

□

References

[1] Enrico Bombieri and Walter Gubler, Heights in Diophantine geometry, New Mathematical Monographs, vol. 4, Cambridge University Press, Cambridge, 2006. MR2216774

[2] Michael Nakamaye, Roth's Theorem: an introduction to diophantine approximation, accessed on Jan 4th 2022 through:
https://mast.queensu.ca/ mikeroth/proceedings/Nakamaye-Roth-Method.pdf

[3] Alin Bostan, Philippe Dumas. Wronskians and linear independence. American Mathematical Monthly, Mathematical Association of America, 2010, 117 (8), pp.722-727. ff10.4169/000298910X515785ff. ffhal00780437f