On some problems in Transcendental number theory and Diophantine approximation

Ngoc Ai Van Nguyen

Thesis submitted to the
Faculty of Graduate and Postdoctoral Studies
in partial fulfillment of the requirements
for the Doctorate in Philosophy degree in Mathematics[1]

Department of Mathematics and Statistics
Faculty of Science
University of Ottawa

[1] The Ph.D. Program is a joint program with Carleton University, administered by the Ottawa-Carleton Institute of Mathematics and Statistics

Abstract

In the first part of this thesis, we present the first non-trivial small value estimate that applies to an algebraic group of dimension 2 and which involves large sets of points. The algebraic group that we consider is the product $\mathbb{C} \times \mathbb{C}^*$, of the additive group $\mathbb{C}$ by the multiplicative group $\mathbb{C}^*$. Our main result assumes the existence of a sequence $(P_D)_{D\geq 1}$ of non-zero polynomials in $\mathbb{Z}[X_1, X_2]$ taking small absolute values at many translates of a fixed point (ξ, η) in $\mathbb{C} \times \mathbb{C}^*$ by consecutive multiples of a rational point $(r, s) \in (\mathbb{Q}^*)^2$ with $s \neq \pm 1$. Under precise conditions on the size of the coefficients of the polynomials P_D, the number of translates of (ξ, η) and the absolute values of the polynomials P_D at these points, we conclude that both ξ and η are algebraic over $\mathbb{Q}$. We also show that the conditions that we impose are close from being best possible upon comparing them with what can be achieved through an application of Dirichlet's box principle.

In the second part of the thesis, we consider points of the form $\boldsymbol{\theta} = (1, \theta_1, \ldots, \theta_{d-1}, \xi)$ where $\{1, \theta_1, \ldots, \theta_{d-1}\}$ is a basis of a real number field K of degree $d \geq 2$ over $\mathbb{Q}$ and where ξ is a real number not in K. Our main results provide sharp upper bounds for the uniform exponent of approximation to $\boldsymbol{\theta}$ by rational points, denoted $\hat{\lambda}(\boldsymbol{\theta})$, and for its dual uniform exponent of approximation, denoted $\hat{\tau}(\boldsymbol{\theta})$. For $d = 2$, these estimates are best possible thanks to recent work of Roy. We do not know if they are best possible for other values of d. However, in Chapter 2, we provide additional information about rational approximations to such a point $\boldsymbol{\theta}$ assuming that its exponent $\hat{\lambda}(\boldsymbol{\theta})$ achieves our upper bound. In the course of the proofs, we introduce new constructions which are interesting by themselves and should be useful for future research.

Acknowledgements

First of all, I would like to express my deepest gratitude to my supervisor Professor Damien Roy for his direction, support, patience, and understanding.

I would like to thank the professors of the Ottawa-Carleton Institute of Mathematics and Statistics for teaching me and thank the staff of the Faculty of Science for helping and giving me a nice environment to study and work in.

I also sincerely thank to my former supervisors Professor Michel Waldschmidt (University of Paris VI) and Professor Bui Xuan Hai (University of Science Ho Chi Minh City) for providing me with the opportunity to study here and for having encouraged me for these years.

I am deeply grateful to all the Vaillancourt family and to Thu Huong Nguyen for giving me warmth, help and encouragement during my staying with them.

Last but not least, I would like to thank my family, especially my grandmother, parents, and my husband. Without their love, I would not have been able to complete this thesis.

Ottawa, September 2013

Ngoc Ai Van Nguyen

Dedication

First and foremost, I dedicate this work to my father to fulfill my last promise to him. Daddy, you left a void never to be filled in my life, but your memory always gave me strength whenever I was weak. I wish you could know that I am always proud of being your daughter.

Mama, although I cannot fill the void Dad left in you, I dedicate this work to you with hope that it will make you happier.

I also dedicate this to my grandmother, who is illiterate, but taught us the value of studying and worked hard to provide us with the opportunities to study.

Introduction

This thesis has two parts. In the first part, which is Chapter 1, we prove a new small value estimate for the group $\mathbb{C} \times \mathbb{C}^*$. This result provides necessary conditions for the existence of certain sequences of non-zero polynomials with integer coefficients taking small absolute values at points of $\mathbb{C} \times \mathbb{C}^*$. In the second part, divided in two chapters, we prove two new results of Diophantine approximation.

Part I.

We present the first non-trivial small value estimate that applies to an algebraic group of dimension 2 and which involves large sets of points. The algebraic group that we consider here is the product $\mathbb{C} \times \mathbb{C}^*$. Our main result shows that if there exists a sequence $(P_D)_{D\geq 1}$ of non-zero polynomials in $\mathbb{Z}[X_1, X_2]$ taking small absolute values at many translates of a fixed point (ξ, η) in $\mathbb{C} \times \mathbb{C}^*$ by multiples of a rational point $(r, s) \in (\mathbb{Q}^*)^2$ with $s \neq \pm 1$, then both ξ and η are algebraic over $\mathbb{Q}$. More precisely, for each integer $D \geq 1$, we request that P_D has degree at most D and norm at most e^{D^β} for some fixed number $\beta > 0$. The translates at which we evaluate P_D are points of the form $\underline{\gamma}_i = (\xi, \eta) + i(r, s)$ with $0 \leq i < 3\lfloor D^\sigma \rfloor$ where $\sigma > 1$ is fixed. We request that

$$|P_D(\underline{\gamma}_i)| \leq e^{-D^\nu} \qquad (0 \leq i < 3\lfloor D^\sigma \rfloor) \tag{1}$$

where ν is fixed. The conclusion that ξ and η are algebraic is then obtained by assuming that the parameters β, σ and ν satisfy the conditions

$$1 \leq \sigma < 2, \qquad \beta > \sigma + 1, \qquad \nu > \max\left\{\beta + 2 - \sigma + \frac{(\sigma - 1)(2 - \sigma)}{\beta - \sigma + 1},\ \sigma + 2\right\}. \tag{2}$$

An application of Dirichlet's Box principle shows that, given $(\xi,\eta),\ (r,s)\in\mathbb{C}\times\mathbb{C}^*$, there always exists such a sequence $(P_D)_{D\geq 1}$ satisfying condition (1) if $0\leq\sigma<2,\ \ \beta>\sigma+1$ and $\nu<\beta+2-\sigma$.

Since $(\sigma-1)(2-\sigma)/(\beta-\sigma+1)\leq 1/8$, the main lower bound that we impose on ν is weaker than

$$\nu\geq(\beta+2-\sigma)+\frac{1}{8}.$$

We do not know if the conditions (2) can be improved but this shows that if it is not best possible, the largest saving that we could achieve is no more than 1/8. Therefore, in a sense, it is close to be best possible.

We also show that, in order to reach the conclusion $\xi,\eta\in\overline{\mathbb{Q}}$, we need the parameter σ to be at least 1. Assuming that $\sigma<1,\beta>2\sigma$, we show the existence of a point (ξ,η) with algebraically independent coordinates for which there is a sequence $(P_D)_{D\geq 1}$ satisfying (1) for any $\nu>0$. This is a consequence of a construction of Khintchine–Philippon.

The proof of our main result is an adaption of the argument of D. Roy in [21]. In this paper, the author proves a similar result. He also considers a sequence $(P_D)_{D\geq 1}$ of polynomials in $\mathbb{Z}[X_1,X_2]$ of degree $\leq D$ and norm $\leq e^{D^\beta}$. The difference is that, these polynomials P_D are assumed to have the absolute values at most e^{-D^ν} at one point (ξ,η) in $\mathbb{C}\times\mathbb{C}^*$ together with their derivatives with respect to the operator $\mathcal{D}=\frac{\partial}{\partial X_1}+X_2\frac{\partial}{\partial X_2}$ up to order $3\lfloor D^\tau\rfloor-1$, while in our work, the polynomials P_D have absolute values at most e^{-D^ν} at $3\lfloor D^\tau\rfloor$ translates of (ξ,η). The constraints on the parameters τ,β,ν in [21] are almost the same as (1) (where τ replaces σ and $\beta>\tau$ replaces $\beta>\sigma+1$). In both cases, the conclusion is that $\xi,\eta\in\overline{\mathbb{Q}}$.

To prove our result, we apply elimination theory in the form developed by M. Laurent and D. Roy in [14] in terms of height of a $\mathbb{Q}$-cycle relative to a convex body. More precisely, as in [19], we consider some homogenization of the polynomials P_D and for each $D\geq 1$, we define an appropriate convex body $\mathcal{C}_D$. Then using elimination theory, we obtain a zero-dimensional $\mathbb{Q}$-subvariety Z_D whose height $h_{\mathcal{C}_D}(Z_D)$ relative to $\mathcal{C}_D$ is very small (negative). Up to this, the argument is very similar to [21]. The rest of the proof is different since we deal with several points.

In order to reach the conclusion, we need to analyze the distance from the points of Z_D and the points $\boldsymbol{\gamma}_i = (1, \xi + ir, \eta s^i)$ $(i \in \mathbb{Z})$. This analysis is complicated and involves a new interpolation estimate as well as a diophantine analysis of the ideal of homogeneous polynomials of $\mathbb{C}[X_0, X_1, X_2]$ vanishing on all the points γ_i with $0 \le i < \lfloor D^\sigma \rfloor$. We refer readers to the precise outline of the proof given in Chapter 1. Despite this big difference in the proof of our main result, it is surprising that we reach the same conclusion $\xi, \eta \in \overline{\mathbb{Q}}$ by asking constraints on σ, β, ν which are almost the same as those in [21] for τ, β, ν.

In [17], D. Roy made a statement in the form of a small value estimate and prove that it is equivalent to Schanuel's conjecture, one of the main open problems in transcendental number theory. In this paper, the author considers a certain sequence $(Q_D)_{D\ge 1}$ of polynomials in $\mathbb{Z}[X_1, X_2]$ with partial degree $\le D^{t_1}$ in X_1 and partial degree $\le D^{t_2}$ in X_2 and norm $\le e^D$. He requests that the polynomials Q_D take the absolute values $\le e^{-D^u}$ with their derivatives up to order D^{s_1} at all the points $m_1\Upsilon_1 + \cdots + m_\ell \Upsilon_\ell$ $(0 \le m_i \le D^{s_2})$ where $\Upsilon_i = (\xi_i, \eta_i)$ $(0 \le i \le \ell)$ are fixed points of the algebraic group $\mathbb{C} \times \mathbb{C}^*$ such that $\xi_1, \dots, \xi_\ell$ are linearly independent over $\mathbb{Q}$.

Assuming that

$$\max\{1, t_1, 2t_2\} < \min\{s_1, 2s_2\}, \quad \max\{s_1, s_2 + t_2\} < u < \frac{1}{2}(1 + t_1 + t_2),$$

he shows that

$$\text{tr.deg}_{\mathbb{Q}}(\xi_1, \dots, \xi_\ell, \eta_1, \dots, \eta_\ell) \ge \ell.$$

Our present result implies that if $\text{tr.deg}_{\mathbb{Q}}(\xi, \eta) \ge 1$, then for each $(r, s) \in \mathbb{Q}^{*2}$ with $s \ne \pm 1$, and for each triple (σ, β, ν) satisfying (2), there exist infinitely many integers D for which any non-zero polynomial P of $\mathbb{Z}[X_1, X_2]$ of degree $\le D$ and norm $\le e^{D^\beta}$ satisfies

$$\max_{0 \le < 3\lfloor D^\sigma \rfloor} |P((\xi, \eta) + i(r, s))| > e^{-D^\nu}.$$

This is a modest step in the direction of the Schanuel conjecture, but it improves on previously known results.

Part II.

The second part of the thesis deals with the two most basic problems of Diophantine approximation. One of them consists in finding good rational approximations to a given real point $(\theta_1, \ldots, \theta_n)$. The other consists in finding small linear integral combination of $1, \theta_1, \ldots, \theta_n$. In their precise form both problems request to solve some systems of linear inequations. In the first case, we look for non-zero integral solutions $\mathbf{x} = (x_0, \ldots, x_n)$ to the system

$$|x_0| \leq X, \quad |x_0\theta_1 - x_1| \leq X^{-\lambda}, \ \ldots, \ |x_0\theta_n - x_n| \leq X^{-\lambda} \tag{3}$$

where $\lambda > 0$ is fixed and X goes to infinity. If $\mathbf{x} = (x_0, \ldots, x_n)$ is a solution of the system with X large enough, then $x_0 \neq 0$ and the point $(x_1/x_0, \ldots, x_n/x_0)$ provides a rational approximation to $(\theta_1, \ldots, \theta_n)$. In the second case, we look for non-zero integral solutions $\mathbf{x} = (x_0, \ldots, x_n)$ of the system

$$|x_0 + x_1\theta_1 + \cdots + x_n\theta_n| \leq X^{-\tau}, \quad |x_1| \leq X, \ \ldots, \ |x_n| \leq X \tag{4}$$

where $\tau > 0$ is fixed and X goes to infinity. The two problems are dual of each other and the geometry of numbers provides remarkable connections between them. In this thesis, we are interested in the so-called uniform exponents of approximation attached to each problem. Following a convention introduced by Bugeaud and Laurent in [2], we denote by $\hat{\lambda}(1, \theta_1, \ldots, \theta_n)$ (resp. by $\hat{\tau}(1, \theta_1, \ldots, \theta_n)$) the supremum of all real numbers $\lambda > 0$ (resp. $\tau > 0$) such that the system (3) (resp. (4)) has a non-zero integer solution for each sufficiently large X. An application of Minkowski's first convex body theorem shows that, if $\boldsymbol{\theta} := (1, \theta_1, \ldots, \theta_n)$ has $\mathbb{Q}$-linearly independent coordinates, then $\hat{\lambda}(\boldsymbol{\theta}) \geq 1/n$ and $\hat{\tau}(\boldsymbol{\theta}) \geq n$.

It came as a surprise when it was shown in [18], some ten years ago, that there exist real points $\boldsymbol{\theta}$ with coordinates in a field of transcendence degree 1 for which at least one of these exponents (and in fact both of them) strictly exceed the above lower bounds. In [2] and [22], Bugeaud, Laurent and Roy produced more examples of such points. However, in all cases, these points lay on an algebraic curve in $\mathbb{R}^3$ defined by an irreducible homogeneous polynomial of $\mathbb{Q}[x_0, x_1, x_2]$ of degree 2. For transcendental points on algebraic curves of higher degree (defined over $\mathbb{Q}$), we only have upper bounds on their exponents of approximation. For example, Davenport and Schmidt showed in [6] that $\hat{\lambda}(1,\theta,\theta^2,\theta^3) \leq 1/2$ for any real number θ which is not an algebraic number of degree ≤ 3. This upper bound was improved by Roy to about 0.4245 in [19], but at present an optimal upper bound is not known. More recently Lozier and Roy showed in [15] that $\hat{\lambda}(1,\theta,\theta^3) \leq 2(9+\sqrt{11})/35 \simeq 0.7038$ for any real number θ such that $1,\theta,\theta^3$ are linearly independent over $\mathbb{Q}$.

Let α be a quadratic real number. It is shown in [22] that, for any $\xi \in \mathbb{R} \setminus \mathbb{Q}(\alpha)$, we have $\hat{\lambda}(1,\alpha,\xi) \leq (\sqrt{5}-1)/2 \simeq 0.618$, with equality for a countable set of real numbers ξ. The proof of the upper bound in this case is simpler than the estimate $\hat{\lambda}(1,\xi,\xi^2) \leq (\sqrt{5}-1)/2$ proved by Davenport and Schmidt for non-quadratic irrational real numbers ξ in [6]. This motivated us to establish upper bounds for the uniform exponents of approximation to points of the form

$$\boldsymbol{\theta} := (1,\theta_1,\ldots,\theta_{d-1},\xi)$$

where $\{1,\theta_1,\ldots,\theta_{d-1}\}$ is a basis of a real number field K of degree $d \geq 2$ over $\mathbb{Q}$ and where $\xi \in \mathbb{R} \setminus K$. In a simplified form, our main result in Chapter 2 says that such a point satisfies

$$\hat{\lambda}(\boldsymbol{\theta}) \leq \lambda_d < \frac{1}{d-1} - \frac{1}{d^2(d-1)} \tag{5}$$

where λ_d is the unique positive real root of the polynomial $(d-1)^{d-1}x^d + \cdots + (d-1)x^2 + x - 1$. This improves on the trivial upper bound $\hat{\lambda}(\boldsymbol{\theta}) \leq \hat{\lambda}(1,\theta_1,\ldots,\theta_{d-1}) = 1/(d-1)$. Similarly, our main result in Chapter 3 is that

$$\hat{\tau}(\boldsymbol{\theta}) \leq \tau_d := \frac{1+\sqrt{5}}{2}(d-1)+1. \tag{6}$$

Following the pioneer work of Davenport and Schmidt in [6], the proofs of both results are based on an analysis of the sequences of so-called minimal points attached to $\boldsymbol{\theta}$, in relation to the problem under consideration.

Our main contribution in Chapter 2 is a careful study of the heights of the subspaces spanned by consecutive minimal points. It leads to an inequality relating the norms of properly chosen minimal points. It took us much work to discover and prove this result but with its help, the proof of (5) goes relatively easily.

Our analysis of the sequence of minimal points attached to the other problem is quite different. In Chapter 3, we assume that $\boldsymbol{\theta} = (1, \alpha, \dots, \alpha^{d-1}, \xi)$ where α is a primitive element of the field K. Then we combine several linearly independent minimal points to construct polynomials in α with small non-zero absolute values and then we use Liouville's inequality to bound from below these absolute values. This yields inequalities relating the corresponding minimal points. These estimates and others coming from geometry of numbers lead to the proof of (6).

A more complete outline of each proof is given in the corresponding chapter. In both chapters we also give alternative proofs of some of our results when they are obtained through non-explicit constructions based on Diriclet's box principle or on geometry of numbers. These alternative arguments are based on the construction of explicit auxiliary polynomials adapted to our problem. In Chapter 2, we also present the construction of a point $(1, \sqrt[3]{2}, \sqrt[3]{4}, \xi)$ with surprising Diophantine properties.

Contents

Chapter 1

A new small value estimate for the group $\mathbb{C} \times \mathbb{C}^*$

1.1 Introduction and results

The theory of transcendental numbers started with Liouville's memoir of 1844. There, he investigated a class of numbers x, now called Liouville numbers, for which there exists a rational number p/q such that $|x - p/q| \leq 1/q^n$ for any positive integer n, and showed that these are transcendental.

In 1873, Hermite showed that e is transcendental. This is the first number proven transcendental but not constructed to be transcendental.

In 1882, Lindemann proved that e to any non-zero algebraic number power is transcendental. As a consequence, π is transcendental. This yields the negative answer for the squaring circle problem, proposed by ancient Greek geometers.

Generalizing the method of Lindemann, Weierstrass established a result, named for both of them.

Theorem 1.1.1. *(Lindemann-Weierstrass) If $\alpha_1, \ldots, \alpha_n$ are algebraic numbers which are linearly independent over $\mathbb{Q}$ then $e^{\alpha_1}, \ldots, e^{\alpha_n}$ are algebraically independent over $\mathbb{Q}$.*

In 1934, Gel'fond and Schneider proved independently that if α and β are algebraic numbers with $\alpha \neq 0$ and $\beta \notin \mathbb{Q}$, then for any choice of $\log \alpha \neq 0$, the number $\alpha^\beta = e^{\beta \log \alpha}$ is transcendental.

A basis tool in transcendental number theory consists of the construction of auxiliary functions taking small values at many points of an algebraic group. If these values are integers < 1, then they all vanish and we can apply a zero estimate to conclude. If these values are algebraic, we can instead apply Liouville's inequality and hopefully conclude that these values are zero, such as in the proof of Gel'fond-Schneider Theorem. When the field generated by these values has transcendence degree 1 over $\mathbb{Q}$, a substitute for Liouville's inequality is given by Gel'fond's criterion in [10]. When the transcendence degree of this field is higher, one can use Philippon's criterion (Theorem 2.11 of [16]). We recall these criterions below.

Gel'fond criterion. *Let $\xi \in \mathbb{C}$. Assume that there exist real numbers*

$$\beta > 1, \;\; \nu > \beta + 1$$

and a sequence of non-zero polynomials $(P_D)_{D\geq 1} \subset \mathbb{Z}[X]$ such that

$$\deg P_D \leq D, \quad \|P_D\| \leq e^{D^\beta}, \quad |P_D(\xi)| \leq e^{-D^\nu}$$

where $\|P_D\|$ denotes the norm of polynomial P_D, i.e. the largest absolute value of its coefficients. Then $P_D(\xi) = 0$ for all sufficiently large integers $D \geq 1$. In particular, $\xi \in \overline{\mathbb{Q}}$.

Philippon's criterion. *Let $\boldsymbol{\theta} = (1, \theta_1, \ldots, \theta_m) \in \mathbb{C}^{m+1}$, let θ denote the corresponding point of $\mathbb{P}_m(\mathbb{C})$, and let k be an integer with $0 \leq k \leq m$. Moreover, let $(D_n)_{n\geq 1}$ be a non-decreasing sequence of positive integers, and let $(T_n)_{n\geq 1}$ and $(V_n)_{n\geq 1}$ be non-decreasing sequences of positive real numbers such that*

$$\limsup_{n\to\infty} \frac{V_n}{(D_n + T_n)D_n^k} = \infty.$$

Suppose also that for each $n \geq 2$ there exists a non-empty family $\mathcal{F}_n$ consisting of homogeneous polynomials in $\mathbb{Z}[X_0, X_1, \ldots, X_m]$ which satisfy the following two properties.

(i) For each $P \in \mathcal{F}_n$, *we have*

$$\deg(P) = D_n, \quad h(P) \le T_n \text{ and } |P(\boldsymbol{\theta})| \le e^{-V_n} \|P\| \, \|\boldsymbol{\theta}\|^{D_n}.$$

(ii) The polynomials of $\mathcal{F}_n$ *have no common zero* α *in* $\mathbb{P}^m(\mathbb{C})$ *with*

$$\operatorname{dist}(\boldsymbol{\theta}, \alpha) \le e^{-V_{n-1}}.$$

Then we have $k < m$ *and the transcendence degree over* $\mathbb{Q}$ *of the field* $\mathbb{Q}(\theta_1, \ldots, \theta_m)$ *is* $\ge k + 1$.

Using his criterion, Gel'fond proved in [9] the following result.

Theorem 1.1.2. *If* α *and* β *are algebraic numbers with* $\alpha \neq 0$ *and* $[\mathbb{Q}(\beta) : \mathbb{Q}] = 3$, *then for any choice of* $\log \alpha \neq 0$, *the numbers* $e^{\beta \log \alpha}$ *and* $e^{\beta^2 \log \alpha}$ *are algebraically independent over* $\mathbb{Q}$.

Applying Philippon's criterion, G. Diaz established the following result in [8].

Theorem 1.1.3. *Let* α *and* β *be algebraic numbers with* $\alpha \neq 0$ *and* $[\mathbb{Q}(\beta) : \mathbb{Q}] = d$. *Then, for any choice of* $\log \alpha \neq 0$, *we have*

$$\operatorname{tr.deg}_{\mathbb{Q}} \mathbb{Q}(e^{\beta \log \alpha}, \ldots, e^{\beta^{d-1} \log \alpha}) \ge \left\lfloor \frac{d+1}{2} \right\rfloor.$$

For future progress in Transcendence and Algebraic Independence, it is desirable to study situations where the values are not small enough so that we can apply Philippon's criterion.

D. Roy presented in [21] such a situation and showed an improvement on a direct application of Philippon's criterion. More precisely, he established the following result.

Theorem 1.1.4. *Let* $(\xi, \eta) \in \mathbb{C} \times \mathbb{C}^*$ *and let* $\tau, \beta, \nu \in \mathbb{R}$ *with*

$$1 \le \tau < 2, \qquad \beta > \tau, \qquad \nu > \max\left\{ \beta + 2 - \tau + \frac{(\tau - 1)(2 - \tau)}{\beta - \tau + 1}, \ \tau + 2 \right\}.$$

Suppose that, for each sufficiently large positive integer D, there exists a non-zero polynomial $P_D \in \mathbb{Z}[X_1, X_2]$ of degree $\leq D$ and norm $\leq \exp(D^\beta)$ such that

$$\max_{0 \leq i < 3\lfloor D^\tau \rfloor} |\mathcal{D}^i P_D(\xi, \eta)| \leq e^{-D^\nu} \qquad \textit{where } \mathcal{D} = \frac{\partial}{\partial X_1} + X_2 \frac{\partial}{\partial X_2}.$$

Then, we have $\xi, \eta \in \overline{\mathbb{Q}}$ and moreover $\mathcal{D}^i P_D(\xi, \eta) = 0$ $(0 \leq i < 3\lfloor D^\tau \rfloor)$ for each sufficiently large integer D.

In this chapter, we adapt the approach of D. Roy in [21] to establish the following result.

Theorem 1.1.5. *Let $(\xi, \eta) \in \mathbb{C} \times \mathbb{C}^*$ and $(r, s) \in \mathbb{Q}^{*2}$ with $s \neq \pm 1$. Let $\sigma, \beta, \nu \in \mathbb{R}$ such that*

$$1 \leq \sigma < 2, \quad \beta > \sigma + 1, \quad \nu > \max\left\{\beta + 2 - \sigma + \frac{(\sigma - 1)(2 - \sigma)}{\beta - \sigma + 1},\ \sigma + 2\right\}.$$

Suppose that, for each sufficiently large positive integer D, there exists a non-zero polynomial $P_D \in \mathbb{Z}[X_1, X_2]$ such that

$$\deg P_D \leq D, \quad \|P_D\| \leq e^{D^\beta}, \quad \max_{0 \leq i < 3\lfloor D^\sigma \rfloor} |P_D(\xi + ir, \eta s^i)| \leq e^{-D^\nu}. \tag{1.7}$$

Then we have $\xi, \eta \in \overline{\mathbb{Q}}$.

For any $(\xi, \eta), (r, s) \in \mathbb{C}^2$, Dirichlet's Box principle ensures the existence of a sequence of polynomials satisfying (3.3) when the condition

$$\nu > \max\{\beta + 2 - \sigma + \frac{(\sigma - 1)(2 - \sigma)}{\beta - \sigma + 1}, \sigma + 2\}$$

is replaced by $\nu < \beta + 2 - \sigma$. So we are not able to conclude anything in this case. More precisely, we have the following result.

Proposition 1.1.6. *Let $(\xi, \eta), (r, s) \in \mathbb{C}^2$. Let $\sigma, \beta, \nu \in \mathbb{R}$ such that*

$$0 \leq \sigma < 2, \quad \beta > \sigma + 1, \quad \nu < \beta + 2 - \sigma.$$

Then, for each $D \gg 1$, there exists $0 \neq P_D \in \mathbb{Z}[X_1, X_2]$ such that

$$\deg P_D \leq D, \quad \|P_D\| \leq e^{D^\beta}, \quad \max_{0 \leq j < 3\lfloor D^\sigma \rfloor} |P_D(\xi + jr, \eta s^j)| \leq e^{-D^\nu}.$$

Proof. Fix a large integer D. Put $S = 3\lfloor D^\sigma \rfloor$. Let U_D be the set of polynomials in $\mathbb{Z}[X_1, X_2]_{\le D}$ with non-negative integer coefficients and norm $\le e^{D^\beta}$. Consider the map

$$\begin{aligned} \bar{f} : U_D &\longrightarrow \mathbb{R}^S \\ P &\longmapsto (P(\xi + jr, \eta s^j))_{0 \le j < S} \end{aligned}$$

We have

$$\mathrm{Card}\, U_D \ge \exp\left(D^\beta \binom{D+2}{2} \right) \ge \exp\left(\frac{1}{2} D^{\beta+2} \right).$$

Moreover, for each $0 \le j < S$, we have

$$|P(\xi + jr, \eta s^j)| \le \binom{D+2}{2} e^{D^\beta} \max\{1, |\xi + jr|, |\eta s^j|\}^D \le e^{4D^\beta}$$

since $\beta > \sigma + 1$. So $(P(\xi + jr, \eta s^j))_{0 \le j < S}$ belongs to S-cube $\left[-e^{4D^\beta}, e^{4D^\beta}\right]^S$.

On the other hand, the interval $\left[-e^{4D^\beta}, e^{4D^\beta}\right]$ can be covered by a union of at most $1 + 2e^{4D^\beta + D^\nu}$ subintervals of length e^{-D^ν}. Hence the S-cube $\left[-e^{4D^\beta}, e^{4D^\beta}\right]^S$ is covered by at most $(3e^{4D^\beta + D^\nu})^S \le \exp(16 D^{\max\{\beta, \nu\} + \sigma})$ smaller S-cubes of edges of length e^{-D^ν}. Since $\sigma < 2$, and $\nu < \beta + 2 - \sigma$, we find that U_D has a cardinal greater than the number of such small S-cubes.

By Dirichlet's Box Principle, there exist two distinct polynomials Q_D, Q'_D in U_D mapping to the same small S-cube. This means that

$$|(Q_D - Q'_D)(\xi + jr, \eta s^j)| \le e^{-D^\nu}$$

for all $0 \le j < S$. Since Q_D and $Q_{D'}$ have coefficients in $[0, e^{D^\beta}]$, the polynomial $P_D = Q_D - Q'_D$ is non-zero and has norm $\|P_D\| \le e^{D^\beta}$. Thus it satisfies the required properties. □

The above Proposition implies that, we cannot reduce the lower bound on ν in Theorem 1.1.5 by more than

$$\frac{(\sigma - 1)(2 - \sigma)}{\beta - \sigma + 1} < \frac{(\sigma - 1)(2 - \sigma)}{2} \le \frac{1}{8}.$$

Now we will explain why we need $\sigma \ge 1$. This follows from a result of Khintchine revisited by Philippon in [16, Appendix].

Theorem 1.1.7. *(Khintchine - Philippon) Let $\psi : \mathbb{N} \longrightarrow (0,1)$ be a decreasing function. Then there exists $(\xi, \eta) \in \mathbb{R} \times \mathbb{R}^*$ with the following properties*

- *ξ and η are algebraically independent over $\mathbb{Q}$,*
- *for each $D \geq 1$, there exists a non-zero linear form $L_D \in \mathbb{Z}[X_1, X_2]$ such that*

$$\|L_D\| \leq D, \quad |L_D(\xi, \eta)| \leq \psi(D).$$

Corollary 1.1.8. *Let $(r, s) \in \mathbb{Q} \times \mathbb{Q}^*$. Let $\sigma, \beta, \nu \in \mathbb{R}$ such that*

$$0 \leq \sigma < 1, \qquad \beta > 2\sigma, \quad \nu > 0.$$

Then there exists $(\xi, \eta) \in \mathbb{R} \times \mathbb{R}^*$ with the following properties

- *ξ, η are algebraically independent over $\mathbb{Q}$,*
- *for each $D \gg 1$, there exists a non-zero polynomial $P_D \in \mathbb{Z}[X_1, X_2]_{\leq D}$ such that*

$$\deg P_D \leq D, \quad \|P_D\| \leq e^{D^\beta}, \quad \max_{0 \leq j < 3\lfloor D^\sigma \rfloor} |P_D(\xi + jr, \eta s^j)| \leq e^{-D^\nu}.$$

Proof. From theorem 1.1.7, we deduce the existence of $(\xi, \eta) \in \mathbb{R} \times \mathbb{R}^*$ with the following properties

- ξ and η are algebraically independent over $\mathbb{Q}$,
- for each $D \geq 1$, there exists a non-zero linear form $L_D \in \mathbb{Z}[X_1, X_2]$ such that

$$\|L_D\| \leq D, \quad |L_D(\xi, \eta)| \leq \exp(-D^\nu - D^\beta).$$

Set

$$P_D(X_1, X_2) = \prod_{0 \leq j < 3\lfloor D^\sigma \rfloor} d^j L_D(X_1 - jr, s^{-j} X_2)$$

where d is a positive integer such that $ds^{-1}, dr \in \mathbb{Z}$. Assuming D large enough, we have

$$\deg P_D = 3\lfloor D^\sigma \rfloor \leq D \ \text{ since } \sigma < 1.$$

Moreover, we get

$$\begin{aligned}
\|P_D\| &\leq 3^{3D^\sigma} \max_{0\leq j<3\lfloor D^\sigma\rfloor} \|d^j L_D(X_1 - jr, s^{-j}X_2)\|^{3D^\sigma} \\
&\leq 3^{3D^\sigma} \left(d^{3D^\sigma}\|L_D\|(1+3D^\sigma|r|+|s^{-1}|^{3D^\sigma})\right)^{3D^\sigma} \\
&\leq \left(3\, d^{3D^\sigma} D(1+|r|+|s^{-1}|)^{3D^\sigma}\right)^{3D^\sigma} \\
&\ll e^{D^\beta} \qquad \text{(since } \beta > 2\sigma\text{)},
\end{aligned}$$

and

$$\begin{aligned}
|P_D(\xi + jr, \eta s^j)| &= d^{9D^{2\sigma}} |L_D(\xi,\eta)| \prod_{\substack{j'\neq j \\ 0\leq j'<3\lfloor D^\sigma\rfloor}} |L_D(\xi+(j'-j)r, \eta s^{j'-j})| \\
&\leq d^{9D^{2\sigma}} e^{-D^\nu - D^\beta} \left(\|L_D\| \left(1+|\xi|+3D^\sigma|r|+|\eta|(|s|+|s^{-1}|)^{3D^\sigma}\right)\right)^{3D^\sigma} \\
&\leq e^{-D^\nu - D^\beta} d^{9D^{2\sigma}} \left(D\left(1+|\xi|+|r|+(|\eta|+1)(|s|+|s^{-1}|)\right)^{3D^\sigma}\right)^{3D^\sigma} \\
&\ll e^{-D^\nu} \qquad \text{(since } \beta > 2\sigma\text{)}. \qquad \square
\end{aligned}$$

This result shows that Theorem 1.1.5 does not hold if we replace the condition $1 \leq \sigma < 2$ by $0 \leq \sigma < 1$. Indeed, for such σ, the pair (ξ, η) constructed by Corollary 1.1.8 satisfies all the hypotheses of the theorem (for any choice of $\beta > \sigma + 1$ and $\nu > 0$) but it does not satisfy the conclusion.

1.2 Preliminaries

In this section, we introduce the results of dimension theory and elimination theory that we will need in the proof of our main result (Theorem 1.1.5).

Let m be a positive integer. We denote by $\mathbb{C}[\mathbf{X}]$ the ring of polynomials in variables $X_0, \ldots, X_m$ with coefficients in $\mathbb{C}$. For each integer $D \geq 0$, we denote by $\mathbb{C}[\mathbf{X}]_D$ its homogeneous part of degree D.

1.2.1 Dimension and degree of algebraic subsets of $\mathbb{P}^m(\mathbb{C})$

Let S be a subset of $\mathbb{C}[\mathbf{X}]$ consisting of homogeneous polynomials. We denote by $\mathcal{Z}(S)$ the set of common zeros in $\mathbb{P}^m(\mathbb{C})$ of the polynomials of S. Then $\mathcal{Z}(S) = \mathcal{Z}(I)$ where I is the homogeneous ideal generated by S.

Given a subset Z of $\mathbb{P}^m(\mathbb{C})$, we say that Z is an *algebraic subset* of $\mathbb{P}^m(\mathbb{C})$ if $Z = \mathcal{Z}(I)$ for some homogeneous ideal I of $\mathbb{C}[\mathbf{X}]$. If the corresponding ideal is prime, we say that Z is an *irreducible algebraic subset* of $\mathbb{P}^m(\mathbb{C})$.

By a $\mathbb{Q}$-*subvariety of* $\mathbb{P}^m(\mathbb{C})$, we mean the zero set in $\mathbb{P}^m(\mathbb{C})$ of a homogeneous prime ideal of $\mathbb{Q}[X_0, X_1, \dots, X_m]$ distinct from the ideal $\langle X_0, \dots, X_m\rangle$. Such a set is non-empty but may not be irreducible as an algebraic subset of $\mathbb{P}^m(\mathbb{C})$.

Let Z be an algebraic subset of $\mathbb{P}^m(\mathbb{C})$. We say that Z has dimension t and write $\dim(Z) = t$ if there exists a chain of irreducible algebraic subsets

$$\emptyset = Z_0 \subsetneq \cdots \subsetneq Z_{t+1} \subseteq Z,$$

but no longer chain.

Example 1.2.1. (i) $\dim(\mathbb{P}^m(\mathbb{C})) = m$.

(ii) $\dim(\emptyset) = -1$.

(iii) $\dim(\mathcal{Z}(P)) = m - 1$ if P is a non-zero homogeneous polynomial of $\mathbb{C}[\mathbf{X}]$.

Fix an algebraic subset Z of $\mathbb{P}^m(\mathbb{C})$ of dimension d. Denote by $\mathcal{I}(Z)$ the ideal generated by all homogeneous polynomials of $\mathbb{C}[\mathbf{X}]$ vanishing on Z. Then $\mathbb{C}[\mathbf{X}]/\mathcal{I}(Z)$ is a graded $\mathbb{C}[\mathbf{X}]$-module whose homogeneous part of degree t is denoted by $(\mathbb{C}[\mathbf{X}]/\mathcal{I}(Z))_t$. It is well-known that there exists a polynomial $H_Z(t) \in \mathbb{Q}[t]$, called the *Hilbert polynomial of* Z, such that

$$H_Z(t) = \dim_{\mathbb{C}}(\mathbb{C}[\mathbf{X}]/\mathcal{I}(Z))_t$$

for each sufficiently large integer t. More precisely, $H_Z(t)$ is a polynomial of degree d of the form

$$H_Z(t) = a_0\binom{t}{d} + a_1\binom{t}{d-1} + \cdots + a_d\binom{t}{0}$$

where $a_0, a_1, \ldots, a_d$ are integers.

If $Z \neq \emptyset$, we have $d \geq 0$, and we define the *degree* of Z to be $\deg(Z) = a_0$. This is a positive integer.

Example 1.2.2. We have

$$H_{\mathbb{P}^m(\mathbb{C})}(t) = \dim_{\mathbb{C}}(\mathbb{C}[X_0, \ldots, X_m]_t) = \binom{t+m}{m},$$

and so $\deg(\mathbb{P}^m(\mathbb{C})) = 1$.

To establish our result, we will work with $\mathbb{Q}$-subvarieties of $\mathbb{P}^m(\mathbb{C})$ of dimension 0. Note that, if Z is a $\mathbb{Q}$-subvariety of $\mathbb{P}^m(\mathbb{C})$ of dimension 0, then Z is finite, more precisely, $\deg(Z) = |Z|$ and if $(\alpha_0, \alpha_1, \ldots, \alpha_m)$ is a representative in $\mathbb{C}^{m+1}$ of a point of Z with at least one coordinate equal to 1, then Z consists of the points $(\sigma(\alpha_0) : \sigma(\alpha_1) : \ldots : \sigma(\alpha_m)) \in \mathbb{P}^m(\mathbb{C})$ where σ runs through all embeddings of $\mathbb{Q}(\alpha_0, \ldots, \alpha_m)$ into $\mathbb{C}$.

1.2.2 Basic results in Elimination Theory

In our work, we will use consequences of the following result, which derives from [5, Lemma 3].

Theorem 1.2.3. *Assume that Z is an algebraic subset of $\mathbb{P}^m(\mathbb{C})$ of dimension $d \geq 1$. Let P be a non-constant homogeneous polynomial of $\mathbb{C}[\mathbf{X}]$ such that $\mathcal{Z}(P)$ does not contain any irreducible component of Z (over $\mathbb{C}$). Then the intersection $Z \cap \mathcal{Z}(P)$ has dimension $d-1$ and degree at most $\deg(Z) \cdot \deg(P)$.*

Moreover, if Z is d-equidimensional, i.e., if every component of its decomposition into irreducible algebraic subsets of $\mathbb{P}^m(\mathbb{C})$ has dimension d, then $Z \cap \mathcal{Z}(P)$ is $(d-1)$-equidimensional.

In fact, Lemma 3 of [5] shows that $\deg(Z \cap \mathcal{Z}(P)) = \deg(Z)\deg(P)$ if P has no multiple factor so that the ideal $\langle P \rangle$ is reduced.

If $Z = \mathbb{P}^m(\mathbb{C})$ then we have $\deg(\mathbb{P}^m(\mathbb{C})) = 1$ and so, by the theorem, we get the following result.

Corollary 1.2.4. *Let P be a non-constant homogeneous polynomial of $\mathbb{C}[\mathbf{X}]$. Then $\deg(\mathcal{Z}(P)) \leq \deg(P)$.*

If $Z = \mathcal{Z}(Q)$ where Q is a non-constant homogeneous polynomial of $\mathbb{C}[\mathbf{X}]$, then $\mathcal{Z}(Q)$ is $(m-1)$-equidimensional. In particular, if P and Q belong to $\mathbb{Q}[\mathbf{X}]$ and have no common factor in $\mathbb{Q}[\mathbf{X}]$, then they also have no common factor in $\mathbb{C}[\mathbf{X}]$. Therefore, we obtain the following result.

Corollary 1.2.5. *Assume that P and Q are non-zero homogeneous polynomials of $\mathbb{C}[\mathbf{X}]$ (resp. $\mathbb{Q}[\mathbf{X}]$) which have no common factor in $\mathbb{C}[\mathbf{X}]$ (resp. $\mathbb{Q}[\mathbf{X}]$). Then $\mathcal{Z}(P,Q)$ is $(m-2)$-equidimensional and has degree $\deg(\mathcal{Z}(P,Q)) \leq \deg(P)\deg(Q)$.*

We now introduce the main tool used in our work, the Chow form of $\mathbb{Q}$-subvarieties Z of $\mathbb{P}^m(\mathbb{C})$. We start with the definition of resultant, which is the Chow form of $\mathbb{P}^m(\mathbb{C})$ as we will see below.

Let $D \in \mathbb{N}^*$. For each $\boldsymbol{\nu} = (\nu_0, \dots, \nu_m) \in \mathbb{N}^{m+1}$, we define $\mathbf{X}^{\boldsymbol{\nu}} = X_0^{\nu_0} \cdots X_m^{\nu_m}$. Let

$$U_i = \sum_{\substack{\boldsymbol{\nu} \in \mathbb{N}^{m+1} \\ |\boldsymbol{\nu}| = D}} u_{i,\boldsymbol{\nu}} \mathbf{X}^{\boldsymbol{\nu}}, \qquad i = 0, \dots, m$$

be $m+1$ generic homogeneous forms in $X_0, \dots, X_m$ of degree D, *i.e.* homogeneous forms in $\mathbf{X}$ with indeterminate coefficients.

As is well-known, there is a polynomial in $u_{i,\boldsymbol{\nu}}$ with integer coefficients, called the *resultant*, denoted $\mathrm{Res}_D(U_0, \dots, U_m)$, such that

- $\mathrm{Res}_D(U_0, \dots, U_m)$ is irreducible over $\mathbb{C}$,
- $\mathrm{Res}_D(U_0, \dots, U_m)$ is homogeneous of degree D^m in $(u_{i,\boldsymbol{\nu}})_{|\boldsymbol{\nu}|=D}$ for each index $i = 0, \dots, m$ and it has total degree $(m+1)D^m$,
- viewing the resultant as a polynomial map $\mathrm{Res}_D : \mathbb{C}[\mathbf{X}]_D^{m+1} \longrightarrow \mathbb{C}$, we have

$$\mathrm{Res}_D(P_0, P_1, \dots, P_m) = 0 \ \text{ iff } \ \mathcal{Z}(P_0, \dots, P_m) \neq \emptyset$$

for any tuple $(P_0, P_1, \dots, P_m) \in \mathbb{C}[\mathbf{X}]_D^{m+1}$.

(See [23, Chapter XI] for more details.)

We now define the Chow form of $\mathbb{Q}$-subvarieties of $\mathbb{P}^m(\mathbb{C})$. Assume that Z is a $\mathbb{Q}$-subvariety of $\mathbb{P}^m(\mathbb{C})$ of dimension t. The first section of [16] shows the existence of a polynomial $F(U_0, \ldots, U_t) \in \mathbb{Z}[u_{i,\boldsymbol{\nu}}; 0 \le i \le t, |\boldsymbol{\nu}| = D]$ with the following properties

- $F(U_0, \ldots, U_t)$ is irreducible over $\mathbb{Z}$,
- F is homogeneous of degree $D^t \deg(Z)$ in $(u_{i,\boldsymbol{\nu}})_{|\boldsymbol{\nu}|=D}$ for each $i = 0, \ldots, t$ and it has total degree $(t+1)D^t \deg(Z)$,
- viewing $F(U_0, \ldots, U_t)$ as a polynomial map $F : \mathbb{C}[\mathbf{X}]_D^{t+1} \longrightarrow \mathbb{C}$, we have

$$\mathcal{Z}(F) = \{(P_0, \ldots, P_t) \in \mathbb{C}[\mathbf{X}]_D^{t+1};\ \ \mathcal{Z}(P_0, \ldots, P_t) \cap Z \neq \emptyset\}.$$

For given Z and D, such a polynomial is unique up to multiplication by ± 1. We call it the *Chow form of Z in degree D.*

We define the (logarithmic) *height* $h(Z)$ of Z as the logarithm of norm of its Chow form in degree 1.

By the definition, when $Z = \mathbb{P}^m(\mathbb{C})$, the corresponding Chow form is simply the resultant in the same degree. For $D = 1$, this is $\pm\det\left((u_{i,\boldsymbol{\nu}})_{\substack{0\le i\le m\\ |\boldsymbol{\nu}|=D}}\right)$ which has non-zero coefficients ± 1. Thus we have $h(\mathbb{P}^m(\mathbb{C})) = 0$.

In the case where Z is a $\mathbb{Q}$-subvariety of $\mathbb{P}^m(\mathbb{C})$ of dimension 0, the corresponding Chow form F in degree 1 is a homogeneous polynomial of degree $\deg(Z)$ in $m+1$ variables. Viewing it as a polynomial map $F : \mathbb{C}[\mathbf{X}]_1 \longrightarrow \mathbb{C}$, we have

$$\mathcal{Z}(F) = \{L \in \mathbb{C}[\mathbf{X}]_1;\ \mathcal{Z}(L) \cap Z \neq \emptyset\}.$$

Note that, for any point of such Z with representative $\boldsymbol{\alpha} = (\alpha_0, \alpha_1, \ldots, \alpha_m)$ in $\mathbb{P}^m(\mathbb{C})$ with at least one coordinate equal to 1, Z consists of the $\deg(Z)$ points

$$(\sigma(\alpha_0) : \sigma(\alpha_1) : \ldots : \sigma(\alpha_m)) \in \mathbb{P}^m(\mathbb{C})$$

where σ runs through all embeddings of $\mathbb{Q}(\alpha_0, \ldots, \alpha_m)$ into $\mathbb{C}$. Therefore, writing F

as a polynomial in $X_0, \ldots, X_m$, F has the form

$$a \prod_{i=1}^{d} \big(\sigma_i(\alpha_0)X_0 + \sigma_i(\alpha_1)X_1 + \cdots + \sigma_i(\alpha_m)X_m\big), \quad a \in \mathbb{Z}.$$

Let $\mathcal{C}$ be a compact subset of $\mathbb{C}[\mathbf{X}]_D$ with non-empty interior. We call it a *convex body of* $\mathbb{C}[\mathbf{X}]_D$ if we have $aP + bQ \in \mathcal{C}$ for any $P,\ Q \in \mathcal{C}$ and for any $a,\ b \in \mathbb{C}$ with $0 \leq |a| + |b| \leq 1$. Then all the polynomials of $\mathbb{C}[\mathbf{X}]_D$ of norm ≤ 1 form a convex body of $\mathbb{C}[\mathbf{X}]_D$. We call it the *unit convex body of* $\mathbb{C}[\mathbf{X}]_D$.

For a $\mathbb{Q}$-subvariety Z of $\mathbb{P}^m(\mathbb{C})$ of dimension t and its corresponding Chow form F in degree D, we define the *height of Z relative to convex body $\mathcal{C}$* of $\mathbb{C}[\mathbf{X}]_D$ to be

$$h_{\mathcal{C}}(Z) = h_{\mathcal{C}}(F) = \log \|F\|_{\mathcal{C}}$$

where $\|F\|_{\mathcal{C}} = \sup\{|F(P_0, \ldots, P_t)|; P_0, \ldots, P_t \in \mathcal{C}\}$. We also use the same notation $\|F\|_{\mathcal{C}}$ not only for the Chow form but also for any polynomial map $F : \mathbb{C}[\mathbf{X}]_D^{t'} \longrightarrow \mathbb{C}$ with $t' \geq 1$.

Given $t \in \{0, \ldots, m\}$, we define a $\mathbb{Q}$-*cycle of dimension t in* $\mathbb{P}^m(\mathbb{C})$ to be a formal linear combination of distinct $\mathbb{Q}$-subvarieties $Z_1, \ldots, Z_s$ of $\mathbb{P}^m(\mathbb{C})$ of dimension t

$$Z = m_1 Z_1 + \cdots + m_s Z_s$$

for some positive integers $m_1, \ldots, m_s$. Such $\mathbb{Q}$-subvarieties $Z_1, \ldots, Z_s$ are called *the irreducible components of Z*.

We extend to cycles the notions of degree, height and height relative to a convex body by writing

$$\deg(Z) = \sum_{i=1}^{s} m_i \deg(Z_i), \qquad h(Z) = \sum_{i=1}^{s} m_i h(Z_i)$$

and

$$h_{\mathcal{C}}(Z) = \sum_{i=1}^{s} m_i h_{\mathcal{C}}(Z_i)$$

where $\mathcal{C}$ stands for an arbitrary convex body of $\mathbb{C}[\mathbf{X}]_D$ for some $D \in \mathbb{N}^*$.

By the definition, we get the following result.

Corollary 1.2.6. *Let Z be a $\mathbb{Q}$-cycle of $\mathbb{P}^m(\mathbb{C})$ and $\mathcal{C}$ be a convex body of $\mathbb{C}[\mathbf{X}]_D$. Assume that*

$$h_{\mathcal{C}}(Z) \leq ah(Z) + b\deg(Z)$$

for some $a, b \in \mathbb{R}$. Then there exists an irreducible component Z' of Z such that

$$h_{\mathcal{C}}(Z') \leq ah(Z') + b\deg(Z').$$

In the proof of our main result, we construct a certain $\mathbb{Q}$-subvariety of dimension 0, obtained as an irreducible component of a certain $\mathbb{Q}$-cycle of $\mathbb{P}^2(\mathbb{C})$ of dimension 0. To derive estimates relative to such a $\mathbb{Q}$-subvariety, we use the following lemmas, taken from the paper [21] of D. Roy (see also [5]).

The first lemma compares the height of a $\mathbb{Q}$-cycle Z with its height relative to the unit convex body of $\mathbb{C}[\mathbf{X}]_D$.

Lemma 1.2.7. *[19, Lemma 2.1] Let D be a positive integer and let $\mathcal{B}$ be the unit convex body of $\mathbb{C}[\mathbf{X}]_D$. Then, for any integer $t \in \{0, 1, \ldots, m\}$ and any $\mathbb{Q}$-cycle Z of $\mathbb{P}^m(\mathbb{C})$ of dimension t, we have*

$$|h_{\mathcal{B}}(Z) - D^{t+1}h(Z)| \leq (t+4)(t+1)\log(m+1)D^{t+1}\deg(Z).$$

In particular, we have $h_{\mathcal{B}}(\mathbb{P}^m) \leq (m+4)(m+1)\log(m+1)D^{m+1}$.

The second lemma provides estimates for the intersection of such a $\mathbb{Q}$-cycle with a certain type of hypersurface.

Lemma 1.2.8. *[19, Proposition 2.2] Let D be a positive integer, let $\mathcal{C}$ be a convex body of $\mathbb{C}[\mathbf{X}]_D$, and let Z be a $\mathbb{Q}$-subvariety of $\mathbb{P}^m(\mathbb{C})$ of dimension $t > 0$. Suppose that there exists a polynomial $P \in \mathbb{Z}[\mathbf{X}]_D \cap \mathcal{C}$ such that $\mathcal{Z}(P)$ does not contain Z. Then there exists a $\mathbb{Q}$-cycle Z' of $\mathbb{P}^m(\mathbb{C})$ of dimension $t-1$ which satisfies:*

(i) $\deg(Z') = D\deg(Z)$;

(ii) $h(Z') \leq Dh(Z) + \deg(Z)\log\|P\| + 2(t+5)(t+1)\log(m+1)D\deg(Z)$;

(iii) $h_{\mathcal{C}}(Z') \leq h_{\mathcal{C}}(Z) + 2t\log(m+1)D^{t+1}\deg(Z)$.

The third lemma deals with the case where the $\mathbb{Q}$-cycle Z has dimension 0.

Lemma 1.2.9. *[19, Proposition 2.3] Let D be a positive integer, let $\mathcal{C}$ be a convex body of $\mathbb{C}[\mathbf{X}]_D$, and let Z be a $\mathbb{Q}$-subvariety of $\mathbb{P}^m(\mathbb{C})$ of dimension 0, and let $\underline{Z}$ be a set of representatives of the points of Z by elements of $\mathbb{C}^{m+1}$ of norm 1. Then, we have*

$$\left| h_{\mathcal{C}}(Z) - Dh(Z) - \sum_{\boldsymbol{\alpha}\in\underline{Z}} \log\sup\{|P(\boldsymbol{\alpha})|; P\in\mathcal{C}\} \right| \leq 9\log(m+1)D\deg(Z).$$

Moreover, if there exists a polynomial $P\in\mathbb{Z}[\mathbf{X}]_D\cap\mathcal{C}$ which does not belong to $\mathcal{I}(Z)$, then we have $h_{\mathcal{C}}(Z)\geq 0$ and

$$0 \leq 7\log(m+1)D\deg(Z) + Dh(Z) + \sum_{\boldsymbol{\alpha}\in\underline{Z}} \log|P(\boldsymbol{\alpha})|.$$

We will also need the following result, which is a special case of Proposition 3.7 in [14].

Lemma 1.2.10. *Let $D,\ s\in\mathbb{N}^*$. Assume that $F_1,\dots,F_s$ are non-zero multi-homogeneous polynomial maps from $\mathbb{C}[\mathbf{X}]_D^{m+1}$ to $\mathbb{C}$ and that $F = F_1\cdots F_s$ has multi-degree $(d_0,\dots,d_m)$. Let $\mathcal{C}$ be a convex body of $\mathbb{C}[\mathbf{X}]_D$. Then we have*

$$\|F\|_{\mathcal{C}} \leq \prod_{i=1}^{s}\|F_i\|_{\mathcal{C}} \leq \binom{D+2}{2}^{2(d_0+\cdots+d_m)}\|F\|_{\mathcal{C}}.$$

1.3 Notation

In this chapter, the letters i,j,k always denote non-negative integers.

We fix $(\xi,\eta)\in\mathbb{C}\times\mathbb{C}^*$ and $(r,s)\in\mathbb{Q}^{*2}$ with $s\neq\pm1$.

For each i, set $\gamma_i = (1:\xi+ir:\eta s^i)\in\mathbb{P}^2(\mathbb{C})$, then $\boldsymbol{\gamma}_i = (1,\xi+ir,\eta s^i)$ is a representative of γ_i in $\mathbb{C}^3$. For each integer T, we put

$$\mathcal{S}_T = \{\gamma_i\ ;\ 0\leq i<T\}$$

and

$$C_T = \begin{cases} \|\gamma_0\| + |r|T & \text{if } |s|<1,\\ |r|T + |s|^T\|\gamma_0\| & \text{if } |s|>1.\end{cases}$$

So we have $\|\boldsymbol{\gamma}_i\| \leq C_T$ for $0 \leq i < T$.

In this chapter, for any ring R, we denote by $R[\mathbf{X}]$ the polynomial ring in the variables X_0, X_1, X_2 with coefficients in R. For any $\boldsymbol{\nu} = (\nu_0, \nu_1, \nu_2) \in \mathbb{N}^3$, we denote by $\mathbf{X}^{\boldsymbol{\nu}}$ the monomial $X_0^{\nu_0} X_1^{\nu_1} X_2^{\nu_2}$ and set $|\boldsymbol{\nu}| = \nu_0 + \nu_1 + \nu_2$.

We define the *norm* $\|P\|$ of a polynomial $P \in \mathbb{C}[\mathbf{X}]$ as the largest absolute value of its coefficients and define the *length* $\mathcal{L}(P)$ as the sum of all absolute values of its coefficients.

Let $\bar{\tau}$ denote the map

$$\begin{aligned} \bar{\tau}: \quad \mathbb{C}^3 &\longrightarrow \mathbb{C}^3 \\ (x, y, z) &\longmapsto (x, y + rx, sz) \end{aligned}$$

and let τ denote the induced map from $\mathbb{P}^2(\mathbb{C})$ to $\mathbb{P}^2(\mathbb{C})$. Viewing $\mathbb{C} \times \mathbb{C}^*$ as a subset of $\mathbb{P}^2(\mathbb{C})$ under the standard embedding mapping (y, z) to $(1 : y : z)$, the map τ restricts to translation by (r, s) in the group $\mathbb{C} \times \mathbb{C}^*$.

Let Φ denote the $\mathbb{C}-$algebra isomorphism on $\mathbb{C}[\mathbf{X}]$ which sends a homogeneous polynomial $P(X_0, X_1, X_2) \in \mathbb{C}[\mathbf{X}]_D$ to $P(X_0, X_1 + rX_0, sX_2) \in \mathbb{C}[\mathbf{X}]_D$. Then we have

$$\Phi^j(P)(\bar{\tau}^i(\mathbf{z})) = \Phi^{i+j}(P)(\mathbf{z}) \quad \text{for all} \quad \mathbf{z} \in \mathbb{C}^3.$$

Now for each integer $T \geq 0$, we denote by $I^{(T)}$ the ideal of $\mathbb{C}[\mathbf{X}]$ generated by all homogeneous polynomials in $\mathbb{C}[\mathbf{X}]$ vanishing on $\mathcal{S}_T$ and denote by $I_D^{(T)}$ its homogeneous part of degree D which consists of 0 and all polynomials in $I^{(T)}$ which are homogeneous of degree D. For any $\alpha \in \mathbb{P}^2(\mathbb{C})$ with representative $\boldsymbol{\alpha}$ in $\mathbb{C}^3$ of norm 1, we also define

$$|I_D^{(T)}|_\alpha = \sup\{|P(\boldsymbol{\alpha})|;\ P \in I_D^{(T)}, \|P\| \leq 1\}.$$

For any subset W of $\mathbb{P}^2(\mathbb{C})$, we write $\underline{W}$ to denote an arbitrary set of representatives of points of W by points of $\mathbb{C}^3$ of norm 1.

1.4 Outline of the proof of Theorem 1.1.5

We provide here an outline of the proof of our main result. The strategy is similar to the one of D. Roy in [21]. The difference is that, in [21], the author considers polynomials whose derivatives are small up to a large order at one point while in our work, we consider polynomials taking small values at a large number of points which are translates of a fixed point (ξ, η) by multiples of a rational point (r, s). Despite this difference, it is surprising that we obtain a so similar looking result.

Arguing by contradiction, as in [21], we first replace P_D by an appropriate homogenization $\tilde{P}_D$ of P_D such that $\tilde{P}_D(\boldsymbol{\gamma}_i)$ is equal to $P_D(\xi + ir, \eta s^i)$ up to a product of powers of η and s, and such that $X_0 \nmid \tilde{P}_D$, $X_2 \nmid \tilde{P}_D$. The last condition ensures that the polynomials $\Phi^i(\tilde{P}_D)$ with $i \in \mathbb{Z}$ are relatively prime.

For each degree $D \geq 1$, we define a convex body $\mathcal{C}_D$ consisting of polynomials of $\mathbb{C}[\mathbf{X}]_D$ of bounded norm taking small values at $\boldsymbol{\gamma}_0, \ldots, \boldsymbol{\gamma}_{T_D}$ where $T_D = \lfloor D^\sigma \rfloor$. The precise condition defining $\mathcal{C}_D$ ensures that $\mathcal{C}_D$ contains all the polynomials $c'^{2DT_D}\Phi^j(\tilde{P}_D)$ with $0 \leq j < 2T_D$ for an appropriate positive integer c'.

The first crucial property which we prove is that the height $h_{\mathcal{C}_D}(\mathbb{P}^2(\mathbb{C}))$ of $\mathbb{P}^2(\mathbb{C})$ relative to $\mathcal{C}_D$ is a very small negative number. Recall that this height is the logarithm of the supremum of the absolute values of the resultant at triples of polynomials from $\mathcal{C}_D$. A result of [21] implies that the resultant vanishes up to order T_D at each triple of homogeneous polynomials vanishing at all points γ_i of $\mathcal{S}_{T_D}$. The problem is that the polynomials of $\mathcal{C}_D$ may not vanish on $\mathcal{S}_{T_D}$. However, they take small values at each point of $\mathcal{S}_{T_D}$. In Section 1.5, we prove an interpolation estimate which shows that, for each polynomial of $\mathcal{C}_D$, there exists a homogeneous polynomial of the same degree and small norm which takes the same values at each point γ_i of $\mathcal{S}_{T_D}$. Therefore, each triple of polynomials of $\mathcal{C}_D$ is close to a triple of polynomials vanishing on $\mathcal{S}_{T_D}$. As the resultant vanishes at the modified triples up to a very large order, an application of Schwarz's lemma implies that the resultant takes very small absolute values at triples in $\mathcal{C}_D^3$. This means that $h_{\mathcal{C}_D}(\mathbb{P}^2(\mathbb{C}))$ is a very small negative number.

Based on this, we adapt the argument in [21] to construct a $\mathbb{Q}$-subvariety Z_D of dimension 0 contained in $\mathcal{Z}(\Phi^j(\tilde{P}_D); 0 \leq j < 2T_D)$ whose height $h_{\mathcal{C}_D}(Z_D)$ relative to $\mathcal{C}_D$ is very small (negative). The existence of this $\mathbb{Q}$-subvariety Z_D is based on the lemmas of Section 1.2 which are not proved in the thesis. However, for the convenience of the reader, we give here some explanation on how Z_D is obtained (for details, see [14] and [21]). First of all, we observe that the divisor of $\tilde{P}_D$ is a $\mathbb{Q}$-cycle of dimension

1 whose height relative to $\mathcal{C}_D$ is very small (negative) since $\tilde{P}_D \in \mathcal{C}_D$ and $h_{\mathcal{C}_D}(\mathbb{P}^2(\mathbb{C}))$ is very small (negative). Then we choose an irreducible component Z' of this $\mathbb{Q}$-cycle whose height relative to $\mathcal{C}_D$ is smallest compared to the standard height and degree of Z'. Since $X_0 \nmid \tilde{P}_D, X_2 \nmid \tilde{P}_D$, there exists a polynomial $\Phi^i(\tilde{P}_D)$ with $0 \le i < D$ not vanishing on Z'. The intersection of Z' with the divisor of $\Phi^i(\tilde{P}_D)$ is a $\mathbb{Q}$-cycle of dimension 0 whose height relative to $\mathcal{C}_D$ is very small (negative). Then, we take for Z_D an irreducible component of this $\mathbb{Q}$-cycle in a similar fashion as we did for Z'.

The rest of the argument is new and differs a lot from the argument in [21] although the same idea is to reach a contradiction by intersecting (a translate of) Z_D with the divisor of a polynomial of the form $\Phi^i(\tilde{P}_D)$ for a smaller degree D'. Such a descent argument is typical in algebraic independence and is crucial for example in the proof of Philippon's criterion for algebraic independence [16]. To put this in practice, we first note that, by the penultimate lemma of Section 1.2, the height $h_{\mathcal{C}_D}(Z_D)$ is essentially equal to

$$\sum_{\boldsymbol{\alpha} \in \underline{Z}_D} \log \sup\{|P(\boldsymbol{\alpha})|;\ P \in \mathcal{C}_D\},$$

where $\underline{Z}_D$ denotes an arbitrary set of representatives of points of Z_D by points of $\mathbb{C}^3$ of norm 1. We also note that

$$\sup\{|P(\boldsymbol{\alpha})|;\ P \in \mathcal{C}_D\} \ge |I_D^{(T_D)}|_{\boldsymbol{\alpha}}$$

for each $\alpha \in Z_D$ with representative $\boldsymbol{\alpha} \in \mathbb{C}^3$ of norm 1. We show in Section 1.7 that, for each $\alpha \in \mathbb{P}^2(\mathbb{C})$, we also have

$$\log \operatorname{dist}(\alpha, \mathcal{S}_{T_D}) \le cT_D^2 + \log |I_D^{(T_D)}|_\alpha$$

for some constant $c > 0$, where $\operatorname{dist}(\alpha, \mathcal{S}_{T_D})$ denotes the smallest distance between α and a point of $\mathcal{S}_{T_D}$ (we use the projective distance defined in Section 1.7). Putting all the estimates together, we conclude that

$$\Theta = \sum_{\alpha \in Z_D^0} \log \operatorname{dist}(\alpha, \mathcal{S}_{T_D})$$

is small (negative), where Z_D^0 is a subset of Z_D obtained by extracting the points of Z_D which are far from any points of $\mathcal{S}_{T_D}$.

For each $\alpha \in Z_D^0$, we choose an integer $t_\alpha \in \{0, 1, \ldots, T_D - 1\}$ for which $\gamma_{t_\alpha} \in \mathcal{S}_{T_D}$ is closest to α. Then we have

$$\Theta = \sum_{\alpha \in Z_D^0} \log \operatorname{dist}(\alpha, \gamma_{t_\alpha}).$$

For each pair of integers (m, n) with $0 \le m < n \le T_D$, we define

$$\Theta(m, n) = \sum_{\substack{\alpha \in Z_D^0 \\ m \le t_\alpha < n}} \log \operatorname{dist}(\alpha, \gamma_{t_\alpha}).$$

We also define recursively a sequence of pair (m_k, n_k) with $k \in \mathbb{N}$ starting with $(m_0, n_0) = (0, T_D)$ such that $n_k - m_k$ is essentially $T_D/2^k$, and $\Theta(m_k, n_k)$ is at most $\dfrac{n_k - m_k}{T_D}\Theta$. We show that there exists a largest integer k such that

$$\tau^{-m_k}(Z_D) \subset \mathcal{Z}(\Phi^i(\tilde{P}_{D_k});\ 0 \le i < 2T_{D_k}), \tag{1.8}$$

where D_k is the smallest integer satisfying $n_k - m_k \le T_{D_k}$. We show that D_k tends to infinity with D. Based on (1.8), we deduce upper bounds for the degree and height of $\tau^{-m_k}(Z_D)$ in terms of D_k. Similar upper bounds then follow for the degree and height of $Z'_D := \tau^{-m_{k+1}}(Z)$ because $|m_k - m_{k+1}| \le T_D$. Now we put $D' = D_{k+1}$ where D_{k+1} is defined similarly as we did for D_k. Because of the choice of k, there exists an integer i_0 with $0 \le i < 2T_{D'}$ such that the polynomial $P := \Phi^{i_0}(\tilde{P}_{D'})$ does not vanish on Z'_D. Using a lemma of Section 1.2, this implies a lower bound for $\sum_{\boldsymbol{\alpha} \in \underline{Z}_D} \log |P(\boldsymbol{\alpha})|$ in terms of the height and degree of Z'_D.

Define W_D to be the set of $\alpha \in Z_D^0$ such that $m_{k+1} \le t_\alpha < n_{k+1}$, and for each $\alpha \in W_D$, define $\alpha' = \tau^{-m_{k+1}}(\alpha)$. Then we obtain a similar lower bound for $\sum_{\alpha \in W_D} \log |P(\boldsymbol{\alpha}')|$ where $\boldsymbol{\alpha}'$ denotes a representative in $\mathbb{C}^3$ of α'.

For each $\alpha \in W_D$, the point α' is close to $\tau^{-m_{k+1}}(\gamma_{t_\alpha}) = \gamma_{\ell_\alpha}$ where $\ell_\alpha = t_\alpha - m_{k+1}$ is an integer in the range $0 \le \ell_\alpha < n_{k+1} - m_{k+1} \le T_{D'}$. Moreover, we have

$$\begin{aligned} |P(\boldsymbol{\alpha}')| &\le \left| P\left(\frac{\boldsymbol{\gamma}_{\ell_\alpha}}{\|\boldsymbol{\gamma}_{\ell_\alpha}\|}\right)\right| + D\mathcal{L}(P)\operatorname{dist}(\alpha', \gamma_{\ell_\alpha}) \\ &\le e^{-\frac{1}{2}D'^\nu} + D'\mathcal{L}(P)\operatorname{dist}(\alpha', \gamma_{\ell_\alpha}). \end{aligned}$$

If, for some $\alpha_0 \in W_D$, we have $|P(\boldsymbol{\alpha}_0')| < 2e^{-\frac{1}{2}D'^{\nu}}$, then this is easily found to contradict the lower bound for $\sum_{\alpha \in W_D} \log |P(\boldsymbol{\alpha}')|$. We are thus reduced to the case where $|P(\boldsymbol{\alpha}')|$ is essentially bounded above by $\mathrm{dist}(\alpha', \gamma_{\ell_\alpha})$ or equivalently by $\mathrm{dist}(\alpha, \gamma_{t_\alpha})$. This give an upper bound for $\sum_{\boldsymbol{\alpha} \in W_D} \log |P(\boldsymbol{\alpha}')|$ in terms of

$$\sum_{\alpha \in W_D} \log \mathrm{dist}(\alpha, \gamma_{t_\alpha}) = \Theta(m_{k+1}, n_{k+1}).$$

Again, this contradicts the lower bound on $\sum_{\boldsymbol{\alpha} \in W_D} \log |P(\boldsymbol{\alpha}')|$.

1.5 An interpolation estimate for homogeneous polynomials

In this section, we establish an upper bound for the length of an arbitrary homogeneous polynomial of $\mathbb{C}[\mathbf{X}]_L$ in terms of the values which it takes at the points of $\mathcal{S}_M$ where $M = \binom{L+2}{2}$. This implies that any polynomial in $\mathbb{C}[\mathbf{X}]_L$ is determined uniquely by its values on $\mathcal{S}_M$. We will use this result to construct interpolation polynomials in the next section.

Lemma 1.5.1. *Let $L \in \mathbb{N}$ and put $M = \binom{L+2}{2}$. Then there exists a constant $c = c(r, s, \xi, \eta) \geq 3$ such that any $Q \in \mathbb{C}[\mathbf{X}]_L$ has length satisfying*

$$\mathcal{L}(Q) \leq \begin{cases} c^{L^2} \cdot \max_{0 \leq i < M} |Q(\boldsymbol{\gamma}_i)| & \text{if } |s| > 1, \\ c^{L^3} \cdot \max_{0 \leq i < M} |Q(\boldsymbol{\gamma}_i)| & \text{if } |s| < 1. \end{cases} \tag{1.9}$$

Consequently, the linear map

$$\begin{aligned} \phi : \mathbb{C}[\mathbf{X}]_L &\longrightarrow \mathbb{C}^M \\ Q &\longmapsto (Q(\boldsymbol{\gamma}_i))_{0 \leq i < M} \end{aligned}$$

is bijective.

Proof. Note that the estimate (1.9) implies that the linear map ϕ is injective. Then, since $\dim \mathbb{C}[\mathbf{X}]_L = \dim \mathbb{C}^M$, this yields that ϕ is bijective.

It remains to show the first assertion. The result is clear for $L = 0$ since then $Q \in \mathbb{C}$. Assume that $L > 0$. We note that, for each $(j,k) \in \mathbb{N}^2$ with $j + k = L$, the polynomial

$$Q_{jk}(\mathbf{X}) = X_0^{L-j-k} \prod_{i=0}^{j-1} (X_1 - (\xi + ir)X_0)$$

has degree j in X_1. Hence, for each $k \le L$, the polynomials $Q_{j,k}$ with $j = 0, \dots, L-k$ are linearly independent. This implies that the polynomials

$$(\eta^{-1}X_2)^k Q_{j,k} \quad ((j,k) \in \mathbb{N}^2,\ j + k = L)$$

are linearly independent, and so form a basis of $\mathbb{C}[\mathbf{X}]_L$ since their cardinal is $M = \dim \mathbb{C}[\mathbf{X}]_L$.

Fix $Q \in \mathbb{C}[\mathbf{X}]_L$. We write

$$Q(\mathbf{X}) = \sum_{j+k \le L} c_{jk} (\eta^{-1}X_2)^k Q_{j,k}(\mathbf{X})$$

for some $c_{jk} \in \mathbb{C}$. We have

$$\begin{aligned} \mathcal{L}(Q) \le & \sum_{j+k \le L} |c_{jk}|\ |\eta|^{-k} \prod_{i=0}^{j-1} (1 + |\xi| + i|r|) \\ \le & \sum_{j+k \le L} |c_{jk}|\ |\eta|^{-k} (1 + |\xi| + |r|) \prod_{i=1}^{j-1} i(1 + |\xi| + |r|) \\ \le & 2^M \max_{j+k \le L} \Big\{ |c_{jk}|\ |\eta|^{-k} (1 + |\xi| + |r|)^j . j! \Big\}. \end{aligned}$$

To find an upper bound for $|c_{jk}|$, we set $P(\mathbf{X}) = Q(X_0, X_1 + \xi X_0, \eta X_2)$. We have

$$P(\mathbf{X}) = \sum_{j+k \le L} c_{jk} X_0^{L-j-k} X_1 (X_1 - rX_0) \cdots (X_1 - (j-1)rX_0) X_2^k.$$

For each $(i,k) \in \mathbb{N}^2$, put

$$u_i^{(j,k)} = \begin{cases} i(i-1)\cdots(i-j+1) r^j s^{ik} & \text{if } j > 0, \\ s^{ik} & \text{if } j = 0, \end{cases}$$

and, for each, $k \in \mathbb{N}$ define a sequence $u^{(j,k)}$ by $u^{(j,k)} = (u_i^{(j,k)})_{i \in \mathbb{N}}$. Set

$$u = \sum_{j+k \le L} c_{jk} u^{(j,k)}.$$

Then

$$u_i = \sum_{j+k\le L} c_{jk}\, u_i^{(j,k)} = P(1, ir, s^i) = Q(\boldsymbol{\gamma}_i).$$

Let τ denote the linear operator on $\mathbb{C}^{\mathbb{N}}$ which sends a sequence $(x_n)_{n\in\mathbb{N}}$ to the shifted sequence $(x_{n+1})_{n\in\mathbb{N}}$. For each $(j', k') \in \mathbb{N}^2$ satisfying $j' + k' \le L$, we will construct a polynomial $F_{j',k'} \in \mathbb{C}[T]$ of degree $< M$ such that

$$\big(F_{j',k'}(\tau)(u^{(j,k)})\big)_0 = \begin{cases} 1 & \text{if} \quad (j', k') = (j, k), \\ 0 & \text{else.} \end{cases} \tag{1.10}$$

If we take this for granted, then $c_{jk} = \big(F_{jk}(\tau)(u)\big)_0$. Moreover, since $\deg F_{jk} < M$, we have

$$\begin{aligned} |c_{jk}| = |\big(F_{jk}(\tau)(u)\big)_0| &\le \mathcal{L}(F_{jk}) \max\{|(\tau^i(u))_0|\,;\ 0 \le i < M\} \\ &\le \mathcal{L}(F_{jk}) \max\{|u_i|\,;\ 0 \le i < M\} \\ &\le \mathcal{L}(F_{jk}) \max\{|Q(\boldsymbol{\gamma}_i)|\,;\ 0 \le i < M\} \end{aligned}$$

So we also need an upper bound for $\mathcal{L}(F_{jk})$ to estimate $|c_{jk}|$.
Fix $(j_0, k_0) \in \mathbb{N}^2$ such that $j_0 + k_0 \le L$. We now proceed to construct $F_{j_0k_0}$. We claim that

$$(\tau - s^k)^m (u^{(j,k)}) = \begin{cases} j(j-1)\cdots(j-m+1)(rs^k)^m u^{(j-m,k)} & \text{if } m \le j \\ 0 & \text{if } m > j \end{cases} \tag{1.11}$$

Indeed, for $m = 1$, and $j \ge 1$, we have

$$\begin{aligned} ((\tau - s^k)(u^{(j,k)}))_i &= (i+1)i\cdots(i-j+2) r^j s^{(i+1)k} - i(i-1)\cdots(i-j+1) r^j s^{ik+k} \\ &= (rs^k)\big((i+1) - (i-j+1)\big) i \cdots (i-j+2)\, r^{j-1} s^{ik} \\ &= (rs^k) j u_i^{(j-1,k)}. \end{aligned}$$

So by induction on m, we find that (1.11) is true for $m \le j$. Since $u_i^{(0,k)} = s^{ik}$, we also have $(\tau - s^k)(u^{(0,k)}) = 0$. From this, we deduce that (2.30) is also true for $m > j$.

Now using (1.11) and $u_0^{(j,k)} = \delta_{0j}$, we get

$$((\tau - s^{k_0})^{j_0} (u^{(j,k_0)}))_0 = (rs^{k_0})^{j_0} j_0! \delta_{j_0 j}. \tag{1.12}$$

In particular, we have

$$(\tau - s^{k_0})^{L-k_0+1}(u^{(j_0,k_0)}) = 0 \quad \text{since } j_0 + k_0 \leq L.$$

Since this holds for any (j_0, k_0) with $j_0 + k_0 < L$, we deduce that

$$\prod_{\substack{k' \neq k_0 \\ k'=0,\ldots,L}} (\tau - s^{k'})^{L-k'+1}(u^{(j,k)}) = 0 \quad \text{when } k \neq k_0,\ j + k \leq L. \tag{1.13}$$

By [19, Lemma 3.2], there exists a unique polynomial $a_{j_0,k_0}(Y) \in \mathbb{C}[Y]$ of degree $\leq L - j_0 - k_0$ such that

$$a_{j_0,k_0}(Y) \prod_{\substack{k' \neq k_0 \\ k'=0,\ldots,L}} \left(1 - \frac{Y}{s^{k'} - s^{k_0}}\right)^{L-k'+1} \equiv 1 \mod Y^{L-j_0-k_0+1} \tag{1.14}$$

and it satisfies

$$\begin{aligned}
\mathcal{L}(a_{j_0,k_0}) &\leq \binom{M - j_0 - 1}{L - j_0 - k_0} \max_{\substack{k' \neq k_0 \\ k'=0,\cdots,L}} \left\{1,\ \frac{1}{|s^{k'} - s^{k_0}|}\right\}^{L-j_0-k_0} \\
&\leq \begin{cases} 2^M \max\left\{1, \frac{1}{|s|-1}\right\}^L & \text{if } |s| > 1, \\ 2^M \max\left\{1, \frac{1}{|s|^L(1-|s|)}\right\}^L & \text{if } |s| < 1 \end{cases} \\
&\leq \begin{cases} 2^M c_1^L & \text{if } |s| > 1 \\ 2^M c_2^{L^2} & \text{if } |s| < 1 \end{cases}
\end{aligned}$$

where $c_1 = \dfrac{|s|}{|s| - 1}$ and $c_2 = \dfrac{1}{|s|(1 - |s|)}$. Replacing Y by $T - s^{k_0}$ in (1.14), we get

$$a_{j_0,k_0}(T - s^{k_0}) \prod_{\substack{k' \neq k_0 \\ k'=0,\ldots,L}} \left(\frac{T - s^{k'}}{s^{k_0} - s^{k'}}\right)^{L-k'+1} \equiv 1 \mod (T - s^{k_0})^{L-j_0-k_0+1}. \tag{1.15}$$

This yields the following congruence modulo $(X - s^{k_0})^{L-k_0+1}$

$$(T - s^{k_0})^{j_0} a_{j_0,k_0}(T - s^{k_0}) \prod_{\substack{k' \neq k_0 \\ k'=0,\ldots,L}} \left(\frac{T - s^{k'}}{s^{k_0} - s^{k'}}\right)^{L-k'+1} \equiv (T - s^{k_0})^{j_0}.$$

Now take

$$F_{j_0,k_0}(T) = \frac{1}{(rs^{k_0})^{j_0} j_0!}(T - s^{k_0})^{j_0} a_{j_0,k_0}(T - s^{k_0}) \prod_{\substack{k \neq k_0 \\ k=0,\ldots,L}} \left(\frac{T - s^k}{s^{k_0} - s^k}\right)^{L-k+1}$$

Then F_{j_0,k_0} has degree $< M$ and from (1.13) and (1.15) we get

$$F_{j_0,k_0}(\tau)(u^{(j,k)}) = \begin{cases} 0 & \text{if } k \neq k_0, \\ \frac{1}{(rs^{k_0})^{j_0} j_0!}(\tau - s^{k_0})^{j_0}(u^{(j,k_0)}) & \text{if } k = k_0. \end{cases}$$

By (1.12), we get (1.10) as required.

Now, it remains to find an upper bound for $\mathcal{L}(F_{j_0,k_0})$. We have

$$\begin{aligned} \mathcal{L}(F_{j_0,k_0}) &\leq \frac{1}{|rs^{k_0}|^{j_0} j_0!}(1 + |s|^{k_0})^{j_0} \mathcal{L}(a_{j_0,k_0})(1 + |s|^{k_0})^{L-j_0-k_0} \prod_{\substack{k \neq k_0 \\ k=0,\ldots,L}} \left(\frac{1 + |s|^k}{|s^k - s^{k_0}|}\right)^{L-k+1} \\ &\leq \frac{\mathcal{L}(a_{j_0,k_0})}{|rs^{k_0}|^{j_0} j_0!}(1 + |s|^{k_0})^{L-k_0} \prod_{\substack{k \neq k_0 \\ k=0,\ldots,L}} \left(\frac{1 + |s|^k}{||s|^k - |s|^{k_0}|}\right)^{L-k+1}. \end{aligned}$$

In the case where $|s| > 1$, we have

$$\begin{aligned} \mathcal{L}(F_{j_0,k_0}) &\leq \frac{2^M c_1^L}{|rs^{k_0}|^{j_0} j_0!}(2|s|^{k_0})^{L-k_0} \prod_{\substack{k \neq k_0 \\ k=0,\ldots,L}} \left(\frac{2|s|^k}{|s|^{k-1}(|s| - 1)}\right)^{L-k+1} \\ &\leq \frac{2^{M+L} c_1^L}{|r|^{j_0} j_0!}|s|^{k_0(L-k_0-j_0)} \prod_{\substack{k \neq k_0 \\ k=0,\ldots,L}} (2c_1)^{L-k+1} \\ &\leq \frac{(4c_1|s|)^{M+L}}{|r|^{j_0} j_0!} \end{aligned}$$

upon noting that $k_0(L - k_0) \leq L^2/4 \leq M$.

In the case where $|s| < 1$, we have

$$\begin{aligned}
\mathcal{L}(F_{j_0,k_0}) &\leq \frac{\mathcal{L}(a_{j_0,k_0})}{|r|^{j_0} j_0!} \frac{(1+|s|^{k_0})^{L-k_0}}{|s|^{k_0(L-k_0)}} \prod_{\substack{k\neq k_0\\ k=0,\dots,L}} \left(\frac{1+|s|^k}{||s|^k - |s|^{k_0}|} \right)^{L-k+1} \\
&\leq \frac{2^M c_2^{L^2}}{|r|^{j_0} j_0!} \prod_{k=0}^{L} \left(\frac{2}{|s|^L (1-|s|)} \right)^{L-k+1} \\
&\leq \frac{4^M c_2^{L(M+L)}}{|r|^{j_0} j_0!} \leq \frac{(2c_2)^{4L^3}}{|r|^{j_0} j_0!}.
\end{aligned}$$

Now we have

$$\begin{aligned}
\mathcal{L}(Q) &\leq 2^M \max_{j+k\leq L} \left\{ (1+|\xi|+|r|)^j j! |\eta|^{-k} |c_{jk}| \right\} \\
&\leq 2^M \max_{j+k\leq L} \left\{ (1+|\xi|+|r|)^j j! |\eta|^{-k} L(F_{jk})| \right\} \max_{0\leq i<M} |Q(\boldsymbol{\gamma}_i)|.
\end{aligned}$$

Take $c' = 1 + \frac{1+|\xi|+|r|}{|r|} + |\eta|^{-1}$ we get

$$\mathcal{L}(Q) \leq \begin{cases} 2^M c'^L (4c_1|s|)^{M+L} \cdot \max\limits_{0\leq i<M} |Q(\boldsymbol{\gamma}_i)| & \text{if } |s| > 1, \\ \\ 2^M c'^L (2c_2)^{4L^3} \cdot \max\limits_{0\leq i<M} |Q(\boldsymbol{\gamma}_i)| & \text{if } |s| < 1. \end{cases}$$

We deduce that there exists $c = c(r, s, \xi, \eta) > 1$ satisfying (1.9). □

Now we will give an example which shows that the estimate (1.9) established in Lemma 1.5.1 is a good upper bound for $\mathcal{L}(Q)$.

Example 1.5.2. Take $r = 1, \xi = 0, \eta = 1$. Since ϕ is an isomorphism, there exists $Q \in \mathbb{C}[\mathbf{X}]_L$ such that $(Q(1, i, s^i))_{0\leq i<M} = (0, \dots, 0, 1)$.
Write

$$Q(\mathbf{X}) = c_{0L} X_2^L + \sum_{\substack{j+k\leq L\\ k\neq L}} c_{jk} X_0^{L-j-k} X_1 (X_1 - rX_0) \cdots (X_1 - (j-1)rX_0) X_2^k.$$

Note that, in the proof of Lemma 1.5.1, if $j + k = L$ then we have $a_{jk}(X) = 1$. Thus, the polynomial

$$F_{0L}(T) = \prod_{k=0}^{L-1} \left(\frac{T - s^k}{s^L - s^k} \right)^{L-k+1}$$

satisfies $c_{0L} = [F_{0L}(\tau)(u)]_0 \leq \mathcal{L}(Q)$ where $u_i = 0$ for all $i < M-1$ and $u_{M-1} = 1$. Since $\deg F_{0L} = \sum_{k=0}^{L-1}(L-k+1) = M-1$ and $(\tau^i(u))_0 = 0$ for $i < M-1$, $[\tau^{M-1}(u)]_0 = 1$, we deduce that $[F_{0L}(\tau)(u)]_0$ is exactly the leading coefficient of $F_{0L}(T)$. So

$$[F_{0L}(\tau)(u)]_0 = \prod_{k=0}^{L-1} \left(\frac{1}{s^L - s^k}\right)^{L-k+1}.$$

Take $s = 1/2$, by induction on L, we can check

$$|[F_{0L}(\tau)(u)]_0| = \prod_{k=0}^{L-1} \left(\frac{2^{L+k}}{2^L - 2^k}\right)^{L-k+1} \geq 2^{\frac{1}{6}L^3}.$$

So

$$2^{\frac{1}{6}L^3} \leq \mathcal{L}(Q) \leq c^{L^3} = c^{L^3} \cdot \max\{|Q(\boldsymbol{\gamma}_i)|, 0 \leq i < M\}.$$

1.6 Decomposition of polynomials in $I^{(T)}$

In general, given an arbitrary homogeneous ideal J in $\mathbb{C}[\mathbf{X}]$, we cannot expect that $J_N \subset \langle J_D \rangle$ when $N \geq D$ where J_N, J_D denote the homogeneous parts of J of respective degrees N, D. In this section, we consider the ideal $I^{(T)} = \mathcal{I}(\mathcal{S}_T)$, defined in section 1.3. We will show that

$$I_N^{(T)} \subset \langle I_D^{(T)} \rangle$$

when $N \geq D$ and $T \leq \binom{\lfloor D/2 \rfloor + 2}{2}$. More precisely, for any polynomial $Q \in I_N^{(T)}$, we will prove that

$$Q = \sum_{\substack{\boldsymbol{\nu} \in \mathbb{N}^3 \\ |\boldsymbol{\nu}| = N-D}} \mathbf{X}^{\boldsymbol{\nu}} Q_{\boldsymbol{\nu}}$$

for some $Q_{\boldsymbol{\nu}} \in I_D^{(T)}$ with an upper bound for $\sum \mathcal{L}(Q_{\boldsymbol{\nu}})$. Assuming that $N = T$, this will lead to an upper bound for $|I_T^{(T)}|_\alpha$ in terms of $|I_D^{(T)}|_\alpha$, valid for any $\alpha \in \mathbb{P}^2(\mathbb{C})$.

Lemma 1.6.1. *Let $K, L, N, T \in \mathbb{N}$ such that*

$$N + L \leq 2K \leq 2N \leq 3K + 2, \qquad T \leq \binom{L+2}{2}$$

and let $Q \in I_N^{(T)}$. *Then we can write*

$$Q = \sum_{j=0}^{2} X_j^{N-K} Q_j$$

for some $Q_j \in I_K^{(T)}$ *satisfying*

$$\sum_{j=0}^{2} \mathcal{L}(Q_j) \leq \begin{cases} 3c^{L^3} c_1^K T^K \mathcal{L}(Q) & \text{if } |s| < 1, \\ 3c^{L^2} c_1^{TK} \mathcal{L}(Q) & \text{if } |s| > 1 \end{cases}$$

where $c_1 = 1 + |\xi| + |\eta| + |r| + |s|$ *and* c *is as in Lemma 1.5.1.*

Proof. Since $N > 3(N-K-1)$, for each triple $\boldsymbol{\nu}$ in $S := \{\boldsymbol{\nu} \in \mathbb{N}^3; \ |\boldsymbol{\nu}| = N\}$, there exists at least one coordinate $\geq N-K$. For each $t = 0, 1, 2$, set

$$S_t = \{\boldsymbol{\nu} = (\nu_0, \nu_1, \nu_2) \in S \ ; \ \nu_t \geq N-K\}.$$

Then

$$S = S_0 \cup S_1 \cup S_2.$$

Fix $Q = \sum_{\substack{\boldsymbol{\nu} \in \mathbb{N}^3 \\ |\boldsymbol{\nu}| = N-D}} c_{\boldsymbol{\nu}} \mathbf{X}^{\boldsymbol{\nu}} \in I_N^{(T)}$. Then we have $Q = \sum_{j=0}^{2} X_j^{N-K} P_j$ where

$$P_0 = \sum_{\boldsymbol{\nu} \in S_0} c_{\boldsymbol{\nu}} \frac{\mathbf{X}^{\boldsymbol{\nu}}}{X_0^{N-K}},$$
$$P_1 = \sum_{\boldsymbol{\nu} \in S_1 \setminus S_0} c_{\boldsymbol{\nu}} \frac{\mathbf{X}^{\boldsymbol{\nu}}}{X_1^{N-K}},$$
$$P_2 = \sum_{\boldsymbol{\nu} \in S_2 \setminus (S_0 \cup S_1)} c_{\boldsymbol{\nu}} \frac{\mathbf{X}^{\boldsymbol{\nu}}}{X_2^{N-K}}$$

are polynomials in $\mathbb{C}[\mathbf{X}]_K$. We find that $\mathcal{L}(Q) = \sum_{j=0}^{2} \mathcal{L}(P_j)$.

Applying Lemma 1.5.1 with $M = \binom{L+2}{2}$, we get that, for each $1 \leq j \leq 2$, there exists $R_j \in \mathbb{C}[\mathbf{X}]_L$ such that

$$R_j(\boldsymbol{\gamma}_i) = \begin{cases} P_j(\boldsymbol{\gamma}_i) & \text{if } 0 \leq i < T, \\ 0 & \text{if } T \leq i < M. \end{cases}$$

and

$$\mathcal{L}(R_j) \le \begin{cases} c^{L^3} \max\limits_{0\le i<T} |P_j(\boldsymbol{\gamma}_i)| & \text{if } |s|<1, \\ c^{L^2} \max_{0\le i<T} |P_j(\boldsymbol{\gamma}_i)| & \text{if } |s|>1. \end{cases}$$

For each $0 \le i < T$, we have

$$\begin{aligned} |P_j(\boldsymbol{\gamma}_i)| &\le \mathcal{L}(P_j)\cdot \max\{1, |\xi+ir|^{t_1}|\eta s^i|^{t_2};\ t_1+t_2\le K\} \\ &\le \begin{cases} c_1^K T^K \cdot \mathcal{L}(P_j) & \text{if } |s|<1, \\ c_1^{TK}\cdot \mathcal{L}(P_j) & \text{if } |s|>1. \end{cases} \end{aligned}$$

Hence

$$\mathcal{L}(R_j) \le \begin{cases} c^{L^3} c_1^K T^K \cdot \mathcal{L}(P_j) & \text{if } |s|<1, \\ c^{L^2} c_1^{TK} \cdot \mathcal{L}(P_j) & \text{if } |s|>1. \end{cases}$$

Since $2K-L \ge N$, and $N \ge K \ge L$, the polynomials

$$\begin{aligned} &Q_0 = P_0 + X_0^{2K-L-N}(X_1^{N-K}R_1 + X_2^{N-K}R_2), \\ &Q_1 = P_1 - X_0^{K-L}R_1, \\ &Q_2 = P_2 - X_0^{K-L}R_2 \end{aligned}$$

belong to $\mathbb{C}[\mathbf{X}]_K$. By construction, we have $Q_1, Q_2 \in I^{(T)}$. Since $Q=\sum_{j=0}^2 X_j^{N-K}Q_j$ belongs to $I^{(T)}$, we deduce that $X_0^{N-K}Q_0 \in I^{(T)}$, hence $Q_0 \in I^{(T)}$. Moreover we have

$$\begin{aligned} \sum_{j=0}^{2}\mathcal{L}(Q_j) &\le 2\mathcal{L}(R_1) + 2\mathcal{L}(R_2) + \sum_{j=0}^{2}\mathcal{L}(P_j) \\ &\le \begin{cases} 2c^{L^3}c_1^K T^K\cdot(\mathcal{L}(P_1)+\mathcal{L}(P_2)) + \mathcal{L}(Q) & \text{if } |s|<1, \\ 2c^{L^2}c_1^{TK}\cdot(\mathcal{L}(P_1)+\mathcal{L}(P_2)) + \mathcal{L}(Q) & \text{if } |s|>1. \end{cases} \\ &\le \begin{cases} 3c^{L^3}c_1^K T^K \mathcal{L}(Q) & \text{if } |s|<1, \\ 3c^{L^2}c_1^{TK}\mathcal{L}(Q) & \text{if } |s|>1. \end{cases} \end{aligned}$$

□

Proposition 1.6.2. *Let D, N, T be positive integers with $N \ge D$ and $T \le \binom{\lfloor D/2\rfloor+2}{2}$. Then any $Q \in I_N^{(T)}$ can be written in the form*

$$Q = \sum_{\substack{\boldsymbol{\nu}\in\mathbb{N}^3 \\ |\boldsymbol{\nu}|=N-D}} \mathbf{X}^{\boldsymbol{\nu}} Q_{\boldsymbol{\nu}}$$

for a choice of polynomials $Q_{\boldsymbol{\nu}} \in I_D^{(T)}$ *satisfying*

$$\sum_{\substack{\boldsymbol{\nu}\in\mathbb{N}^3 \\ |\boldsymbol{\nu}|=N-D}} \mathcal{L}(Q_{\boldsymbol{\nu}}) \leq \begin{cases} c^{N^3} c_1^{2N} T^{2N} \cdot \mathcal{L}(Q) & \text{if } |s|<1, \\ c^{N^2} c_1^{2NT} \cdot \mathcal{L}(Q) & \text{if } |s|>1, \end{cases} \tag{1.16}$$

where c_1, c *are as in Lemma 1.6.1 .*

Proof. We will proceed by induction on N. The result is clear for $N = D$. When $N > D$, we consider two cases.

Case 1: $2N \leq 3D$

Take $K = D$ and $L = 2D - N$. Then we have

$$N + L = 2K \leq 2N \leq 3K$$

and $L \geq D/2$ (since $2N \leq 3D$), so

$$T \leq \binom{\lfloor D/2 \rfloor + 2}{2} \leq \binom{L+2}{2}.$$

Lemma 1.6.1 ensures the existence of $Q_0, Q_1, Q_2 \in I_D^{(T)}$ such that $Q = \sum_{j=0}^{2} X_j^{N-D} Q_j$ and

$$\sum_{j=0}^{2} \mathcal{L}(Q_j) \leq \begin{cases} 3c^{L^3} c_1^{D} T^{D} \cdot \mathcal{L}(Q) & \text{if } |s|<1, \\ 3c^{L^2} c_1^{DT} \cdot \mathcal{L}(Q) & \text{if } |s|>1, \end{cases}$$

and (1.16) is satisfied since $D \leq N$, $L < N$ and $c \geq 3$.

Case 2: $2N > 3D$

Take $K = N - \lfloor N/3 \rfloor$, $L = \lfloor N/3 \rfloor$. Since $N/3 \geq D/2$, we have $L \geq \lfloor D/2 \rfloor$ and so

$$T \leq \binom{\lfloor D/2 \rfloor + 2}{2} \leq \binom{L+2}{2}.$$

On the other hand, we have

$$\begin{aligned} N + L = N + \lfloor N/3 \rfloor &\leq N + (N - 2\lfloor N/3 \rfloor) = 2K \\ &\leq 2N \leq 2N + (N - 3\lfloor N/3 \rfloor) = 3K. \end{aligned}$$

Lemma 1.6.1 ensures the existence of $Q_0, Q_1, Q_2 \in I_K^{(T)}$ such that $Q = \sum_{j=0}^{2} X_j^{N-K} Q_j$ and

$$\sum_{j=0}^{2} \mathcal{L}(Q_j) \leq \begin{cases} 3c^{L^3} c_1^K T^K \cdot \mathcal{L}(Q) & \text{if } |s| < 1, \\ 3c^{L^2} c_1^{KT} \cdot \mathcal{L}(Q) & \text{if } |s| > 1. \end{cases}$$

If $K \leq D$ then (1.16) is satisfied since $L, D < N$. Otherwise, applying the induction hypothesis, for each $0 \leq j \leq 2$, we can write

$$Q_j = \sum_{\substack{\boldsymbol{\nu}' \in \mathbb{N}^3 \\ |\boldsymbol{\nu}'| = K-D}} \mathbf{X}^{\boldsymbol{\nu}'} Q_{j\boldsymbol{\nu}'}$$

for a choice of polynomials $Q_{j\boldsymbol{\nu}'} \in I_D^{(T)}$ satisfying

$$\sum_{\substack{\boldsymbol{\nu}' \in \mathbb{N}^3 \\ |\boldsymbol{\nu}'| = K-D}} \mathcal{L}(Q_{j\boldsymbol{\nu}'}) \leq \begin{cases} c^{K^3} c_1^{2K} T^{2K} \cdot \mathcal{L}(Q_j) & \text{if } |s| < 1, \\ c^{K^2} c_1^{2KT} \cdot \mathcal{L}(Q_j) & \text{if } |s| > 1. \end{cases}$$

So

$$Q = \sum_{j=0}^{2} X_j^{N-K} \left(\sum_{\substack{\boldsymbol{\nu}' \in \mathbb{N}^3 \\ |\boldsymbol{\nu}'| = K-D}} \mathbf{X}^{\boldsymbol{\nu}'} Q_{j\boldsymbol{\nu}'} \right)$$

with

$$\begin{aligned} \sum_{j=0}^{2} \sum_{\substack{\boldsymbol{\nu}' \in \mathbb{N}^3 \\ |\boldsymbol{\nu}'| = K-D}} \mathcal{L}(Q_{j\boldsymbol{\nu}'}) &\leq \begin{cases} c^{K^3} c_1^{2K} T^{2K} \cdot 3c^{L^3} c_1^K T^K \cdot \mathcal{L}(Q) & \text{if } |s| < 1, \\ c^{K^2} c_1^{2KT} \cdot 3c^{L^2} c_1^{KT} \cdot \mathcal{L}(Q) & \text{if } |s| > 1, \end{cases} \\ &\leq \begin{cases} c^{N^3} c_1^{2N} T^{2N} \cdot \mathcal{L}(Q) & \text{if } |s| < 1, \\ c^{N^2} c_1^{2NT} \cdot \mathcal{L}(Q) & \text{if } |s| > 1, \end{cases} \end{aligned}$$

using $K^3 + L^3 < (K+L)^3 = N^3$, $K^2 + L^2 < (K+L)^2 = N^2$ and $c \geq 3$. $\square$

Applying the above proposition with $N = T$, we obtain the following result.

Corollary 1.6.3. *Let D, T be positive integers with $D \leq T \leq \binom{\lfloor D/2 \rfloor + 2}{2}$. Let c and c_1 be as in Lemma 1.6.1. For any $\alpha \in \mathbb{P}^2(\mathbb{C})$, we have*

$$|I_T^{(T)}|_\alpha \leq \begin{cases} c^{T^3} c_1^{2T} T^{2T} 3^D \cdot |I_D^{(T)}|_\alpha & \text{if } |s| < 1, \\ c^{T^2} c_1^{2T^2} 3^D \cdot |I_D^{(T)}|_\alpha & \text{if } |s| > 1. \end{cases}$$

Proof. Let $\boldsymbol{\alpha} \in \mathbb{C}^3$ be a representative of α of norm 1 and let $Q \in I_T^{(T)}$ with $\|Q\| \leq 1$. Write $Q = \sum_{\substack{\boldsymbol{\nu}\in\mathbb{N}^3 \\ |\boldsymbol{\nu}|=T-D}} \mathbf{X}^{\boldsymbol{\nu}} Q_{\boldsymbol{\nu}}$ as in Proposition 1.6.2. Then

$$\begin{aligned}
|Q(\boldsymbol{\alpha})| &\leq \sum_{\substack{\boldsymbol{\nu}\in\mathbb{N}^3 \\ |\boldsymbol{\nu}|=T-D}} |Q_{\boldsymbol{\nu}}(\boldsymbol{\alpha})| \leq \sum_{\substack{\boldsymbol{\nu}\in\mathbb{N}^3 \\ |\boldsymbol{\nu}|=T-D}} \|Q_{\boldsymbol{\nu}}\| \cdot |I_D^{(T)}|_\alpha \\
&\leq \sum_{\substack{\boldsymbol{\nu}\in\mathbb{N}^3 \\ |\boldsymbol{\nu}|=T-D}} \mathcal{L}(Q_{\boldsymbol{\nu}}) \cdot |I_D^{(T)}|_\alpha \\
&\leq \begin{cases} c^{T^3} c_1^{2T} T^{2T} \mathcal{L}(Q) \cdot |I_D^{(T)}|_\alpha & \text{if } |s| < 1, \\ c^{T^2} c_1^{2T^2} \mathcal{L}(Q) \cdot |I_D^{(T)}|_\alpha & \text{if } |s| > 1. \end{cases}
\end{aligned}$$

The conclusion follows since $\mathcal{L}(Q) \leq 3^D \|Q\| \leq 3^D$ and $c > 3$. □

1.7 Distance

For any points $u, v \in \mathbb{P}^2(\mathbb{C})$ with representatives $\mathbf{u} = (u_0, u_1, u_2)$, $\mathbf{v} = (v_0, v_1, v_2)$ in $\mathbb{C}^3$, we define the *projective distance* between u and v by

$$\operatorname{dist}(u, v) = \frac{\|\mathbf{u} \wedge \mathbf{v}\|}{\|\mathbf{u}\| \, \|\mathbf{v}\|}.$$

This is independent of the choice of $\mathbf{u}$ and $\mathbf{v}$. The *projective distance* from v to a finite subset $\mathcal{S}$ of $\mathbb{P}^2(\mathbb{C})$ is defined by

$$\operatorname{dist}(v, \mathcal{S}) = \min\{\operatorname{dist}(v, \gamma); \gamma \in \mathcal{S}\}.$$

Recall that γ_i is the point of $\mathbb{P}^2(\mathbb{C})$ with homogeneous coordinates $\boldsymbol{\gamma}_i = (1, \xi + ir, \eta s^i)$ and that $\mathcal{S}_T$ is the set of points γ_i with $0 \leq i < T$. Recall also that

$$C_T = \begin{cases} \|\gamma_0\| + |r|T & \text{if } |s| < 1, \\ |r|T + |s|^T \|\gamma_0\| & \text{if } |s| > 1. \end{cases}$$

In this section, we establish some estimates for the projective distance which are crucial for the proof of the main result.

Lemma 1.7.1. *Let $\alpha \in \mathbb{P}^2(\mathbb{C})$ with representative $\boldsymbol{\alpha} = (\alpha_0, \alpha_1, \alpha_2)$ of norm 1.*

(i) If $\mathrm{dist}(\alpha, \gamma_i) < \dfrac{1}{2\|\boldsymbol{\gamma}_i\|}$ *for some $i \geq 0$, then* $|\alpha_0| > \dfrac{1}{2\|\boldsymbol{\gamma}_i\|}$.

(ii) For any positive integer T , there exists at most one non-negative integer $i < T$ such that

$$\mathrm{dist}(\alpha, \gamma_i) < \frac{|r|}{4C_T^2}.$$

Proof. (i) Assume that $\mathrm{dist}(\alpha, \gamma_i) < 1/(2\|\boldsymbol{\gamma}_i\|)$. Then we have

$$\max\{|\alpha_0(\xi + ir) - \alpha_1|, |\alpha_0 \eta s^i - \alpha_2|\} \leq \|\boldsymbol{\alpha} \wedge \boldsymbol{\gamma}_i\| < 1/2.$$

This implies that

$$|\alpha_0| > \frac{\max\{|\alpha_1|, |\alpha_2|\} - 1/2}{\|\boldsymbol{\gamma}_i\|},$$

which yields the required estimate for α_0 since $\|\boldsymbol{\alpha}\| = 1$.

(ii) Assume that $\mathrm{dist}(\alpha, \gamma_i) < \dfrac{|r|}{4C_T^2}$ for some $i < T$. Since $C_T \geq \max\{|r|, \|\gamma_i\|\}$, we find that $\mathrm{dist}(\alpha, \gamma_i) < (2\|\gamma_i\|)^{-1}$. We conclude from part (i) that $|\alpha_0| > (2\|\gamma_i\|)^{-1} > (2C_T)^{-1}$. For any integer j with $j \neq i$, we have

$$\begin{aligned}\mathrm{dist}(\alpha, \gamma_i) + \mathrm{dist}(\alpha, \gamma_j) &\geq \frac{\|\boldsymbol{\alpha} \wedge \boldsymbol{\gamma}_i\| + \|\boldsymbol{\alpha} \wedge \boldsymbol{\gamma}_j\|}{C_T} \\ &\geq \frac{\|\boldsymbol{\alpha} \wedge (\boldsymbol{\gamma}_i - \boldsymbol{\gamma}_j)\|}{C_T} \\ &\geq \frac{|\alpha_0(i-j)r|}{C_T} \\ &\geq \frac{|r|}{2C_T^2}.\end{aligned}$$

Using the assumption, we conclude that $\mathrm{dist}(\alpha, \gamma_j) \geq |r|(4C_T^2)^{-1}$. □

Proposition 1.7.2. *Let D, T be as in Corollary 1.6.3. Then there exists a constant $c_2 = c_2(r, s, \xi, \eta) > 1$ such that*

$$\mathrm{dist}(\alpha, \mathcal{S}_T) \leq \begin{cases} c_2^{T^3} |I_D^{(T)}|_\alpha & \text{if } |s| < 1, \\ c_2^{T^2} |I_D^{(T)}|_\alpha & \text{if } |s| > 1 \end{cases} \tag{1.17}$$

for any $\alpha \in \mathbb{P}^2(\mathbb{C})$.

Proof. Let $\alpha \in \mathbb{P}^2(\mathbb{C})$ with representative $\boldsymbol{\alpha}$ in $\mathbb{C}^3$ of norm 1. Note that, for each i, we have

$$\operatorname{dist}(\alpha, \gamma_i) = \max\{|L_i(\boldsymbol{\alpha})|, |L_i'(\boldsymbol{\alpha})|, |L_i''(\boldsymbol{\alpha})|\}$$

where

$$\begin{aligned} L_i &= \|\boldsymbol{\gamma}_i\|^{-1}((\xi + ir)X_0 - X_1), \\ L_i' &= \|\boldsymbol{\gamma}_i\|^{-1}(\eta s^i X_0 - X_2), \\ L_i'' &= \|\boldsymbol{\gamma}_i\|^{-1}(\eta s^i X_1 - (\xi + ir)X_2). \end{aligned}$$

Let $M_i \in \{L_i, L_i'', L_i'''\}$ such that $\operatorname{dist}(\alpha, \gamma_i) = M_i(\boldsymbol{\alpha})$. Then we have $\|M_i\| \leq 1$ and $M_i(\boldsymbol{\gamma}_i) = 0$. We conclude that the polynomial

$$Q = \prod_{i=0}^{T-1} M_i$$

belongs to $I_T^{(T)}$ and has length $\mathcal{L}(Q) \leq 2^T$. Applying Corollary 1.6.3, we get

$$\prod_{i=0}^{T-1} \operatorname{dist}(\alpha, \gamma_i) = |Q(\boldsymbol{\alpha})| \leq \mathcal{L}(Q)|I_T^{(T)}|_\alpha \leq \begin{cases} c^{T^3} c_1^{2T} T^{2T} 6^T \cdot |I_D^{(T)}|_\alpha & \text{if } |s| < 1, \\ c^{T^2} c_1^{2T^2} 6^T \cdot |I_D^{(T)}|_\alpha & \text{if } |s| > 1. \end{cases}$$

By Lemma 1.7.1 (ii), we also have

$$\prod_{i=0}^{T-1} \operatorname{dist}(\alpha, \gamma_i) \geq (4C_T^2)^{1-T} \cdot |r|^{T-1} \cdot \operatorname{dist}(\alpha, \mathcal{S}_T).$$

Hence

$$\operatorname{dist}(\alpha, \mathcal{S}_T) \leq \begin{cases} c^{T^3} c_1^{2T} T^{2T} 6^{2T} C_T^{2(T-1)} \cdot |r|^{1-T} \cdot |I_D^{(T)}|_\alpha & \text{if } |s| < 1, \\ c^{T^2} c_1^{2T^2} 6^{2T} C_T^{2(T-1)} \cdot |r|^{1-T} \cdot |I_D^{(T)}|_\alpha & \text{if } |s| > 1. \end{cases}$$

So there exists a constant $c_2 > 1$ which depends only on r, s, ξ, η and satisfies (1.19).

□

Proposition 1.7.3. *Let $\mu, \alpha \in \mathbb{P}^2(\mathbb{C})$ with representatives $\boldsymbol{\mu}, \boldsymbol{\alpha}$ of norm 1 and let $P \in \mathbb{C}[\mathbf{X}]_D$. Then*

$$|P(\boldsymbol{\alpha})| \leq |P(\boldsymbol{\mu})| + D\mathcal{L}(P) \operatorname{dist}(\alpha, \mu).$$

Proof. Without loss of generality, we can assume that $\boldsymbol{\mu} = (1, \mu_1, \mu_2)$. Write $P(\mathbf{X}) = \sum_{i+j\le D} c_{i,j} X_0^{D-i-j} X_1^i X_2^j$. Then

$$\begin{aligned} P(\boldsymbol{\alpha}) - \alpha_0^D P(\boldsymbol{\mu}) &= \sum_{i+j\le D} c_{i,j}(\alpha_0^{D-i-j}\alpha_1^i\alpha_2^j - \alpha_0^D\mu_1^i\mu_2^j) \\ &= \sum_{i+j\le D} c_{i,j}\left(\sum_{t=1}^{i}(\alpha_1 - \alpha_0\mu_1)\alpha_0^{D-i-j+t-1}\alpha_1^{i-t}\alpha_2^j\mu_1^{t-1}\right. \\ &\qquad \left. + \sum_{t=1}^{j}(\alpha_2 - \alpha_0\mu_2)\alpha_0^{D-j+t-1}\alpha_2^{j-t}\mu_1^i\mu_2^{t-1}\right) \end{aligned}$$

So

$$|P(\boldsymbol{\alpha})| \le |\alpha_0^D P(\boldsymbol{\mu})| + \sum_{i+j\le D} |c_{i,j}| D \operatorname{dist}(\alpha, \mu) \le |P(\boldsymbol{\mu})| + D\mathcal{L}(P)\operatorname{dist}(\alpha,\mu).$$

□

Recall that the map $\bar{\tau} : \mathbb{C}^3 \longrightarrow \mathbb{C}^3$ sends (x, y, z) to $(x, y + rx, sz)$ and induces $\tau : \mathbb{P}^2(\mathbb{C}) \longrightarrow \mathbb{P}^2(\mathbb{C})$.

Lemma 1.7.4. *Let α, γ be points of $\mathbb{P}^2(\mathbb{C})$ and t be an integer. Then there exists a constant c_3 which depends only on s and $\mathbb{C}[\mathbf{X}]$ such that*

$$|\log \operatorname{dist}(\tau^t(\alpha), \tau^t(\gamma)) - \log \operatorname{dist}(\alpha, \gamma)| \le c_3|t|. \tag{1.18}$$

Proof. Let $\boldsymbol{\alpha} = (\alpha_0, \alpha_1, \alpha_2)$ and $\boldsymbol{\gamma} = (\gamma_0, \gamma_1, \gamma_2)$ be representatives of α and γ in $\mathbb{C}^3$ of norm 1. We may assume that one of the coordinates of $\boldsymbol{\alpha}$ is 1. We have

$$\operatorname{dist}(\alpha, \gamma) = \max\{|\alpha_1\gamma_0 - \alpha_0\gamma_1|, |\alpha_2\gamma_0 - \alpha_0\gamma_2|, |\alpha_1\gamma_2 - \alpha_2\gamma_1|\}$$

and

$$\operatorname{dist}(\tau^t(\alpha), \tau^t(\gamma)) = \frac{\|\bar{\tau}^t(\boldsymbol{\alpha}) \wedge \bar{\tau}^t(\boldsymbol{\gamma})\|}{\|\bar{\tau}^t(\boldsymbol{\alpha})\| \cdot \|\bar{\tau}^t(\boldsymbol{\gamma})\|}$$

where $\bar{\tau}^t(\boldsymbol{\alpha}) = (\alpha_0, \alpha_1 + t\alpha_0, s^t\alpha_2)$ and $\bar{\tau}^t(\boldsymbol{\gamma}) = (\gamma_0, \gamma_1 + t\gamma_0, s^t\gamma_2)$. We find that

$$\begin{aligned} \|\bar{\tau}^t(\boldsymbol{\alpha}) \wedge \bar{\tau}^t(\boldsymbol{\gamma})\| = \max\big\{&|\alpha_1\gamma_0 - \alpha_0\gamma_1|, |(\alpha_2\gamma_0 - \alpha_0\gamma_2)s^t|, \\ &|(\alpha_1 + tr\alpha_0)\gamma_2 - \alpha_2(\gamma_1 + tr\gamma_0)| \cdot |s|^t\big\}. \end{aligned}$$

Since

$$|(\alpha_1 + tr\alpha_0)\gamma_2 - \alpha_2(\gamma_1 + tr\gamma_0)| \leq |(\alpha_2\gamma_1 - \alpha_1\gamma_2)| + |tr(\alpha_2\gamma_0 - \alpha_0\gamma_2)|,$$

we deduce that

$$\mathrm{dist}(\tau^t(\alpha), \tau^t(\gamma)) \leq \left(1 + (|tr| + 1)|s|^t\right) \frac{\mathrm{dist}(\alpha, \gamma)}{\|\bar{\tau}^t(\boldsymbol{\alpha})\| \cdot \|\bar{\tau}^t(\boldsymbol{\gamma})\|}. \tag{1.19}$$

Note that

$$\begin{aligned} \max\{|\alpha_0|, |1 + tr\alpha_0|\} &\geq \frac{(|tr| + 1) \cdot \max\{|\alpha_0|, 1 - |tr\alpha_0|\}}{|tr| + 1}, \\ &= \frac{\max\{|\alpha_0|(|tr| + 1), 1 + |tr|(1 - |\alpha_0|(|tr| + 1))\}}{|tr| + 1} \\ &\geq \frac{1}{|tr| + 1}. \end{aligned}$$

Since one of the coordinates of $(\alpha_0, \alpha_1, \alpha_2)$ is equal to 1, as we assumed before, then we find that

$$\begin{aligned} \|\bar{\tau}^t(\boldsymbol{\alpha})\| &= \max\{|\alpha_0|, |\alpha_1 + tr\alpha_0|, |s^t\alpha_2|\} \\ &\geq \begin{cases} |\alpha_0| = 1 & \text{if } \alpha_0 = 1, \\ \max\{|\alpha_0|, |1 + tr\alpha_0|\} & \text{if } \alpha_1 = 1, \\ |s^t| & \text{if } \alpha_2 = 1, \end{cases} \\ &\geq \min\{|s^t|, (|tr| + 1)^{-1}\}. \end{aligned}$$

and so

$$\frac{1}{\|\bar{\tau}^t(\boldsymbol{\alpha})\|} \leq \max\{|s^{-t}|, |tr| + 1\}.$$

Similarly,

$$\frac{1}{\|\bar{\tau}^t(\boldsymbol{\gamma})\|} \leq \max\{|s^{-t}|, |tr| + 1\}.$$

From (1.19), this yields the existence of c_3 which only depends on $|s|$ and $|r|$ satisfying (1.18). $\square$

1.8 Construction of $\mathbb{Q}$-subvarieties of dimension 0

In this section, we define a general convex body $\mathcal{C}$ of $\mathbb{C}[\mathbf{X}]_D$ which is adapted to our problem. Then, we construct a $\mathbb{Q}$-subvariety Z of $\mathbb{P}^2(\mathbb{C})$ of dimension 0 and provide estimates for $h_{\mathcal{C}}(Z), \deg(Z), h(Z)$ (in this order).

We first recall the following result.

Theorem 1.8.1. *[19, Theorem 5.6] Let Σ be a non-empty finite subset of $\mathcal{G} = \mathbb{C} \times \mathbb{C}^*$ and let S be a positive integer. Denote by I the ideal of $\mathbb{C}[\mathbf{X}]$ generated by the homogeneous polynomials P satisfying*

$$\mathcal{D}^i P(1,\gamma) = 0 \quad \textit{for each } \gamma \in \Sigma \textit{ and each } i = 0, \dots, S-1. \tag{1.20}$$

Suppose that there exists a finite subset Σ_1 of $\mathcal{G}$ and an integer $S_1 \geq 0$ such that

$$D < (S_1 + 1) \min\{|\pi_1(\Sigma_1)|, |\pi_2(\Sigma_1)|\}, \tag{1.21}$$

$$(S + S_1)|\Sigma + \Sigma_1| < \binom{D+2}{2}, \tag{1.22}$$

where $\Sigma + \Sigma_1 = \{\gamma + \gamma_1;\ \gamma \in \Sigma, \gamma_1 \in \Sigma_1\}$ denotes the sumset of Σ and Σ_1 in $\mathcal{G}$. Then, the resultant in degree D viewed as a polynomial map

$$\mathrm{Res}_D : \quad \mathbb{C}[\mathbf{X}]_D^3 \longrightarrow \mathbb{C}$$

vanishes up to order $S|\Sigma|$ at each point of $(I_D)^3$.

Here, $\pi_1 : \mathcal{G} \to \mathbb{C}$ and $\pi_2 : \mathcal{G} \to \mathbb{C}^*$ are the projections from $\mathcal{G}$ to its first and second coordinates.

Let T and D be positive integers. Set

$$\Sigma = \{(\xi + ir, \eta s^i);\ 0 \leq i < T\}, \quad \Sigma_1 = \{(\xi + ir, \eta s^i);\ 0 \leq i \leq D\}$$

and set $S = 1,\ S_1 = 0$. Note that if $T \leq \binom{D+1}{2}$, then the condition (1.21) and (1.22) are satisfied because $|\pi_1(\Sigma_1)| = |\pi_2(\Sigma_1)| = D + 1$ and $|\Sigma + \Sigma_1| = T + D$. Moreover, by definition, $I^{(T)}$ is the ideal of $\mathbb{C}[\mathbf{X}]$ generated by all the homogeneous polynomials vanishing at all points $(1, \gamma)$ with $\gamma \in \Sigma$. Therefore, the above theorem has the following consequence.

Lemma 1.8.2. *Let T and D be positive integers such that $T \leq \binom{D+1}{2}$. Then the resultant in degree D viewed as a polynomial map*

$$\mathrm{Res}_D: \quad \mathbb{C}[\mathbf{X}]_D^3 \longrightarrow \mathbb{C}$$

vanishes up to order T at each triple (P, Q, R) of elements of $I_D^{(T)}$.

We now introduce the convex body $\mathcal{C}$ that is relevant to our problem and estimate the corresponding height of $\mathbb{P}^2(\mathbb{C})$. Recall that, for any convex body $\mathcal{C}$ of $\mathbb{C}[\mathbf{X}]_D$, the height of $\mathbb{P}^2(\mathbb{C})$ relative to $\mathcal{C}$ is

$$h_{\mathcal{C}}(\mathbb{P}^2(\mathbb{C})) = h_{\mathcal{C}}(\mathrm{Res}_D) = \log \|\mathrm{Res}_D\|_{\mathcal{C}} \tag{1.23}$$

where $\|\mathrm{Res}_D\|_{\mathcal{C}} = \sup\{\mathrm{Res}_D(P_0, P_1, P_2);\ P_0, P_1, P_2 \in \mathcal{C}\}$.

Proposition 1.8.3. *Let D, T be positive integers with $T \leq \binom{D+1}{2}$ and let Y, U be positive real numbers such that*

$$Y \geq \begin{cases} 2T \log c & \text{if } |s| > 1 \\ 3T^{3/2} \log c & \text{if } |s| < 1 \end{cases}$$

with c as in Lemma 1.5.1. Then, for the choice of convex body

$$\mathcal{C} = \{P \in \mathbb{C}[\mathbf{X}]_D; \|P\| \leq e^Y, \max_{0 \leq i < T} |P(\boldsymbol{\gamma}_i)| < e^{-U}\},$$

we have

$$h_{\mathcal{C}}(\mathbb{P}^2(\mathbb{C})) \leq -TU + 3YD^2 + 21\ \log(3)D^3.$$

Proof. By Lemma 1.2.7, we get

$$h_{\mathcal{B}}(\mathrm{Res}_D) = h_{\mathcal{B}}(\mathbb{P}^2(\mathbb{C})) \leq 18 \log(3) D^3 \tag{1.24}$$

where $\mathcal{B}$ is the unit convex body of $\mathbb{C}[\mathbf{X}]_D$.

As $\mathcal{C}$ is compact, there exist $P_0, P_1, P_2 \in \mathcal{C}$ such that $\|\mathrm{Res}_D\|_{\mathcal{C}} = |\mathrm{Res}_D(P_0, P_1, P_2)|$ and so, by (1.23), we have

$$h_{\mathcal{C}}(\mathbb{P}^2(\mathbb{C})) = \log |\mathrm{Res}_D(P_0, P_1, P_2)|.$$

Let L denote the smallest non-negative integer such that $T \leq \binom{L+2}{2}$. Since $T \leq \binom{D+1}{2}$, we have $L < D$. Moreover, we have $L^2 < 2\binom{L+1}{2} < 2T$, so $L^3 < 3T^{3/2}$. Set $M = \binom{L+2}{2}$. For each $j = 0, 1, 2$, Lemma 1.5.1 ensures the existence of a unique polynomial $Q_j \in \mathbb{C}[\mathbf{X}]_L$ such that

$$Q_j(\boldsymbol{\gamma}_i) = \begin{cases} P_j(\boldsymbol{\gamma}_i) & \text{if} \quad 0 \leq i < T \\ 0 & \text{if} \quad T \leq i < M \end{cases}$$

and

$$\begin{aligned} \|Q_j\| \leq \mathcal{L}(Q_j) &\leq \begin{cases} c^{L^2} \cdot \max_{0 \leq i < M} |Q_j(\boldsymbol{\gamma}_i)| & \text{if } |s| > 1 \\ c^{L^3} \cdot \max_{0 \leq i < M} |Q_j(\boldsymbol{\gamma}_i)| & \text{if } |s| < 1 \end{cases} \\ &\leq \begin{cases} c^{2T} e^{-U} & \text{if } |s| > 1 \\ c^{3T^{3/2}} e^{-U} & \text{if } |s| < 1 \end{cases} \\ &\leq e^{Y-U}. \end{aligned}$$

We also have $P_j - X_0^{D-L} Q_j \in \mathbb{C}[\mathbf{X}]_D$, and $(P_j - X_0^{D-L} Q_j)(\boldsymbol{\gamma}_i) = 0$ for $0 \leq i < T$. Hence $P_j - X_0^{D-L} Q_j \in I_D^{(T)}$. According to Lemma 1.8.2, the polynomial

$$f(z) = \mathrm{Res}_D(P_0 - (1-z)X_0^{D-L}Q_0, \ldots, P_2 - (1-z)X_0^{D-L}Q_2) \in \mathbb{C}[z]$$

vanishes up to order at least T at $z = 0$. Then we can write $f(z) = z^T g(z)$ for some $g(z) \in \mathbb{C}[z]$. Using the Maximum Modulus Principle, we find that

$$|f(1)| = |g(1)| \leq \|g\|_R \leq R^{-T} \|f\|_R$$

for any $R \geq 1$. Choosing $R = e^U$, we get

$$\exp(h_{\mathcal{C}}(\mathrm{Res}_D)) = |\mathrm{Res}_D(P_0, P_1, P_2)| = |f(1)| \leq e^{-TU} \|f\|_{e^U}. \tag{1.25}$$

Note that, since $\|Q_j\| \leq e^{Y-U}$, for any $|z| \leq e^U$, we get

$$\|P_j - (1-z)X_0^{D-L}Q_j\| \leq \|P_j\| + (1+e^U)\|Q_j\| \leq 3e^Y.$$

Therefore, we have

$$\begin{aligned}
&\|f\|_{e^U} = \sup\{|f(z)|; |z| \le e^U\} \\
&\le \sup\left\{|\mathrm{Res}_D(R_0, R_1, R_2)|; R_j \in \mathbb{C}[\mathbf{X}]_D, \|R_j\| \le 3e^Y, 0 \le j \le 2\right\} \\
&\le (3e^Y)^{3D^2} \sup\{|\mathrm{Res}_D(R_0, R_1, R_2)|; R_j \in \mathbb{C}[\mathbf{X}]_D, \|R_j\| \le 1,\ 0 \le j \le 2\} \\
&= (3e^Y)^{3D^2} \exp(h_{\mathcal{B}}(\mathrm{Res}_D)). \qquad (1.26)
\end{aligned}$$

where the penultimate inequality follows from the fact that Res_D is homogeneous of total degree $3D^2$. Combining inequalities (1.24), (1.25) and (1.26), we get

$$\begin{aligned}
\exp(h_{\mathcal{C}}(Res_D)) &\le e^{-TU}(3e^Y)^{3D^2} \exp(h_{\mathcal{B}}(Res_D)) \\
&\le e^{-TU}(3e^Y)^{3D^2} 3^{18D^3} \\
&\le \exp(-TU + 3YD^2 + 21\ \log(3)D^3).
\end{aligned}$$

□

Recall that

$$\begin{aligned}
\Phi: \quad \mathbb{C}[\mathbf{X}] &\longrightarrow \mathbb{C}[\mathbf{X}] \\
P(X_0, X_1, X_2) &\longmapsto P(X_0, X_1 + rX_0, sX_2)
\end{aligned}$$

is a $\mathbb{C}-$algebra isomorphism which preserves homogeneity and degree of polynomials of $\mathbb{C}[\mathbf{X}]$.

The construction of Z needs the two following results.

Lemma 1.8.4. *Let $D \in \mathbb{N}$, let $i \in \mathbb{Z}$ and let $P \in \mathbb{Q}[\mathbf{X}]_D$ be irreducible in $\mathbb{Q}[\mathbf{X}]$. Then $\Phi^i(P)$ is also irreducible in $\mathbb{Q}[\mathbf{X}]$. Moreover, if $i \neq 0$, then P divides $\Phi^i(P)$ if and only if P is a constant multiple of either X_0 or X_2.*

Proof. Fix $i \in \mathbb{Z}$. Let $P \in \mathbb{Q}[\mathbf{X}]_D$ be irreducible in $\mathbb{Q}[\mathbf{X}]$. Since Φ^i is a $\mathbb{Q}-$algebra isomorphism, it preserves irreducibility. So $\Phi^i(P)$ is irreducible in $\mathbb{Q}[\mathbf{X}]$.

Now, suppose that $i \neq 0$, we will prove the last statement.

Assume that P divides $\Phi^i(P)$. We will show that P is a constant multiple of either X_0 or X_2. The converse is obvious.

Since P is irreducible, it is enough to prove that P is divisible by either X_0 or X_2. To this end, we assume that P is not divisible by X_0 and show that P is divisible by X_2.

Since $\deg P = \deg \Phi^i(P)$ and $P|\Phi^i(P)$, there exists a constant $c \in \mathbb{Q}$ such that $P = c\,\Phi^i(P)$, *i.e.*

$$P(X_0, X_1, X_2) = cP(X_0, X_1 + irX_0, s^i X_2). \tag{1.27}$$

Write $P(X_0, X_1, X_2) = \sum_{j+k\le D} c_{jk}\, X_0^{D-j-k} X_1^j X_2^k$ with $c_{jk} \in \mathbb{Q}$. Substituting $X_0 = 0$ into (1.27), we obtain

$$\sum_{j+k=D} c_{jk}\, X_1^j X_2^k = c \sum_{j+k=D} c_{jk}\, X_1^j (s^i X_2)^k = c \sum_{j+k=D} c_{jk}\, s^{ik} X_1^j X_2^k. \tag{1.28}$$

So $c_{jk} = c\, c_{jk}\, s^{ik}$ for each $(j,k) \in \mathbb{N}^2$ with $j + k = D$. As X_0 does not divide P, there exists a pair (j,k) with $j+k = D$ such that $c_{jk} \neq 0$. Since $s \neq \pm 1$, we deduce that there exists a unique $(j_0, k_0) \in \mathbb{N}^2$ with $j_0 + k_0 = D$ such that $c_{j_0k_0} \neq 0$ and, for this choice of (j_0, k_0), we have $c = s^{-ik_0}$. Now we have

$$P(X_0, X_1, X_2) = \sum_{j+k<D} c_{jk} X_0^{D-j-k} X_1^j X_2^k + c_{D-k_0,k_0} X_1^{D-k_0} X_2^{k_0} \tag{1.29}$$

In the case where $k_0 \neq 0$, substituting $X_2 = 0$ into (1.27) and using (1.29), we find

$$\sum_{0\le j<D} c_{j0} X_0^{D-j} X_1^j = c \sum_{0\le j<D} c_{j0} X_0^{D-j} (X_1 + irX_0)^j$$

Suppose that there exists an integer j with $0 \le j < D$ such that $c_{j0} \neq 0$ and let j' be the largest one. We deduce that

$$c_{j'0} X_0^{D-j'} X_1^{j'} = c\, c_{j'0} X_0^{D-j'} X_1^{j'},$$

so $c_{j'0} = c\, c_{j'0}$. Since $c = s^{-ik_0} \neq 1$, this is a contradiction. We conclude that $c_{j0} = 0$ for all $j < D$. Thus X_2 divides P.

In the case where $k_0 = 0$, we have $c = 1$ and $c_{D,0} \neq 0$. Replacing X_2 by 0 into (1.27) and using (1.29), we get

$$\sum_{0\le j<D} c_{j0} X_0^{D-j} X_1^j + c_{D0} X_1^D = \sum_{0\le j<D} c_{j0} X_0^{D-j} (X_1 + irX_0)^j + c_{D0}(X_1 + irX_0)^D$$

Then

$$c_{D-1,0}X_0X_1^{D-1} = c_{D-1,0}X_0X_1^{D-1} + c_{D0}DirX_0X_1^{D-1}.$$

Since $c_{D0} \neq 0$, this is a contradiction. □

Lemma 1.8.5. *Let D be a positive integer and let $P \in \mathbb{Q}[\mathbf{X}]_D$ with $X_0 \nmid P$ and $X_2 \nmid P$. Then the polynomials $P, \Phi(P), \ldots, \Phi^D(P)$ have no common irreducible factor in $\mathbb{Q}[\mathbf{X}]$. Moreover, there exist $a_1, \ldots, a_D \in \mathbb{Z}$ in the range $0 \leq a_i \leq D$ which are not all 0 and for which*

$$Q = \sum_{i=1}^{D} a_i \Phi^i(P)$$

is relatively prime to P.

Proof. Write $P = P_1^{e_1} \cdots P_k^{e_k}$ as a product of irreducible factors in $\mathbb{Q}[\mathbf{X}]$. Then $\Phi^i(P) = \Phi^i(P_1)^{e_1} \cdots \Phi^i(P_k)^{e_k}$ is also a decomposition of $\Phi^i(P)$ into irreducible factors.

Suppose that $P, \Phi(P), \ldots, \Phi^D(P)$ have a common irreducible factor, say P_1. Then for each $i \in \{0, \ldots, D\}$, there exists $j_i \in \{1, \ldots, k\}$ such that P_1 and $\Phi^i(P_{j_i})$ are constant multiples of each other. Since $D \geq k$, then there exist two distinct indices $i_1, i_2 \in \{0, \ldots, D\}$ such that $j_{i_1} = j_{i_2} =: j'$. So both $\Phi^{i_1}(P_{j'}) = \Phi^{i_1-i_2}(\Phi^{i_2}(P_{j'}))$ and $\Phi^{i_2}(P_{j'})$ are constant multiples of P_1, this mean that they divide each other. Lemma 1.8.4 implies that $\Phi^{i_2}(P_{j'})$ is a constant multiple of either X_0 or X_2. So P_1 is also a constant multiple of either X_0 or X_2. This is a contradiction since $X_0 \nmid P$ and $X_2 \nmid P$. We deduce that $P, \Phi(P), \ldots, \Phi^D(P)$ have no common irreducible factor in $\mathbb{Q}[\mathbf{X}]$.

To prove the last statement, we fix $\xi_1, \xi_2 \in \mathbb{C}$ which are algebraically independent over $\mathbb{Q}$ and consider the canonical maps

$$\begin{aligned} \varphi_i :\ \mathbb{Q}[\mathbf{X}] &\longrightarrow \mathbb{Q}[\mathbf{X}]/\langle P_i \rangle \\ Q &\longmapsto \overline{Q} := Q + \langle P_i \rangle \end{aligned}$$

for $i = 1, \ldots, k$. By Normalization Theory, for each i, there exist $Y_i, Y_i' \in \mathbb{Q}[\mathbf{X}]$ algebraically independent over $\mathbb{Q}(P_i)$ such that $\mathbb{Q}[\mathbf{X}]/\langle P_i \rangle$ is integral over $\mathbb{Q}\left[\overline{Y}_i, \overline{Y_i'}\right]$. Since $\xi_1, \xi_2 \in \mathbb{C}$ are algebraically independent over $\mathbb{Q}$, for each i, there exists an embedding $\tilde{\varphi}_i$ of $\mathbb{Q}\left[\overline{Y}_i, \overline{Y_i'}\right]$ into $\mathbb{C}$ which sends $\overline{Y_i}$ to ξ_1 and sends $\overline{Y_i'}$ to ξ_2. Since $\mathbb{Q}[\mathbf{X}]/\langle P_i\rangle$ is integral over $\mathbb{Q}\left[\overline{Y}_i, \overline{Y_i'}\right]$, there exists an embedding $\overline{\varphi_i}$ of $\mathbb{Q}[\mathbf{X}]/\langle P_i\rangle$ into $\mathbb{C}$ which extends the embedding $\tilde{\varphi}_i$.

Let $U_1, \ldots, U_D$ be indeterminates over $\mathbb{C}$. Set

$$R(U_1, \ldots, U_D) = \prod_{i=1}^{k} \left(\sum_{j=1}^{D} U_j \, \overline{\varphi_i} \left(\varphi_i \left(\Phi^j(P) \right) \right) \right).$$

Then $R(U_1, \ldots, U_D)$ is a homogeneous polynomial in $U_1, \ldots, U_D$ of degree k with coefficients in $\mathbb{C}$. We claim that $R(U_1, \ldots, U_D) \neq 0$. Otherwise, there exists i with $1 \leq i \leq k$ such that

$$\sum_{j=1}^{D} U_j \, \overline{\varphi_i} \left(\varphi_i \left(\Phi^j(P) \right) \right) = 0.$$

This implies that $\overline{\varphi_i}\left(\varphi_i\left(\Phi^j(P)\right)\right) = 0$ for all $j = 1, \ldots, D$. Thus, $\varphi_i\left(\Phi^j(P)\right) = 0$, i.e., $P_i \mid \Phi^j(P)$ for all $j = 1, \ldots, D$, which is impossible since $P, \Phi(P), \ldots, \Phi^D(P)$ have no common factor.

Since $R(U_1, \ldots, U_D)$ is a non-zero homogeneous polynomial in $U_1, \ldots, U_D$ of degree k, there exist integers $a_1, \ldots, a_D \in \{0, 1, \ldots, k\}$ such that

$$R(a_1, a_2, \ldots, a_D) \neq 0.$$

Hence, for each $i = 1, \ldots, k$, we get

$$\overline{\varphi_i} \left(\varphi_i \left(\sum_{j=1}^{D} a_j \, \Phi^j(P) \right) \right) = \sum_{j=1}^{D} a_j \, \overline{\varphi_i} \left(\varphi_i \left(\Phi^j(P) \right) \right) \neq 0.$$

This means that $\varphi_i\left(\sum_{j=1}^{D} a_j \, \Phi^j(P)\right) \neq 0$ for all $i = 1, \ldots, k$. So $\sum_{j=1}^{D} a_j \, \Phi^j(P)$ is relatively prime to P. Note that $k \leq \deg(P) = D$ so $a_1, \ldots, a_D \leq D$ as required. □

Let c' be the smallest positive integer such that $c'r, c's \in \mathbb{Z}$. Then, for any polynomial $P \in \mathbb{Z}[\mathbf{X}]_D$, we have $c'^{iD}\Phi^i(P) \in \mathbb{Z}[\mathbf{X}]_D$ for all $i \in \mathbb{N}$. In the proof of the main result, we use the following proposition to construct a $\mathbb{Q}$-subvariety of dimension 0 of small height relative to an appropriate convex body.

Proposition 1.8.6. *Let D, T, Y, U and $\mathcal{C}$ be as in Proposition 1.8.3 and set $A = TU/(D^2Y)$. Suppose that*

$$5 \le A, \quad D < 2T, \quad 25\log(3)D \le Y.$$

Suppose that there exists a non-zero polynomial $P \in \mathbb{Z}[\mathbf{X}]_D \cap \mathcal{C}$ such that $X_0 \nmid P$, $X_2 \nmid P$ and $c'^{iD}\Phi^i(P) \in \mathcal{C}$ for all $i = 1, \dots, 2T-1$.

Then there exists a $\mathbb{Q}$-subvariety $Z \subset \mathcal{Z}(\Phi^i(P); 0 \le i < 2T)$ of dimension 0 with

$$h_{\mathcal{C}}(Z) \le -A'(Dh(Z) + Y \deg Z)$$

where $A' = (A-5)/6$.

Proof. We have $\dim(\mathbb{P}^2(\mathbb{C})) = 2$, $\deg(\mathbb{P}^2(\mathbb{C})) = 1$, $h(\mathbb{P}^2(\mathbb{C})) = 0$ and $P \in \mathbb{Z}[\mathbf{X}]_D \cap \mathcal{C}$. Applying Lemma 1.2.8 with $Z = \mathbb{P}^2(\mathbb{C})$, we deduce that there exists a $\mathbb{Q}$-cycle Z' of $\mathbb{P}^2(\mathbb{C})$ of dimension 1 and degree D with

$$\begin{aligned} h(Z') &\le Y + 42\log(3)D \le 3Y, \\ h_{\mathcal{C}}(Z') &\le h_{\mathcal{C}}(\mathbb{P}^2(\mathbb{C})) + 4\log(3)D^3. \end{aligned}$$

By Proposition 1.8.3, we get

$$\begin{aligned} h_{\mathcal{C}}(Z') &\le -TU + 3D^2Y + 25\log(3)D^3 \\ &\le -(A-4)D^2Y \\ &\le -\frac{A-4}{6}D\big(Dh(Z') + 3Y\deg(Z')\big). \end{aligned}$$

Lemma 1.2.6 ensures the existence of an irreducible component Z_1 of Z' with

$$h_{\mathcal{C}}(Z_1) \le -\frac{A-4}{6}D\big(Dh(Z_1) + 3Y\deg(Z_1)\big).$$

By Lemma 1.8.5, the polynomials $P, \Phi(P), \dots, \Phi^D(P)$ have no common factor. We deduce that there exists $0 \le i \le D$ such that $\Phi^i(P) \notin \mathcal{I}(Z_1)$. Since $c'^{iD}\Phi^i(P) \in \mathcal{C} \cap \mathbb{Z}[\mathbf{X}]_D$, Lemma 1.2.8 implies that there exists a $\mathbb{Q}$-cycle Z'' of dimension 0 and degree $D\deg(Z_1)$ satisfying

$$\begin{aligned} h(Z'') &\le Dh(Z_1) + \deg(Z_1)\log\|c'^{iD}\Phi^i(P)\| + 24\log(3)D\deg(Z_1) \\ &\le Dh(Z_1) + 2Y\deg(Z_1), \end{aligned}$$

and

$$\begin{aligned}
h_{\mathcal{C}}(Z'') &\leq h_{\mathcal{C}}(Z_1) + 2\log(3)D^2\deg(Z_1) \\
&\leq -\frac{A-4}{6}\,D\big(Dh(Z_1) + 3Y\deg(Z_1)\big) + \frac{2}{25}DY\deg(Z_1) \\
&= -\frac{A-4}{6}\,D\big(Dh(Z_1) + 2Y\deg(Z_1)\big) - \left(\frac{A-4}{6} - \frac{2}{25}\right)DY\deg(Z_1) \\
&\leq -\frac{A-5}{6}\,(Dh(Z'') + Y\deg(Z'')).
\end{aligned}$$

Similarly, by linearity of degree and height, we deduce that there exists a subvariety $Z \subset Z''$ such that

$$h_{\mathcal{C}}(Z) \leq -\frac{A-5}{6}\,(Dh(Z) + Y\deg(Z)).$$

So $h_{\mathcal{C}}(Z) < 0$. From Lemma 1.2.8, we deduce that

$$I(Z) \supset (\mathcal{C} \cap \mathbb{Z}[\mathbf{X}]_D) \supset \{c'^{jD}\phi^j(P);\ 0 \leq j < 2T\}.$$

Therefore, $Z \subset \mathcal{Z}(\phi^j(P);\ 0 \leq j < 2T)$. □

In the proof of our main result, we need to consider translates of a $\mathbb{Q}$-subvariety of dimension 0 and we need to estimate their heights. The next proposition fulfills this purpose.

Proposition 1.8.7. *Let Z be a $\mathbb{Q}$-subvariety of $\mathbb{P}^2(\mathbb{C})$ of dimension 0 with $Z \not\subseteq \mathcal{Z}(X_0)$ and let t be an integer. Then*

$$|h(\tau^t(Z)) - h(Z)| \ll |t|\deg(Z)$$

where the constant involved in the symbol $\ll$ depends only on r, s.

Proof. Let F and G be Chow forms of Z and $\tau^t(Z)$ in degree 1. Since $Z \not\subseteq \mathcal{Z}(X_0)$, the variety Z contains a point $\alpha \in \mathbb{P}^2(\mathbb{C})$ with representative $(1, \alpha_1, \alpha_2) \in \overline{\mathbb{Q}}^3$. As Z is a $\mathbb{Q}$-subvariety of dimension 0, we have

$$Z = \{(1 : \sigma(\alpha_1) : \sigma(\alpha_2));\ \sigma \in \mathfrak{G}\}$$

where $\mathfrak{G}$ is the set of all embeddings of $\mathbb{Q}(\alpha_1, \alpha_2)$ into $\mathbb{C}$ (see the preliminaries in Section 1.2). By definition of τ, this implies that

$$\tau^t(Z) = \{(1 : \sigma(\alpha_1 + tr) : \sigma(s^t\alpha_2));\ \sigma \in \mathfrak{G}\}.$$

Therefore, we have

$$F(\mathbf{X}) = a \prod_{\sigma\in\mathfrak{G}} (X_0 + \sigma(\alpha_1)X_1 + \sigma(\alpha_2)X_2),$$
$$G(\mathbf{X}) = b \prod_{\sigma\in\mathfrak{G}} (X_0 + (\sigma(\alpha_1) + tr)X_1 + s^t\sigma(\alpha_2)X_2),$$

where $|a|$ and $|b|$ are the smallest positive integers such that the above products belong to $\mathbb{Z}[\mathbf{X}]$. Let c be a common positive denominator of r, s and s^{-1} and set

$$P(\mathbf{X}) = F(c^{|t|}(X_0 + trX_1), c^{|t|}X_1, c^{|t|}s^tX_2).$$

Then P belongs to $\mathbb{Z}[\mathbf{X}]$ and since $\deg F = \deg(Z)$, we get

$$P(\mathbf{X}) = ac^{|t|\deg(Z)} \prod_{\sigma\in\mathfrak{G}} (X_0 + (\sigma(\alpha_1) + tr)X_1 + s^t\sigma(\alpha_2)X_2).$$

So P is a constant multiple of G. Since G is irreducible over $\mathbb{Z}$, we deduce that G divides P in $\mathbb{Z}[\mathbf{X}]$. Therefore, by the definition of P, we obtain

$$\|G\| \le \|P\| \le c^{|t|\deg(Z)}(|s^t| + |tr| + 1)^{\deg(Z)}\|F\| \le (c(|s| + |r| + 1))^{|t|\deg(Z)}\|F\|.$$

Since $h(Z) = \log\|F\|$ and $h(\tau^t(Z)) = \log\|G\|$, this implies that

$$h(\tau^t(Z)) \le h(Z) + c'|t|\deg(Z)$$

where $c' = \log(c(|s| + |r| + 1))$. Since $Z = \tau^{-t}(\tau^t(Z))$ and $\deg(Z) = \deg(\tau(Z))$, this result applied with Z replaced by $\tau^t(Z)$ and t replaced by $-t$ implies in turn that

$$h(Z) = h(\tau^{-t}(\tau^t(Z))) \le h(\tau^t(Z)) + c'|t|\deg(Z).$$

The conclusion follows. □

The last proposition provides upper bound estimates for the degree and the height of $\mathbb{Q}$-varieties of dimension 0 contained in the zero set of families of polynomials of the form $\Phi^i(P)$ with $P \in \mathbb{Z}[\mathbf{X}]_D$ fixed.

Proposition 1.8.8. *Let $D, T \in \mathbb{N}^*$. Let $P \in \mathbb{Z}[\mathbf{X}]_D$ with $X_0 \nmid P$ and $X_2 \nmid P$ and let $Y \in \mathbb{R}$. Suppose that*

$$\max\left\{25\log(3)D, \log\|P\|, \log\|c'^{D^2}\Phi(P)\|, \dots, \log\|c'^{D^2}\Phi^D(P)\|\right\} < Y$$

and that $W = \mathcal{Z}(\Phi^i(P); 0 \le i < T + D)$ is not empty. Then W has dimension 0. Moreover, any $\mathbb{Q}$-subvariety Z of $\mathbb{P}^2(\mathbb{C})$ contained in W has dimension 0 with

$$\deg Z \le \frac{D^2}{T} \quad \text{and} \quad \sum_{i=0}^{T-1} h(\tau^i(Z)) \le 3DY.$$

In particular, we have $h(\tau^i(Z)) \ll \dfrac{DY}{T} + D^2$ for each $0 \le i < T$.

Proof. Since $X_0 \nmid P$ and $X_2 \nmid P$, Lemma 1.8.5 implies that there exist integers $a_1, \dots, a_D$ not all 0, with $0 \le a_i \le D$, such that

$$Q = \sum_{i=1}^{D} a_i (c'^{D^2}\Phi^i(P)) \in \mathbb{Z}[\mathbf{X}]$$

is relatively prime to P. Then $\dim \mathcal{Z}(P, Q) = 0$ and $W \subset \mathcal{Z}(P, Q)$. Since $W \neq \emptyset$, we deduce that $\dim W = 0$.

Let $Z \subset W$ be an arbitrary $\mathbb{Q}$-subvariety of $\mathbb{P}^2(\mathbb{C})$, so $\dim Z = 0$ and Z is finite. Then, for each $0 \le i < T$ and for each representative $\mathbf{z}$ in $\mathbb{C}^3$ of a point z of Z, we have

$$\Phi^j(P)(\bar{\tau}^i(\mathbf{z})) = \Phi^{i+j}(P)(\mathbf{z}) = 0$$

when $0 \le j \le D$ since $z \in W = \mathcal{Z}(\Phi^i(P); 0 \le i < T + D)$, and so

$$Q(\bar{\tau}^i(\mathbf{z})) = c'^{D^2} \sum_{j=1}^{D} a_i \Phi^j(P)\left(\bar{\tau}^i(\mathbf{z})\right) = 0.$$

Thus $\tau^i(z) \in \mathcal{Z}(P, Q)$ for all $i < T$. Since Z is irreducible, so is $\tau^i(Z)$ for all $i < T$. The above observation then implies that $Z, \tau(Z), \dots, \tau^{T-1}(Z)$ are disjoint irreducible components of $\mathcal{Z}(P, Q)$. Since they all have dimension 0 as $\mathcal{Z}(P, Q)$, we have

$$\sum_{i=0}^{T-1} \deg(\tau^i(Z)) = \sum_{i=0}^{T-1} \left|\tau^i(Z)\right| \le |\mathcal{Z}(P, Q)| = \deg(\mathcal{Z}(P, Q)) \le D^2 \tag{1.30}$$

where the last inequality follows from Corollary 1.2.5. Since $\deg(Z) = \deg(\tau^i(Z))$ for all i, we deduce that

$$\deg(\tau^i(Z)) = \deg Z \leq \frac{D^2}{T}. \tag{1.31}$$

Now we will prove that $\sum_{i=0}^{T-1} h(\tau^i(Z)) \leq 3DY$.

Consider the polynomial map

$$\begin{aligned} F: \ \mathbb{C}[\mathbf{X}]_D &\longrightarrow \mathbb{C} \\ L \ &\longmapsto \mathrm{Res}_D(P, Q, L). \end{aligned}$$

Since Res_D is homogeneous of degree D^2 in each of its polynomial arguments, we conclude that the polynomial underlying F is homogeneous of degree D^2.

For each $0 \leq i < T$, denote by F_i a Chow form of the $\mathbb{Q}$-subvariety $\tau^i(Z)$ in degree D (viewed as a polynomial map from $\mathbb{C}[\mathbf{X}]_D$ to $\mathbb{C}$). We have

$$h_{\mathcal{B}}(\tau^i(Z)) = h_{\mathcal{B}}(F_i) = \log \sup\{|F_i(L)|; L \in \mathcal{B}\} \tag{1.32}$$

where $\mathcal{B} = \{R \in \mathbb{C}[\mathbf{X}]_D; \|R\| \leq 1\}$. So, for such i, Lemma 1.2.7 gives

$$\begin{aligned} D\, h(\tau^i(Z)) &\leq 4 \log(3)\, D \deg(\tau^i(Z)) + h_{\mathcal{B}}(\tau^i(Z)) \\ &= 4 \log(3)\, D \deg(Z) + h_{\mathcal{B}}(F_i), \end{aligned} \tag{1.33}$$

using (1.32) and $\deg(\tau^i(Z)) = \deg(Z)$.

Since $\tau^i(Z) \subset \mathcal{Z}(P, Q)$, we get $\mathcal{Z}(F_i) \subset \mathcal{Z}(F)$. So $F_i | F$ for all $i < T$. Since $Z, \tau(Z), \ldots, \tau^{T-1}(Z)$ are disjoint irreducible varieties, the polynomials $F_0, \ldots, F_{T-1}$ are non-associate irreducible polynomials. Hence $\prod_{i=0}^{T-1} F_i$ divides F as polynomials over $\mathbb{Q}$. Moreover, since F, F_i have coefficients in $\mathbb{Z}$ and F_i is irreducible over $\mathbb{Z}$, we deduce $\prod_{i=0}^{T-1} F_i$ divides F as polynomials over $\mathbb{Z}$. Hence there exists a polynomial G with coefficients in $\mathbb{Z}$ such that $F = G \prod_{i=0}^{T-1} F_i$. Then we have $1 \leq \|G\| \leq \|G\|_{\mathcal{B}}$ and so $h_{\mathcal{B}}(G) \geq 0$. This implies that

$$\begin{aligned} \sum_{i=0}^{T-1} h_{\mathcal{B}}(F_i) &\leq h_{\mathcal{B}}(G) + \sum_{i=0}^{T-1} h_{\mathcal{B}}(F_i) \\ &\leq h_{\mathcal{B}}(F) + 2D^2 \log \binom{D+2}{2} \qquad \text{(by Lemma 1.2.10)} \\ &\leq h_{\mathcal{B}}(F) + 2D^3 \log(3). \end{aligned} \tag{1.34}$$

Since $\mathrm{Res}_D(P,Q,L)$ is homogeneous of degree D^2 in both P and Q and since we have $\|P\| < e^Y$ and $\|Q\| \le \sum_{i=1}^{D} D\|c'^{D^2}\Phi^i(P)\| < D^2 e^Y$, we find that

$$|\mathrm{Res}_D(P,Q,L)| \le \left|\mathrm{Res}_D\left(\frac{P}{\|P\|}, \frac{Q}{\|Q\|}, L\right)\right| (e^Y)^{D^2}(D^2e^Y)^{D^2}$$

for any $L \in \mathbb{C}[\mathbf{X}]_D$. Therefore, we get

$$\begin{aligned} h_{\mathcal{B}}(F) &= \log\sup\{|\mathrm{Res}_D(P,Q,L)|;\ \|L\| \le 1\} \\ &\le \log\sup\left\{\left|\mathrm{Res}_D\left(\frac{P}{\|P\|}, \frac{Q}{\|Q\|}, L\right)\right|; \|L\| \le 1\right\} + 2D^2Y + 2D^2\log D \\ &\le h_{\mathcal{B}}(\mathbb{P}^2) + 2D^2Y + 2D^2 \log D \qquad \text{(since } h_{\mathcal{B}}(\mathbb{P}^2) = \log\|\mathrm{Res}_D\|_{\mathcal{B}}) \\ &\le 18\ \log(3)\, D^3 + 2D^2Y + 2D^2 \log D \qquad \text{(by Lemma 1.2.7)} \\ &\le 19\ \log(3) D^3 + 2D^2Y. \end{aligned} \tag{1.35}$$

Since $\deg(\tau^i(Z)) = \deg(Z)$, it follows from (1.33) that

$$\begin{aligned} D\sum_{i=0}^{T-1} h(\tau^i(Z)) &\le 4\ \log(3)\, D\, T\ \deg Z + \sum_{i=0}^{T-1} h_{\mathcal{B}}(F_i) \\ &\le 4\ \log(3)\, D^3 + (h_{\mathcal{B}}(F) + 2\ \log(3)\, D^3) \qquad \text{(using (1.34))} \\ &\le 25\log(3)D^3 + 2D^2Y \qquad \text{(using (1.35))} \\ &\le 3D^2Y. \end{aligned}$$

So we have $\sum_{i=0}^{T-1} h(\tau^i(Z)) \le 3DY$.

To show the last inequality, we note that, for each index j with $0 \le j < T$, we have

$$\sum_{i=0}^{T-1} h(\tau^i(Z)) = Th(\tau^j(Z)) + \sum_{i=0}^{T-1} \big(h(\tau^i(Z)) - h(\tau^j(Z))\big).$$

This implies that

$$\begin{aligned} |h(\tau^j(Z))| &\le \frac{1}{T}\left(\sum_{i=0}^{T-1} h(\tau^i(Z)) + \sum_{i=0}^{T-1} \big|h(\tau^i(Z)) - h(\tau^j(Z))\big|\right) \\ &\ll \frac{1}{T}\left(3DY + \sum_{i=0}^{T-1} |i-j| \deg(\tau^j(Z))\right) \qquad \text{(by Proposition 1.8.7)} \\ &\ll \frac{DY}{T} + D^2 \qquad \text{(by (1.31)).} \end{aligned}$$

□

1.9 Proof of the main theorem 1.1.5

Proof. Suppose on the contrary that $(1 : \xi : \eta) \notin \mathbb{P}^2(\overline{\mathbb{Q}})$. We will show that this leads to a contradiction.

Fix a positive integer D. In the computations below, we assume that D is sufficiently large so that all the inequalities marked with a star (*i.e.* $\leq^*$ or $\geq^*$) are satisfied.

Step 0. *Reduction to the case where* $|s| > 1$.

Suppose that $|s| < 1$. We set

$$\beta' = \beta + \frac{1}{3}\epsilon\ , \quad \nu' = \nu - \frac{1}{2}\epsilon$$

where $\epsilon = \nu - \max\left\{\beta + 2 - \sigma + \dfrac{(\sigma-1)(2-\sigma)}{\beta - (\sigma - 1)},\ \sigma + 2\right\}$ so that

$$\nu' > \max\left\{\beta' + 2 - \sigma + \frac{(\sigma-1)(2-\sigma)}{\beta - (\sigma - 1)},\ \sigma + 2\right\} \quad \text{and} \quad \beta' > \sigma + 1.$$

Moreover, for each integer D, the polynomial

$$P_D^*(X_1, X_2) = c'^{DT_D^*} P_D(X_1 + T_D^* r, s^{T_D^*} X_2), \quad (\text{with } T_D^* = 3\lfloor D^\sigma \rfloor - 1)$$

belongs to $\mathbb{Z}[X_1, X_2]_{\leq D}$ and satisfies

$$\begin{aligned}\max_{0 \leq i < 3\lfloor D^\sigma \rfloor} \{|P_D^*(\xi + i(-r), \eta(s^{-1})^i)|\} &= \max_{0 \leq i < 3\lfloor D^\sigma \rfloor} \{c'^{DT_D^*} |P_D(\xi + ir, \eta s^i)|\} \\ &\leq c'^{3D^{1+\sigma}} e^{-D^\nu} \\ &\leq^* e^{-D^{\nu'}}\end{aligned}$$

and

$$\begin{aligned}\|P_D^*\| &\leq c'^{DT_D^*} 3^D \|P_D\| (1 + T_D^* |r|)^D && \text{since } |s| < 1 \\ &\leq c'^{3D^{1+\sigma}} 3^D e^{D^\beta} (1 + |r|)^{3D^{1+\sigma}} && \text{since } \|P_D\| \leq e^{D^\beta} \\ &\leq^* e^{D^{\beta'}}.\end{aligned}$$

So if we replace r by $-r$, s by s^{-1}, ν by ν', β by β', and P_D by P_D^*, then all the hypotheses of the theorem still hold. Therefore, it is enough to consider the case where $|s| > 1$. We therefore assume from now on that $|s| > 1$.

Step 1. *Construction of a convex body.*

For each $D \in \mathbb{N}$, we put

$$T_D = \lfloor D^\sigma \rfloor, \quad Y_D = 2D^\beta, \quad U_D = \frac{1}{2}D^\nu$$

and define a convex body of $\mathbb{C}[\mathbf{X}]_D$ by

$$\mathcal{C}_D = \{Q \in \mathbb{C}[\mathbf{X}]_D;\ \|Q\| \le e^{Y_D}, \max_{0 \le i < T_D} |Q(1, \xi + ir, \eta s^i)| \le e^{-U_D}\}.$$

We also denote by $\tilde{P}_D$ the homogeneous polynomial of $\mathbb{Z}[\mathbf{X}]_D$ determined by the condition

$$\tilde{P}_D(1, X_1, X_2) = X_1^{a_D} X_2^{-b_D} P_D(X_1, X_2)$$

where b_D stands for the largest integer b such that X_2^b divides P_D, and where $a_D = D - \deg(P_D) + b_D$. Then, by construction, $\tilde{P}_D$ is not divisible by neither X_0 nor X_2, moreover, $\|\tilde{P}_D\| = \|P_D\|$.

By the definition of c' given just before Proposition 1.8.6, we have

$$c'^{2DT_D} \Phi^j(\tilde{P}_D) \in \mathbb{Z}[\mathbf{X}]_D$$

for any positive integer $j < T_D$. We claim that, *for any sufficiently large D, we have*

$$c'^{2DT_D} \Phi^j(\tilde{P}_D) \in \mathcal{C}_D \cap \mathbb{Z}[\mathbf{X}]_D$$

for all integers j with $0 \le j < 2T_D$. In particular, this means that

$$\Phi^j(\tilde{P}_D) \in \mathcal{C}_D$$

for all integers j with $0 \le j < 2T_D$ since $c' > 1$.

To prove the claim, fix an integer j with $0 \le j < 2T_D$. Since $\beta > \sigma + 1$, we have

$$\begin{aligned}
\|c'^{2DT_D}\Phi^j(\tilde{P}_D)\| &\le c'^{2DT_D}\binom{D+2}{2}\|\tilde{P}_D\| \cdot \max_{t_1+t_2\le D}\{(1+|jr|)^{t_1}|s^j|^{t_2}\} \\
&\le c'^{2D^{\sigma+1}}3^D e^{D^\beta}(1+|jr|+|s|^j)^D \\
&\le 3^D c'^{2D^{\sigma+1}} e^{D^\beta}\,(1+|r|+|s|)^{2D^{\sigma+1}} \\
&\le^* e^{Y_D}.
\end{aligned}$$

Moreover, for each $0 \le i < T_D$, we have

$$\begin{aligned}
&|c'^{2DT_D}\Phi^j\tilde{P}_D(1,\xi+ir,\eta s^i)| \le \left|c'^{2D^{\sigma+1}}\tilde{P}_D\left(1,\xi+(i+j)r,\eta s^{i+j}\right)\right| \\
&= c'^{2D^{\sigma+1}}|\xi+(i+j)r|^{a_D}\cdot|\eta s^{i+j}|^{-b_D}\cdot|P_D(\xi+(i+j)r,\eta s^{i+j})| \\
&\le c'^{2D^{\sigma+1}}(i+j)^D(|\xi|+|r|)^D|\eta|^{-b_D}e^{-D^\nu} \\
&\le^* e^{-\frac{1}{2}D^\nu}
\end{aligned}$$

since $\nu > \sigma + 1$.

Step 2. *Construction of a $\mathbb{Q}$-subvariety of dimension 0.*

Since $\nu > \beta - \sigma + 2$, $1 \le \sigma < 2$, and $\beta > \sigma$, the hypotheses of Proposition 1.8.6 hold for $T = T_D,\ Y = Y_D,\ U = U_D$ and the convex body $\mathcal{C}_D$ for each sufficiently large D. So there exists a $\mathbb{Q}$-subvariety Z_D of $\mathbb{P}^2(\mathbb{C})$ contained in $Z(\Phi^j(\tilde{P}_D);\ 0 \le i < 2T_D)$ with $\dim Z_D = 0$ and

$$h_{\mathcal{C}_D}(Z_D) \le -\frac{1}{25}D^{\nu-\beta+\sigma-2}(2D^\beta\deg(Z_D) + Dh(Z_D)).$$

By Lemma 1.2.9, we get

$$\begin{aligned}
\sum_{\boldsymbol{\alpha}\in\underline{Z}_D}\log\sup\{|Q(\boldsymbol{\alpha})|; Q\in\mathcal{C}_D\} &\le h_{\mathcal{C}_D}(Z_D) - Dh(Z_D) + 9\log(3)D\deg(Z_D) \\
&\le h_{\mathcal{C}_D}(Z_D) + 9\log(3)D\deg(Z_D) \qquad \text{(since } h(Z_D)\ge 0\text{)} \\
&\le -\frac{1}{25}D^{\nu-\beta+\sigma-2}(D^\beta\deg(Z_D) + Dh(Z_D)) \qquad (1.36)
\end{aligned}$$

since $9\log(3)D \le^* (1/25)D^{\nu+\sigma-2}$. For any $\alpha \in \mathbb{P}^2(\mathbb{C})$ with representative $\boldsymbol{\alpha} \in \mathbb{C}^3$ of norm 1, we have

$$\sup\{|Q(\boldsymbol{\alpha})|; Q\in\mathcal{C}_D\} \ge \sup\{|Q(\boldsymbol{\alpha})|; Q\in I_D^{(T_D)},\ \|Q\|\le 1\} = |I_D^{(T_D)}|_\alpha$$

since $I_D^{(T_D)} \subset \mathcal{C}_D$. Proposition 1.7.2 gives

$$|I_D^{(T_D)}|_\alpha \geq c_2^{-T_D^2} \operatorname{dist}(\alpha, S_{T_D}) \geq c_2^{-D^{2\sigma}} \operatorname{dist}(\alpha, S_{T_D}). \tag{1.37}$$

Put

$$Z_D^0 = \{\alpha \in Z_D;\ \operatorname{dist}(\alpha, S_{T_D}) < (4C_{T_D})^{-1}\}$$

where $C_{T_D} = |r|T_D + |s|^{T_D}\|\gamma_0\|$. For $\alpha \in Z_D \backslash Z_D^0$, we get

$$|I_D^{(T_D)}|_\alpha \geq c_2^{-D^{2\sigma}} \frac{1}{4C_{T_D}},$$

and so we have

$$0 \leq^* \log |I_D^{(T_D)}|_\alpha + \log(2c_2)\, D^{2\sigma}$$

because $\log C_{T_D} \ll T_D \leq D^\sigma$. For the other points $\alpha \in Z_D^0$, the inequality (1.37) gives

$$\log \operatorname{dist}(\alpha, S_{T_D}) \leq \log |I_D^{(T_D)}|_\alpha + \log(c_2) D^{2\sigma}.$$

We conclude that

$$\begin{aligned}
&\sum_{\alpha \in Z_D^0} \log \operatorname{dist}(\alpha, \mathcal{S}_{T_D}) \\
&\leq \sum_{\alpha \in Z_D^0} \Big(\log |I_D^{(T_D)}|_\alpha + \log(c_2) D^{2\sigma}\Big) + \sum_{\alpha \in Z_D \backslash Z_D^0} \Big(\log |I_D^{(T_D)}|_\alpha + \log(2c_2)\, D^{2\sigma}\Big) \\
&\leq \sum_{\alpha \in Z_D} \log |I_D^{(T_D)}|_\alpha + \log(2c_2) D^{2\sigma} \deg(Z_D) \quad (\text{since } |Z_D^0| \leq |Z_D| = \deg(Z_D)) \\
&\leq \sum_{\boldsymbol{\alpha} \in \underline{Z}_D} \log \sup\{|Q(\boldsymbol{\alpha})|; Q \in \mathcal{C}_D\} + \log(2c_2) D^{2\sigma} \deg(Z_D) \\
&\leq -\frac{1}{25} D^{\nu-\beta+\sigma-2}(D^\beta \deg(Z_D) + Dh(Z_D)) + \log(2c_2) D^{2\sigma} \deg(Z_D) \\
&\leq^* -\frac{1}{30} D^{\nu-\beta+\sigma-2}(D^\beta \deg(Z_D) + Dh(Z_D)).
\end{aligned}$$

where the penultimate estimate uses (1.36) and the last estimate uses the fact that $\nu > \sigma + 2$.

Step 3. *Subsets of the $\mathbb{Q}$-subvariety.*

For each $\alpha \in \mathbb{P}^2(\mathbb{Q})$, we denote by t_α the smallest non-negative integer with $0 \leq t_\alpha < T_D$ such that $\operatorname{dist}(\alpha, \mathcal{S}_{T_D}) = \operatorname{dist}(\alpha, \gamma_{t_\alpha})$.

For each $m, n \in \mathbb{N}$ with $0 \le m \le n < T_D$, define

$$\Theta(m,n) = \sum_{\substack{\alpha \in Z_D^0 \\ m \le t_\alpha < n}} \log \operatorname{dist}(\alpha, \gamma_{t_\alpha}).$$

Step 2 provides an upper bound for $\Theta(0, T_D)$. Our goal is to construct subsums of $\Theta(0, T_D)$ of the form $\Theta(m, n)$ which are small compared to the number $n - m$ of values of t_α that they involve. In fact, we construct recursively a finite sequence of subsums such that each subsum is computed over an interval that is essentially half of the one of the preceding subsum. More precisely, it is its first half or its second half of this interval depending on which gives the smaller subsum compared to its length (which may vary by ± 1). Technically, we define recursively a finite sequence of pairs (m_j, n_j) by putting

$$(m_0, n_0) = (0, T_D)$$

and

$$(m_{j+1}, n_{j+1}) = \begin{cases} (m_j, k_j) & \text{if} \quad \Theta(m_j, k_j) \le \frac{k_j - m_j}{n_j - m_j} \Theta(m_j, n_j), \\ (k_j, n_j) & \text{else,} \end{cases}$$

where $k_j = \lfloor (m_j + n_j)/2 \rfloor$ as long as $n_j - m_j \ge 2$.

When $n_j - m_j \ge 2$, we have $m_j < k_j < n_j$ and

$$\Theta(m_j, n_j) = \Theta(m_j, k_j) + \Theta(k_j, n_j).$$

We deduce that

$$\Theta(m_{j+1}, n_{j+1}) \le \frac{n_{j+1} - m_{j+1}}{n_j - m_j} \Theta(m_j, n_j).$$

By induction, this yields $\Theta(m_j, n_j) \le \dfrac{n_j - m_j}{T_D} \Theta(0, T_D)$. Using the upper bound for $\Theta(0, T_D)$ computed in Step 2, we deduce that

$$\begin{aligned} \Theta(m_j, n_j) &\le \frac{n_j - m_j}{D^\sigma} \Theta(0, T_D) \\ &\le -\frac{n_j - m_j}{30} \left(D^{\nu-2} \deg(Z_D) + D^{\nu-\beta-1} h(Z_D) \right) \end{aligned} \tag{1.38}$$

for all pairs (m_j, n_j) of our sequence.

Step 4. *Selection of a particular subset*

Define $D_0 = D$ and $D_j = \lceil (n_j - m_j)^{\frac{1}{\sigma}} \rceil$ so that $T_{D_j} \geq n_j - m_j$ and thus

$$\{\gamma_0, \ldots, \gamma_{n_j - m_j - 1}\} \subset \{\gamma_0, \ldots, \gamma_{T_{D_j}}\} = \mathcal{S}_{T_{D_j}} \tag{1.39}$$

Then by the hypothesis, the functions $\Phi^i \tilde{P}_{D_j}$ with $0 \leq i < 2T_{D_j}$ take small absolute values at those points .

Note that, since $m_0 = 0$, we have

$$\tau^{-m_0}(Z_D) = Z_D \subset \mathcal{Z}(\Phi^i \tilde{P}_{D_0};\ 0 \leq i < 2T_{D_0}).$$

So, for fixed D, there exists a largest non-negative integer k such that $n_k - m_k \geq 2$ and

$$\tau^{-m_k}(Z_D) \subset \mathcal{Z}(\Phi^i \tilde{P}_{D_k};\ 0 \leq i < 2T_{D_k}). \tag{1.40}$$

Note that the set $\mathcal{Z}(\Phi^i \tilde{P}_{D_k};\ 0 \leq i < 2T_{D_k})$ is finite.

We claim that D_k *goes to infinity with* D.

Indeed, suppose on the contrary that D_k is bounded above by some positive integer D^* independently of the choice of D. Then $\tau^{-m_k}(Z_D)$ is contained in the set

$$\bigcup_{N=1}^{D^*} \mathcal{Z}(\Phi^i \tilde{P}_{N_k};\ 0 \leq i < 2T_{N_k}),$$

which is finite and independent of D. By equation (1.38) and the fact that $\Theta(m_k, n_k)$ involves at most $\deg(Z_D)$ terms, there exists (for sufficiently large D) a point $\alpha \in Z_D^0$ with $m_k \leq t_\alpha < n_k$ such that

$$\log \operatorname{dist}(\alpha, \gamma_{t_\alpha}) \leq -\frac{n_k - m_k}{30} D^{\nu-2} \leq -\frac{1}{15} D^{\nu-2}.$$

Then we find

$$\begin{aligned}
\log \operatorname{dist}(\tau^{-m_k}(\alpha), \mathcal{S}_{T_{D^*}}) &\leq \log \operatorname{dist}(\tau^{-m_k}(\alpha), \mathcal{S}_{T_{D_k}}) && \text{since } D_k \leq D^* \\
&\leq \log \operatorname{dist}(\tau^{-m_k}(\alpha), \gamma_{t_\alpha - m_k}) && \text{by (1.39)} \\
&\leq \log \operatorname{dist}(\alpha, \gamma_{t_\alpha}) + c_3 m_k && \text{by Lemma 1.7.4} \\
&\leq -\frac{1}{15} D^{\nu-2} + c_3 D^\sigma && \\
&\ll -D^{\nu-2} && \text{since } \nu > \sigma + 2.
\end{aligned}$$

Thus, as D goes to infinity, the distance between $\tau^{-m_k}(\alpha)$ and $\mathcal{S}_{T_{D^*}}$ tends to zero. However, it is not equal to zero since $\mathcal{S}_{T_{D^*}} \cap \mathbb{P}^2(\overline{\mathbb{Q}}) = \emptyset$. So the points $\tau^{-m_k}(\alpha)$ make an infinite sequence in $\cup_{D\in\mathbb{N}} \tau^{-m_k}(Z_D)$. This contradicts the finiteness of $\cup_{D\in\mathbb{N}} \tau^{-m_k}(Z_D)$. Now the claim is verified.

Step 5. *The conclusion*

Put $D' = D_{k+1}$. Since $n_{k+1} - m_{k+1} \asymp n_k - m_k$, we have

$$D' = \lceil (n_{k+1} - m_{k+1})^{1/\sigma} \rceil \asymp \lceil (n_k - m_k)^{1/\sigma} \rceil \asymp D_k,$$

and so D' and $T_{D'} \asymp T_{D_k}$ go to infinity with D.

Put

$$Z'_D = \tau^{-m_{k+1}}(Z_D).$$

Note that, since Z_D is a $\mathbb{Q}$-subvariety of $\mathbb{P}^2(\mathbb{C})$ of dimension 0, so is Z'_D. Set

$$W_D = \{\alpha \in Z^0_D;\ m_{k+1} \le t_\alpha < n_{k+1}\}.$$

Since $W_D \subset Z^0_D \subset Z_D$, we have

$$|W_D| \le |Z_D| = \deg(Z_D), \quad \tau^{-m_{k+1}}(W_D) \subset Z'_D.$$

For any $\alpha \in W_D$, we set

$$\alpha' := \tau^{-m_{k+1}}(\alpha) \in Z'_D,$$
$$\ell_\alpha := t_\alpha - m_{k+1},$$

then we have

$$(\alpha', \gamma_{\ell_\alpha}) = (\tau^{-m_{k+1}}(\alpha), \tau^{-m_{k+1}}(\gamma_{t_\alpha})), \tag{1.41}$$

and

$$0 \le \ell_\alpha < T_{D'}$$

since $t_\alpha - m_{k+1} \le n_{k+1} - m_{k+1} \le \lceil (n_{k+1} - m_{k+1})^{1/\sigma} \rceil^\sigma$. Note that, there is no reason to conclude that $\ell_\alpha = t_{\alpha'}$.

Consider

$$S = \sum_{\alpha\in W_D} \log \operatorname{dist}(\alpha', \gamma_{\ell_\alpha}).$$

We will find an upper bound and a lower bound for S in terms of $h(Z'_D)$ and $\deg(Z_D)$. This will lead to the desired contradiction.

By (1.41), Lemma 1.7.4 gives

$$\begin{aligned} S &\leq \Theta(m_{k+1}, n_{k+1}) + c_3 m_{k+1}|W_D| \\ &\leq \Theta(m_{k+1}, n_{k+1}) + c_3 D^{\sigma} \deg(Z_D) \end{aligned}$$

since $m_{k+1} \leq T_D \leq D^{\sigma}$ and $|W_D| \leq \deg(Z_D)$. Using (1.38), we find that

$$S \leq -\frac{n_{k+1} - m_{k+1}}{30}(D^{\nu-2}\deg(Z_D) + D^{\nu-\beta-1}h(Z_D)) + c_3 D^{\sigma}\deg(Z_D).$$

Since $D^{\nu-2} > D^{\sigma}$ and since $n_{k+1} - m_{k+1} \asymp D'^{\sigma}$ goes to infinity with D, we deduce that

$$S \ll -D'^{\sigma}(D^{\nu-\beta-1}h(Z_D) + D^{\nu-2}\deg(Z_D)).$$

By Proposition 1.8.7, there exists a constant $c'' > 0$ such that

$$h(Z_D) \geq h(Z'_D) - c'' m_{k+1}\deg(Z_D) \geq h(Z'_D) - c'' D^{\sigma}\deg(Z_D)$$

since $m_{k+1} \leq T_D \leq D^{\sigma}$. We conclude that

$$\begin{aligned} S &\ll -D'^{\sigma}D^{\nu-\beta-1}h(Z'_D) - D'^{\sigma}(D^{\nu-2} - c'' D^{\nu-\beta-1+\sigma})\deg(Z_D) \\ &\leq^* -D'^{\sigma}D^{\nu-\beta-1}h(Z'_D) - \frac{1}{2}D'^{\sigma}D^{\nu-2}\deg(Z_D)) \end{aligned} \tag{1.42}$$

where the last inequality follows from the fact that $D^{\nu-2} \geq^* 2c'' D^{\nu-\beta-1+\sigma}$ since $\beta > \sigma + 1$. This gives an upper bound for S in terms of $h(Z'_D)$ and $\deg(Z_D)$. Now we search for a lower bound.

By Step 4, D_k goes to infinity with D, so we have $n_k - m_k \geq^* 2$. By the choice of k, we deduce that

$$Z'_D \not\subset Z(\Phi^i \tilde{P}_{D'};\ 0 \leq i < 2T_{D'}).$$

So there exists an integer i_0 with $0 \leq i_0 < 2T_{D'}$ such that $\Phi^{i_0}\tilde{P}_{D'}$ does not vanish on Z'_D.

For any $\alpha \in W_D$, Proposition 1.7.3 gives

$$\begin{aligned}|\Phi^{i_0}\tilde{P}_{D'}(\boldsymbol{\alpha}')| &\leq \|\boldsymbol{\gamma}_{\ell_\alpha}\|^{-D'} |\Phi^{i_0}(\tilde{P}_{D'})(\boldsymbol{\gamma}_{\ell_\alpha})| + D'\mathcal{L}(\Phi^{i_0}(\tilde{P}_{D'}))\,\mathrm{dist}(\alpha', \gamma_{\ell_\alpha}) \\ &\leq |\Phi^{i_0}(\tilde{P}_{D'})(\boldsymbol{\gamma}_{\ell_\alpha})| + D'2^{D'}\|\Phi^{i_0}(\tilde{P}_{D'})\|\,\mathrm{dist}(\alpha', \gamma_{\ell_\alpha})\end{aligned}$$

where $\boldsymbol{\alpha}'$ is a representative of α' in $\mathbb{C}^3$ of norm 1 and where the last inequality uses $\|\boldsymbol{\gamma}_{\ell_\alpha}\| \geq 1$.

By Step 1, we get

$$\|\Phi^{i_0}\tilde{P}_{D'}\| \leq^* e^{2D'^\beta},$$

and

$$|\Phi^{i_0}(\tilde{P}_{D'})(\boldsymbol{\gamma}_{\ell_\alpha})| \leq^* e^{-(1/2)D'^\nu}$$

since $0 \leq \ell_\alpha \leq T_{D'}$. This implies that

$$|\Phi^{i_0}\tilde{P}_{D'}(\boldsymbol{\alpha}')| \leq^* e^{-(1/2)D'^\nu} + \frac{1}{2}e^{3D'^\beta}\,\mathrm{dist}(\alpha', \gamma_{\ell_\alpha}) \tag{1.43}$$

for any $\alpha \in W_D$.

By Step 1 and the fact that $0 \leq i_0 < 2T_{D'}$, we also have

$$c'^{2D'T_{D'}}\Phi^{i_0}(\tilde{P}_{D'}) \in (\mathcal{C}_{D'} \cap \mathbb{Z}[\mathbf{X}])\backslash\mathcal{I}(Z'_D).$$

Applying Lemma 1.2.9 to this polynomial, we obtain

$$0 \leq 7\log(3)D'\deg(Z'_D) + D'h(Z'_D) + \sum_{\boldsymbol{\alpha}\in\underline{Z}'_D} \log\left|c'^{2D'T_{D'}}\Phi^{i_0}(\tilde{P}_{D'})(\boldsymbol{\alpha})\right|$$

Since $|Z'_D| = \deg(Z'_D) = \deg(Z_D)$, this implies that

$$\begin{aligned}&\sum_{\boldsymbol{\alpha}\in\underline{Z}'_D} \log|\Phi^{i_0}\tilde{P}_{D'}(\boldsymbol{\alpha})| \\ &\qquad\geq -7\log(3)D'\deg(Z_D) - D'h(Z'_D) - 2\log(c')D'T_{D'}\deg(Z_D) \\ &\qquad\geq^* -D'h(Z'_D) - 3\,\log(c')D'^{1+\sigma}\deg(Z_D),\end{aligned}$$

using $7\log(3) \leq^* T_{D'} \leq D'^\sigma$. Since $\log\|\Phi^{i_0}\tilde{P}_{D'}\| \leq 2D'^\beta$, we find

$$\log|\Phi^{i_0}\tilde{P}_{D'}(\boldsymbol{\alpha})| \leq D'\log(3) + \log\|\Phi^{i_0}\tilde{P}_{D'}\| \leq 4D'^\beta$$

for any $\boldsymbol{\alpha} \in \mathbb{C}^3$ of norm 1. Hence, for any non-empty subset $\underline{W} \subset \underline{Z}'_D$, we have

$$\begin{aligned}\sum_{\boldsymbol{\alpha}\in\underline{W}} \log|\Phi^{i_0}\tilde{P}_{D'}(\boldsymbol{\alpha})| &\geq \sum_{\boldsymbol{\alpha}\in\underline{Z}'_D} \log|\Phi^{i_0}\tilde{P}_{D'}(\boldsymbol{\alpha})| - 4D'^{\beta}\deg(Z_D)\\ &\geq -D'h(Z'_D) - 3\log(c')D'^{1+\sigma}\deg(Z_D) - 4D'^{\beta}\deg(Z_D)\\ &\geq^* -D'h(Z'_D) - 5D'^{\beta}\deg(Z_D) \qquad (1.44)\end{aligned}$$

since $D'^{\beta} \geq^* 3\log(c')D'^{1+\sigma}$.

By the choice of k, we have

$$\begin{aligned}\tau^{-m_k}(Z_D) &\subset \mathcal{Z}(\Phi^i\tilde{P}_{D_k};\ 0 \leq i < 2T_{D_k})\\ &\subset \mathcal{Z}(\Phi^i\tilde{P}_{D_k};\ 0 \leq i < T_{D_k} + D_k)\end{aligned}$$

Recall that, by construction, we have $X_0 \nmid \tilde{P}_{D_k}$, $X_2 \nmid \tilde{P}_{D_k}$. Moreover, the estimates of Step 1 give

$$\max\left\{25\log(3)D_k, \log\|\tilde{P}_{D_k}\|, \log\|c'^{D_k^2}\tilde{P}_{D_k}\|, \dots, \log\|c'^{D_k^2}\Phi^{D_k}\tilde{P}_{D_k}\|\right\} < Y_{D_k} = 2D_k^{\beta}.$$

Applying Proposition 1.8.8 to $\tau^{-m_k}(Z_D)$, we get

$$\deg Z_D = \deg(\tau^{-m_k}(Z_D)) \leq \frac{D_k^2}{T_{D_k}} \asymp D_k^{2-\sigma} \asymp D'^{2-\sigma} \qquad (1.45)$$

and

$$h(\tau^{-m_k}(Z_D)) \ll \frac{D_k Y_{D_k}}{T_{D_k}} + D_k^2 \asymp D_k^{\beta-\sigma+1} \asymp D'^{\beta-\sigma+1}$$

since $\beta > \sigma + 1$. By Proposition 1.8.7, this implies that

$$\begin{aligned}h(Z'_D) &= h(\tau^{m_k - m_{k+1}}(\tau^{-m_k}(Z_D)))\\ &\ll h(\tau^{-m_k}(Z_D)) + (m_{k+1} - m_k)\deg(Z_D)\\ &\ll D'^{\beta-\sigma+1} + T_{D'}D'^{2-\sigma}\\ &\ll D'^{\beta-\sigma+1} \qquad (1.46)\end{aligned}$$

since $0 \leq m_{k+1} - m_k \leq n_k - m_k \leq T_{D_k} \asymp T_{D'} \leq D'^{\sigma}$ and $\beta > \sigma + 1$.

Combining (1.44), (1.45) and (1.46), we obtain

$$\sum_{\boldsymbol{\alpha}\in\underline{W}} \log|\Phi^{i_0}\tilde{P}_{D'}(\boldsymbol{\alpha})| \gg -D'^{\beta-\sigma+2}. \qquad (1.47)$$

For each $\alpha \in W_D$, applying the above inequality to $\underline{W} = \{\boldsymbol{\alpha}'\}$ where $\boldsymbol{\alpha}'$ is a representative of $\alpha' = \tau^{-m_{k+1}}(\alpha)$ in $\mathbb{C}^3$ of norm 1, we get

$$|\Phi^{i_0}\tilde{P}_{D'}(\boldsymbol{\alpha}')| \geq 2e^{-(1/2)D'^{\nu}}$$

when D' is sufficiently large, *i.e.*, when D is sufficiently large, since $\nu > \beta - \sigma + 2$. By (1.43), we conclude that

$$2e^{-\frac{1}{2}D'^{\nu}} \leq |\Phi^{i_0}\tilde{P}_{D'}(\boldsymbol{\alpha}')| \leq e^{-\frac{1}{2}D'^{\nu}} + \frac{1}{2}e^{3D'^{\beta}} \operatorname{dist}(\alpha', \gamma_{\ell_\alpha}) \quad \text{when } D \gg 1.$$

So, for such points, when D is large, we have

$$e^{-\frac{1}{2}D'^{\nu}} \leq \frac{1}{2}e^{3D'^{\beta}} \operatorname{dist}(\alpha', \gamma_{\ell_\alpha}),$$

and thus

$$|\Phi^{i_0}\tilde{P}_{D'}(\boldsymbol{\alpha}')| \leq e^{3D'^{\beta}} \operatorname{dist}(\alpha', \gamma_{\ell_\alpha}).$$

This means that

$$\log \operatorname{dist}(\alpha', \gamma_{\ell_\alpha}) \geq \log |\Phi^{i_0}\tilde{P}_{D'}(\boldsymbol{\alpha}')| - 3D'^{\beta}$$

for any $\alpha \in W_D$. This yields that

$$\begin{aligned} S = \sum_{\alpha \in W_D} \log \operatorname{dist}(\alpha', \gamma_{\ell_\alpha}) &\geq \sum_{\alpha \in W_D} \log |\Phi^{i_0}\tilde{P}_{D'}(\boldsymbol{\alpha}')| - 3D'^{\beta}|W_D| \\ &\geq \sum_{\alpha \in W_D} \log |\Phi^{i_0}\tilde{P}_{D'}(\boldsymbol{\alpha}')| - 3D'^{\beta} \deg(Z_D). \end{aligned}$$

Applying (1.44) to $W = \tau^{-m_{k+1}}(W_D) \subset Z'_D$, we obtain

$$\sum_{\alpha \in W_D} \log |\Phi^{i_0}\tilde{P}_{D'}(\boldsymbol{\alpha}')| \geq -D'h(Z'_D) - 5D'^{\beta} \deg(Z_D).$$

So we conclude that

$$S \geq -D'h(Z'_D) - 8D'^{\beta} \deg(Z_D).$$

We just found a lower bound for S in the term of $h(Z'_D)$ and $\deg(Z_D)$. Combining it with the upper bound given by (1.42), we get

$$D'h(Z'_D) + 8D'^{\beta} \deg(Z_D) \geq \lambda \left(D'^{\sigma} D^{\nu-\beta-1} h(Z'_D) + \frac{1}{2} D'^{\sigma} D^{\nu-2} \deg(Z_D) \right)$$

for some constant $\lambda > 0$ which is independent of the choice of D. This implies that

$$\begin{aligned}(D' - \lambda D'^{\sigma} D^{\nu-\beta-1}) h(Z'_D) &\geq \left(\frac{\lambda}{2} D'^{\sigma} D^{\nu-2} - 8D'^{\beta}\right) \deg(Z_D) \\ &\geq^* \frac{\lambda}{4} D'^{\sigma} D^{\nu-2} \deg(Z_D) > 0\end{aligned}$$

where the last estimate follows from the fact that

$$\frac{\lambda}{4} D'^{\sigma} D^{\nu-2} \geq \frac{\lambda}{4} D'^{\sigma+\nu-2} \geq^* 8D'^{\beta}$$

since $\nu > \max\{\beta + (2-\sigma), 2\}$. Note that

$$0 \leq h(Z'_D) \ll D'^{\beta-\sigma+1}, \quad \text{and} \quad \deg(Z_D) \geq 1.$$

We conclude that

$$D' >^* \lambda D'^{\sigma} D^{\nu-\beta-1}$$

and

$$D'^{\sigma} D^{\nu-2} \ll D' h(Z'_D) \ll D'^{\beta-\sigma+2}.$$

This implies that

$$D'^{\sigma-1} \ll D^{\beta+1-\nu} \quad \text{and} \quad D^{\nu-2} \ll D'^{\beta-2\sigma+2}. \tag{1.48}$$

Since $\sigma \geq 1$, this implies that

$$D^{(\nu-2)(\sigma-1)} \ll D'^{(\beta-2\sigma+2)(\sigma-1)} \ll D^{(\beta+1-\nu)(\beta-2\sigma+2)},$$

and thus

$$(\nu-2)(\sigma-1) \leq (\beta+1-\nu)(\beta-2\sigma+2).$$

This means that

$$\nu \leq \beta + 2 - \sigma + \frac{(\sigma-1)(2-\sigma)}{\beta-(\sigma-1)}.$$

which contradicts the hypothesis on ν. We conclude that $\xi, \eta \in \overline{\mathbb{Q}}$. $\square$

Chapter 2

On approximation by rational points

2.1 Introduction

2.1.1 Statement of the results

Let $\boldsymbol{\theta} = (1, \theta_1, \dots, \theta_d) \in \mathbb{R}^{d+1}$. We say that a real number $\lambda \geq 0$ is *a uniform exponent of approximation to* $\boldsymbol{\theta}$ if there exists a constant $c = c(\boldsymbol{\theta}) > 0$ such that

$$|x_0| \leq X, \quad \max_{1 \leq i \leq d} |x_0\theta_i - x_i| \leq cX^{-\lambda} \tag{2.1}$$

admits a non-zero solution $(x_0, x_1, \dots, x_d) \in \mathbb{Z}^{d+1}$ for each $X \geq 1$. We denote by $\hat{\lambda}(\boldsymbol{\theta})$ the supremum of all these exponents.

Note that for $\boldsymbol{\theta} \in \mathbb{C}^{d+1} \setminus \mathbb{R}^{d+1}$, this definition would give $\hat{\lambda}(\boldsymbol{\theta}) = 0$. Indeed, WLOG, suppose that $\mathrm{Im}(\theta_1) \neq 0$. Then $|x_0\theta_1 - x_1| > |\mathrm{Im}(\theta_1)| > 0$ for any integer $x_0 \neq 0$. Hence, if $(x_0, x_1, \dots, x_d) \in \mathbb{Z}^{d+1}$ is a solution of (2.1) with X large enough and some fixed $\lambda > 0$ then the inequality $|x_0\theta_1 - x_1| \leq cX^{-\lambda}$ implies that $x_0 = 0$, and so we have $x_i = 0$ for all $i \leq d$. This is impossible.

The following lemma gathers several properties of the exponent $\hat{\lambda}$.

Lemma 2.1.1. *Let* $\boldsymbol{\theta} = (1, \theta_1, \dots, \theta_d) \in \mathbb{R}^{d+1}$.

(i) We have $\hat{\lambda}(1, \theta_1, \dots, \theta_m) \geq \hat{\lambda}(\boldsymbol{\theta})$ *if* $m \leq d$.

(ii) Let $\{1, e_1, \dots, e_t\}$ *be a basis of the vector space* $\langle 1, \theta_1, \dots, \theta_d \rangle_{\mathbb{Q}}$. *Then* λ *is a uniform exponent of approximation to* $\boldsymbol{\theta}$ *if and only if* λ *is a uniform exponent of approximation to* $(1, e_1, \dots, e_t)$. *In particular, we have*

$$\hat{\lambda}(1, e_1, \dots, e_t) = \hat{\lambda}(\boldsymbol{\theta}).$$

Proof. The assertion (i) is clear from the definition.

Assume that λ is a uniform exponent of approximation to $\boldsymbol{\theta}' = (1, e_1, \dots, e_t)$, *i.e.* that there exists a constant $c > 0$ such that the inequalities

$$|x_0| \leq X, \quad \max_{1 \leq i \leq t} |x_0 e_i - x_i| \leq c X^{-\lambda} \tag{2.2}$$

admit a solution in $\mathbb{Z}^{t+1} \setminus \{0\}$ for any sufficiently large value of X.

We will show that λ is also a uniform exponent of approximation to $\boldsymbol{\theta}$.

Let $M \in \mathrm{Mat}(\mathbb{Q})$ be the $(t+1) \times (d+1)$ matrix with coefficients in $\mathbb{Q}$ such that $\boldsymbol{\theta} = \boldsymbol{\theta}' M$. The first column of M is ${}^t(1, 0 \dots, 0)$. Let $m \in \mathbb{N}$ such that $mM \in \mathrm{Mat}(\mathbb{Z})$. Suppose that $\mathbf{x} \in \mathbb{Z}^{t+1}$ is a solution of (2.2) for some $X > 1$. Then the point $\mathbf{y} = m\mathbf{x}M$ belongs to $\mathbb{Z}^{d+1}$ and upon writing $\mathbf{y} = (y_0, \dots, y_d)$, we have

$$\begin{aligned} &|y_0| = |m x_0| \leq mX, \\ &\max_{1 \leq i \leq d} |y_0 \theta_i - y_i| = \|m x_0 \boldsymbol{\theta}' M - m\mathbf{x}M\| \ll \|x_0 \boldsymbol{\theta}' - \mathbf{x}\| \ll X^{-\lambda} \end{aligned}$$

with implied constants depending on M. Thus λ is also a uniform exponent of approximation to $\boldsymbol{\theta}$.

Conversely, assume that λ is a uniform exponent of approximation to $\boldsymbol{\theta}$. WLOG, we may assume that $\{1, \theta_1, \dots, \theta_t\}$ is a basis of $\langle 1, \theta_1, \dots, \theta_d \rangle_{\mathbb{Q}} = \langle 1, e_1, \dots, e_t \rangle_{\mathbb{Q}}$. It follows from the definition that λ is also a uniform exponent of approximation to $(1, \theta_1, \dots, \theta_t)$ and so, by the above, it is also a uniform exponent of approximation to $(1, e_1, \dots, e_t)$ since $\{1, \theta_1, \dots, \theta_t\}$ is a basis of $\langle 1, e_1, \dots, e_t \rangle_{\mathbb{Q}}$. □

Throughout this chapter, we restrict to points $\boldsymbol{\theta} = (1, \theta_1, \dots, \theta_d) \in \mathbb{R}^{d+1}$ with $\mathbb{Q}$-linearly independent coordinates.

Lemma 2.1.2. *Let $\boldsymbol{\theta} = (1, \theta_1, \ldots, \theta_d) \in \mathbb{R}^{d+1}$ with $\mathbb{Q}$-linearly independent coordinates. Then*

(i) $\hat{\lambda}(\boldsymbol{\theta}) \geq 1/d$;

(ii) $\hat{\lambda}(\boldsymbol{\theta}) = 1/d$ *if* $\theta_1, \ldots, \theta_d$ *are algebraic over* $\mathbb{Q}$.

Proof.

(i) If $\lambda = 1/d$ and $c = 1$, then the volume of the convex body defined by (2.1) is 2^{d+1} for any $X > 0$. From Minkowski's First Convex Body Theorem, it follows that for any $X > 0$, this convex body contains a non-zero point of $\mathbb{Z}^{d+1}$. This shows that $1/d$ is a uniform exponent of approximation to $\boldsymbol{\theta}$ and so $\hat{\lambda}(\boldsymbol{\theta}) \geq 1/d$.

(ii) Suppose that $\hat{\lambda}(\boldsymbol{\theta}) \neq 1/d$. From (i), we have $\hat{\lambda}(\boldsymbol{\theta}) > 1/d$, *i.e.*, there exist $\epsilon > 0$ and $c > 0$ such that the inequalities

$$|x_0| \leq X, \quad \max_{1 \leq i \leq d} |x_0\theta_i - x_i| \leq cX^{-1/d-\epsilon}$$

have a non-zero solution $\mathbf{x} = (x_0, \ldots, x_d)$ in $\mathbb{Z}^{d+1}$ for each $X > 1$. This in turn implies the existence of $\epsilon' > 0$ such that

$$\max_{1 \leq i \leq d} |x_0\theta_i - x_i| < \|\mathbf{x}\|^{-1/d-\epsilon'}$$

admits a non-zero solution $\mathbf{x} \in \mathbb{Z}^{d+1}$ for each $X \gg 1$. Such solution $\mathbf{x}$ satisfies

$$|M_0(\mathbf{x})M_1(\mathbf{x}) \cdots M_d(\mathbf{x})| < \|\mathbf{x}\|^{-d\epsilon'}$$

where $M_0(\mathbf{x}) = x_0, M_1(\mathbf{x}) = x_0\theta_1 - x_1, \ldots, M_d(\mathbf{x}) = x_0\theta_1 - x_d$ are $\mathbb{Q}$-linearly independent linear forms with algebraic coefficients. By Schmidt's Subspace Theorem, these points lie in a finite number of proper subspaces of $\mathbb{R}^{d+1}$ defined over $\mathbb{Q}$. However, these points converge to $\boldsymbol{\theta}$ projectively as X goes to infinity. So $\boldsymbol{\theta}$ must belong to one of these proper subspaces. This is impossible since $\boldsymbol{\theta}$ has linearly independent coordinates.

□

The following are results that apply to points of the form $\boldsymbol{\theta} = (1, \theta, \ldots, \theta^d)$ where θ is either transcendental or algebraic of degree $> d$.

It is well-known that $\hat{\lambda}(1, \theta) = 1$.

In 1969, H. Davenport and W. M. Schmidt proved in [6] that

$$\hat{\lambda}(1, \theta, \ldots, \theta^d) \leq \begin{cases} 1/\gamma \simeq 0.618 & \text{if } d = 2, \\ 1/2 & \text{if } d = 3, \\ \lfloor d/2 \rfloor^{-1} & \text{if } d \geq 4, \end{cases}$$

where $\gamma = \dfrac{1+\sqrt{5}}{2}$ denotes the golden ratio.

In the case $d = 2$, it is shown in [18, 2004] that the above upper bound is best possible. More precisely, there exist real non-quadratic irrational numbers θ such that $1/\gamma$ is a uniform exponent of approximation to $(1, \theta, \theta^2)$. Any such θ is transcendental over $\mathbb{Q}$, and the set of these numbers is countable.

Nevertheless, no optimal upper bound for $\lambda(1, \theta, \ldots, \theta^d)$ is known for $d \geq 3$ when θ is transcendental. Note that, when θ is algebraic of degree $> d$, then it follows from Lemma 2.1.2 that $\hat{\lambda}(1, \theta, \ldots, \theta^d) = 1/d$.

In [13, 2003], M. Laurent proved that $\hat{\lambda}(1, \theta, \ldots, \theta^d) \leq \lceil d/2 \rceil^{-1}$ if $d \geq 3$ which improves the result of H. Davenport and W. M. Schmidt for odd $d \geq 5$.

In [19, 2008], D. Roy sharpened the estimate in case $d = 3$, by showing that

$$\hat{\lambda}(1, \theta, \theta^2, \theta^3) \leq \frac{1}{2}\left(2 + \sqrt{5} - \sqrt{7 + 2\sqrt{5}}\right) \simeq 0.4245.$$

In this chapter, we will consider points of the form $\boldsymbol{\theta} = (1, \theta_1, \ldots, \theta_{d-1}, \xi)$ where $\{1, \theta_1, \ldots, \theta_{d-1}\}$ is a basis of a real field extension K of $\mathbb{Q}$ of degree $d \geq 2$ and $\xi \in \mathbb{R} \backslash K$. These conditions ensure that the coordinates of $\boldsymbol{\theta}$ are $\mathbb{Q}$-linearly independent. By noting that $K = \mathbb{Q}(\alpha)$ for some algebraic number $\alpha \in \mathbb{R}$ of degree d, we deduce from Lemma 2.1.1 (ii) that

$$\hat{\lambda}(1, \theta_1, \ldots, \theta_{d-1}, \xi) = \hat{\lambda}(1, \alpha, \ldots, \alpha^{d-1}, \xi).$$

From the two previous lemmas , we deduce that

$$\frac{1}{d} \leq \hat{\lambda}(\boldsymbol{\theta}) \leq \hat{\lambda}(1, \alpha, \ldots, \alpha^{d-1}) = \frac{1}{d-1}. \tag{2.3}$$

In the case $d = 2$, it is shown in [22] that $1/\gamma$ is an optimal upper bound for $\hat{\lambda}(1, \alpha, \xi)$. More precisely, D. Roy proved in [22] that this value is the largest exponent of approximation achieved by points with $\mathbb{Q}$-linearly independent coordinates on any real conic defined over $\mathbb{Q}$.

The main result of this chapter applies to any integer $d \geq 2$. We establish a general upper bound for $\hat{\lambda}(\boldsymbol{\theta})$ which reduces to $1/\gamma$ when $d = 2$. Moreover, this upper bound is strictly smaller than $\frac{1}{d} + \frac{1}{d^2} = \frac{1}{d-1} - \frac{1}{d^2(d-1)}$, which is a notable improvement on (2.3).

Theorem 2.1.3. *Let K be a real number field of degree $d \geq 2$ with basis $\{1, \theta_1, \ldots, \theta_{d-1}\}$ over $\mathbb{Q}$ and let $\xi \in \mathbb{R} \setminus K$. Let c and λ be positive real numbers. Suppose that for any sufficiently large value of X, the inequalities*

$$\begin{cases} |x_0| \leq X \\ |x_0\theta_1 - x_1| \leq cX^{-\lambda} \\ \qquad \cdots \\ |x_0\theta_{d-1} - x_{d-1}| \leq cX^{-\lambda} \\ |x_0\xi - x_d| \leq cX^{-\lambda} \end{cases} \tag{2.4}$$

admit a non-zero solution $x = (x_0, x_1, \ldots, x_d) \in \mathbb{Z}^{d+1}$. Then $\lambda \leq \lambda_d$ where λ_d is the unique positive real root of the equation

$$x + (d-1)x^2 + \cdots + (d-1)^{d-1}x^d = 1. \tag{2.5}$$

The following corollary provides an estimate for λ_d. However, we do not know if our upper bound λ_d is optimal for $d \geq 3$.

Corollary 2.1.4. *Under the notation of Theorem 2.1.3, we have*

$$\hat{\lambda}(1, \theta_1, \ldots, \theta_{d-1}, \xi) \leq \begin{cases} 1/\gamma & \text{if } d = 2, \\ \lambda_3 \simeq 0.40527 & \text{if } d = 3, \\ \lambda_d < \frac{1}{d-1} - \frac{1}{d^2(d-1)} & \text{if } d \geq 2. \end{cases}$$

Applying the main result of Y. Bugeaud and M. Laurent in [3] to our main result, we obtain the following consequence.

Corollary 2.1.5. *Let the notation be as in Theorem 2.1.3. Assume that* $\lambda > \lambda_d$. *Then, for any* $\eta \in \mathbb{R}$, *there are arbitrarily large values of* X *such that the inequalties*

$$\begin{cases} |x_0 + x_1\theta_1 + \cdots + x_{d-1}\theta_{d-1} + x_d\xi + \eta| \leq X^{-1/\lambda} \\ \|\mathbf{x}\| \leq X \end{cases} \tag{2.6}$$

have a solution $\mathbf{x} = (x_0, \ldots, x_d)$ *in* $\mathbb{Z}^{d+1}$.

The proof of our main theorem follows the approach of Davenport and Schmidt in [6]. Its details occupy four sections. In the notation of the theorem, let $\boldsymbol{\theta} = (1, \theta_1, \ldots, \theta_{d-1}, \xi)$. In Section 2.2, we construct a canonical sequence of primitive integer points $(\mathbf{x}_i)_{i\in\mathbb{N}}$ converging to $\boldsymbol{\theta}$ projectively. We call it a sequence of minimal points for $\boldsymbol{\theta}$ and establish some basic properties of this sequence, similarly as it is done in [6]. Section 2.3 however is novel and provides the key to the proof of our theorem. In this section, we look at subspaces of $\mathbb{R}^{d+1}$ spanned by consecutive minimal points and study how their dimension varies with the length of the sequence, i.e. as a function of the first and last minimal point in the spanning set. In this way, based on the choice of a fixed "initial" minimal point $\mathbf{x}_{i_0}$, we construct, for each $k = 1, \ldots, d$, families of subspaces $(U_t^k)_{k-1\leq t\leq d-1}$ of dimension k and $(V_t^{k+1})_{k-1\leq t\leq d-1}$ of dimension $k+1$. Based on properties of these spaces under sum and intersection, we obtain some strong inequality linking their heights. This is done by descending induction on k, using a theorem of Schmidt. Then, our key inequality is obtained by taking $k = 1$. The latter relates the heights of some explicit set of minimal points associated with the choice of $\mathbf{x}_{i_0}$. Section 2.4 provides the last tool that we need, a very general upper bound for the norm of any minimal point in terms of the norm of the next minimal point. It is obtained through geometry of numbers, by observing that the first d coordinates of any minimal point provide a good rational approximation to the point $(1, \theta_1, \ldots, \theta_{d-1})$. The proof of Theorem 2.1.3 is presented in Section 2.5, based on all these estimates. Thus, we have $\hat{\lambda}(\boldsymbol{\theta}) \leq \lambda_d$. In the same section, we also consider the hypothetical situation where $\hat{\lambda}(\boldsymbol{\theta}) = \lambda_d$ is precisely the uniform exponent of approximation to $\boldsymbol{\theta}$. In that case, we show that there exists a subsequence $(\mathbf{y}_i)_{i\in\mathbb{N}}$ of the sequence of minimal points which satisfies very rigid growth estimates and which "explains" the fact that $\hat{\lambda}(\boldsymbol{\theta}) = \lambda_d$. Moreover, any $d+1$ consecutive points in this sequence are linearly independent and their determinant is bounded from above. This situation is very similar to that of the extremal numbers in [18], except that here we don't know if extremal points $\boldsymbol{\theta}$ exist. The precise construction is delicate and obtained by "pasting" together the finite sequences of minimal points defined in Section 2.3.

Section 2.6 provides an alternative proof of the main estimate of Section 4. In this section, we construct a multi-linear symmetric polynomial map Φ from $(\mathbb{R}^{d+1})^d$ to $\mathbb{R}$ defined over $\mathbb{Q}$, whose restriction $\varphi(\mathbf{x}) = \Phi(\mathbf{x}, \dots, \mathbf{x})$ to the diagonal is closely connected to the norm map from K to $\mathbb{Q}$. Looking at the values of φ at minimal points and showing that they are non-zero, we obtain an alternative proof for the main estimate of Section 2.4. In Section 2.7, we use Φ to construct a polynomial map $\Psi : (\mathbb{R}^{d+1})^d \to \mathbb{R}^{d+1}$. Then, we study its properties and use them to provide algebraic relations between the points of the sequence $(\mathbf{y}_i)_{i\in\mathbb{N}}$ constructed in Section 2.5 in the case where $\hat{\lambda}(\boldsymbol{\theta}) = \lambda_d$. We view Ψ as an analog of the bracket operator of [18, §2]. We were not able to go further on these lines of investigation but hope that the above mentioned result will be useful for further study in this topic.

The last section of this chapter derives from several unsuccesful trials to construct points $\boldsymbol{\theta}$ of the above form, for which the uniform exponent of approximation $\hat{\lambda}(\boldsymbol{\theta})$ is greater than the trivial lower bound $1/d$ provided by the box principle. In this section, we fix $d = 3$, set $\alpha = \sqrt[3]{2}$, and construct a transcendental number $\xi \in \mathbb{R}$ such that $\hat{\lambda}(1, \alpha, \alpha^2, \xi) \geq 1/3$. However, the sequence of minimal points attached to $(1, \alpha, \alpha^2, \xi)$ have their norms growing in the fastest possible way, something that cannot be achieved by an application of the box principle.

2.1.2 Proofs of the corollaries

Proof of Corollary 2.1.4. By direct computation, we get $\lambda_2 = 1/\gamma$ and $\lambda_3 \simeq 0.40527$. We will verify that $\lambda_d < \frac{d+1}{d^2}$ for $d \geq 2$. Set $y = (d-1)x$. The equation (2.5) is equivalent to

$$y + y^2 + \cdots + y^d = d - 1.$$

Set $f(y) = 1 + y + y^2 + \cdots + y^d - d$. Then $f(y)$ is an increasing function on $\mathbb{R}^+$. We need to prove that the unique positive real zero of f is less than $y_0 = (d^2-1)/d^2$. It is enough to show that $f(y_0) > 0$.

We have

$$f(y_0) = \frac{1 - y_0^{d+1}}{1 - y_0} - d = d^2 - d - d^2\left(\frac{d^2-1}{d^2}\right)^{d+1}$$

The inequality $f(y_0) > 0$ is equivalent to

$$d^2 - d > d^2\left(\frac{d^2-1}{d^2}\right)^{d+1},$$

which is equivalent to

$$\left(\frac{d}{d-1}\right)^{d} > \left(\frac{d+1}{d}\right)^{d+1}.$$

This is true since the function $\left(\dfrac{d}{d-1}\right)^{d}$ is decreasing for $d > 1$. □

The proof of Corollary 2.1.5 is based on the main result of Y. Bugeaud and M. Laurent in [3]. In order to state this result, we first introduce the following notation.

For any positive integer n, and for any point $\mathbf{x} \in \mathbb{R}^n$, we denote by

$$\{\mathbf{x}\} = \min_{\mathbf{y} \in \mathbb{Z}^n} \|\mathbf{x} - \mathbf{y}\|$$

the distance from $\mathbf{x}$ to a closest integer point.

Let A be a real $n \times m$ matrix. For any columm vector $\boldsymbol{\eta}$ in $\mathbb{R}^n$, we denote by $\omega(A, \boldsymbol{\eta})$ the supremum of the real numbers ω for which, for *arbitrarily large real numbers* X, the inequalities

$$\{A \cdot \mathbf{x} + \boldsymbol{\eta}\} \le X^{-\omega}, \quad \|\mathbf{x}\| \le X \tag{2.7}$$

have a non-zero solution $\mathbf{x} = (x_0, \ldots, x_d)$ in $\mathbb{Z}^m$. We denote by $\hat{\omega}(A, \boldsymbol{\eta})$ the supremum of the real numbers ω for which, for *all sufficiently large real numbers* X, the inequalities (2.7) have a solution $\mathbf{x}$ in $\mathbb{Z}^m$. We define furthermore two homogeneous exponents $\omega(A)$ and $\hat{\omega}(A)$ by setting $\omega(A) := \omega(A, 0)$ and $\hat{\omega}(A) := \hat{\omega}(A, 0)$.

The main result in [3] is reads as follows.

Theorem 2.1.6 (Y. Bugeaud, M. Laurent, 2005)**.** *For any real $n \times m$ matrix A, and any column vector $\boldsymbol{\eta} \in \mathbb{R}^n$, we have the lower bounds*

$$\omega(A, \boldsymbol{\eta}) \geq \frac{1}{\hat{\omega}(A^t)} \quad \text{and} \quad \hat{\omega}(A, \boldsymbol{\eta}) \geq \frac{1}{\omega(A^t)} \tag{2.8}$$

with equality in (2.8) *for almost all $\boldsymbol{\eta}$ with respect to the Lebesgue measure on $\mathbb{R}^n$.*

Based on this, we can now prove Corollary 2.1.5.

Proof of Corollary 2.1.5. Set $\boldsymbol{\theta} = (1, \theta_1, \ldots, \theta_{d-1}, \xi)$, $\boldsymbol{\eta} = (\eta, 0, \ldots, 0) \in \mathbb{R}^{d+1}$ and set

$$A_{\boldsymbol{\theta}} = \begin{pmatrix} 0 & \theta_1 & \ldots & \theta_{d-1} & \xi \\ 0 & -1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & -1 & 0 \\ 0 & 0 & \ldots & 0 & -1 \end{pmatrix}.$$

Then, for any $\mathbf{x} \in \mathbb{Z}^{d+1}$, we have

$$A_{\boldsymbol{\theta}}^t \mathbf{x}^t = (0, x_0\theta_1 - x_1, \ldots, x_0\theta_{d-1} - x_{d-1}, x_0\xi - x_d)^t$$

and

$$\{A_{\boldsymbol{\theta}} \cdot \mathbf{x}^t + \boldsymbol{\eta}^t\} = \{x_1\theta_1 + \cdots + x_{d-1}\theta_{d-1} + x_d\xi + \eta\}.$$

From definition, we conclude that $\hat{\lambda}(\boldsymbol{\theta}) = \hat{\omega}(A_{\boldsymbol{\theta}}^t)$. By (2.8), we get

$$\omega(A_{\boldsymbol{\theta}}, \boldsymbol{\eta}) \geq \frac{1}{\hat{\omega}(A_{\boldsymbol{\theta}}^t)} = \frac{1}{\hat{\lambda}(\boldsymbol{\theta})} \geq \frac{1}{\lambda_d}.$$

Since $\lambda > \lambda_d$, this implies that $\omega(A_{\boldsymbol{\theta}}, \boldsymbol{\eta}) > 1/\lambda$. This means that there are arbitrarily large real numbers X such that the system

$$\{x_1\theta_1 + \cdots + x_{d-1}\theta_{d-1} + x_d\xi + \eta\} \leq X^{-1/\lambda}, \quad \|\mathbf{x}\| \leq X/2$$

has a solution in $\mathbf{x} = (x_0, \ldots, x_d) \in \mathbb{Z}^{d+1}$. If X is large enough then the system (2.6) also has a solution in $\mathbb{Z}^{d+1}$. □

2.1.3 Notation

.

In this chapter, for any point $\mathbf{x}$ in $\mathbb{R}^{d+1}$, we denote by $\mathbf{x}^-$ the point of $\mathbb{R}^d$ whose coordinates are the first d coordinates of $\mathbf{x}$.

For any point $\boldsymbol{\theta} = (\theta_0, \theta_1, \dots, \theta_d)$ in $\mathbb{R}^{d+1}$, we define the function $L_{\boldsymbol{\theta}} : \mathbb{R}^{d+1} \to \mathbb{R}$ by

$$L_{\boldsymbol{\theta}}(\mathbf{x}) = \max_{1 \le i \le d} |x_0\theta_i - \theta_0 x_i|$$

for each $\mathbf{x} = (x_0, \dots, x_d) \in \mathbb{R}^{d+1}$.

2.2 Construction of minimal points

In this section, we fix a point $\boldsymbol{\theta} = (1, \theta_1, \dots, \theta_d) \in \mathbb{R}^{d+1}$ with $\mathbb{Q}$-linearly independent coordinates.

To study the problem of uniform aproximation to $\boldsymbol{\theta}$, we follow the approach of Davenport and Schmidt in [6] by first defining a certain sequence of primitive points $(\mathbf{x}_i)_{i\in\mathbb{N}}$ in $\mathbb{Z}^{d+1}$, called *minimal points*, which converges projectively to $\boldsymbol{\theta}$.

First of all, for each real $X > 1$, we consider the set of integer points $\mathbf{x} = (x_0, \dots, x_d)$ with

$$1 \le x_0 \le \|\mathbf{x}\| \le X, \quad |x_0\theta_1 - x_1| \le \frac{1}{2}, \dots, |x_0\theta_d - x_d| \le \frac{1}{2}.$$

Since $1, \theta_1, \dots, \theta_d$ are linearly independent over $\mathbb{Q}$, there is a unique point among them for which $L_{\boldsymbol{\theta}}(\mathbf{x})$ has its least value, and we call this point *the minimal point corresponding to X*.

It is clear that the minimal points are primitive. Moreover, if $\mathbf{x}$ is the minimal point corresponding both to X' and to X'', it is also the minimal point corresponding to any X between X' and X''. Hence there is a sequence of integers $X_1 < X_2 < \dots$ such that the same minimal point $\mathbf{x}_i$ corresponds to all X in the range $X_i \le X < X_{i+1}$ but to no X outside this range.

So for fixed $\boldsymbol{\theta}$, the sequences of minimal points $(\mathbf{x}_i)_{i\in\mathbb{N}}$ are uniquely determined up to the choice of their first points.

Now fix such a sequence $(\mathbf{x}_i)_{i\in\mathbb{N}}$. Then $(\mathbf{x}_i)_{i\in\mathbb{N}}$ has the following properties

(a) $\mathbf{x}_i$ is primitive for each i,

(b) the norms $X_i = \|\mathbf{x}_i\|$ form a strictly increasing sequence,

(c) the positive real numbers $L_i = L_{\boldsymbol{\theta}}(\mathbf{x}_i)$ form a strictly decreasing sequence,

(d) if a non-zero point $\mathbf{x} \in \mathbb{Z}^{d+1}$ satisfies $L_{\boldsymbol{\theta}}(\mathbf{x}) < L_i$ for some $i \geq 1$ then $\|\mathbf{x}\| \geq X_{i+1}$.

The following lemma shows that one can compute $\hat{\lambda}(\boldsymbol{\theta})$ directly from a sequence of minimal points.

Lemma 2.2.1. *A positive real number λ is a uniform exponent of approximation to $\boldsymbol{\theta}$ if and only if $L_i \ll X_{i+1}^{-\lambda}$ for each index i.*

Proof. Assume that λ is a uniform exponent of approximation to $\boldsymbol{\theta}$, *i.e.* that there exists a constant $c = c(\theta) > 0$ such that

$$|x_0| \leq X, \quad L_{\boldsymbol{\theta}}(\mathbf{x}) \leq cX^{-\lambda} \tag{2.9}$$

admits a non-zero solution $\mathbf{x} = (x_0, x_1, \ldots, x_d) \in \mathbb{Z}^{d+1}$ for each $X \geq 1$. Then there exists a constant $c' = c'(\boldsymbol{\theta}) > 0$ such that any such solution $\mathbf{x}$ satisfies

$$|x_0| \leq \|\mathbf{x}\| \leq c'|x_0|.$$

Now fix a sufficiently large index i so that $c'^{-1}X_{i+1} > 1$. For any real number X with $1 < X < c'^{-1}X_{i+1}$, a solution $\mathbf{x} \in \mathbb{Z}^{d+1}$ to (2.9) satisfies

$$\|\mathbf{x}\| \leq c'|x_0| < X_{i+1}, \quad L_{\boldsymbol{\theta}}(\mathbf{x}) \leq cX^{-\lambda}.$$

From the property (d), we deduce that

$$L_i \leq L_{\boldsymbol{\theta}}(\mathbf{x}) \leq cX^{-\lambda}.$$

Since we can choose X arbitrarily close to $c'^{-1}X_{i+1}$, we conclude that

$$L_i \leq c(c'^{-1}X_{i+1})^{-\lambda}.$$

The reverse implication is easy to prove. $\square$

We also note that, any two consecutive minimal points $\mathbf{x}_i, \mathbf{x}_{i+1}$ are $\mathbb{Q}$-linearly independent since they are primitive and distinct with positive first coordinates. We have the following estimate for the height of the vector spaces generated by two such points.

Lemma 2.2.2. *Let V_i be the $\mathbb{R}$-vector space generated by $\mathbf{x}_i$ and $\mathbf{x}_{i+1}$. Then, we have $V_i \cap \mathbb{Z}^{d+1} = \langle \mathbf{x}_i, \mathbf{x}_{i+1} \rangle_{\mathbb{Z}}$ and $H(V_i) \asymp X_{i+1} L_i$.*

Proof. Assume that $V_i \cap \mathbb{Z}^{d+1} \neq \langle \mathbf{x}_i, \mathbf{x}_{i+1} \rangle_{\mathbb{Z}}$. Then there exist $r,\ r' \in \mathbb{R}$ with $|r|, |r'| \leq \frac{1}{2}$ such that

$$\mathbf{z} = r\mathbf{x}_i + r'\mathbf{x}_{i+1} \in \mathbb{Z}^{d+1} \setminus \{0\}.$$

So we get

$$\|\mathbf{z}\| \leq |r|\|\mathbf{x}_i\| + |r'|\|\mathbf{x}_{i+1}\| < X_{i+1},$$

$$L_{\boldsymbol{\theta}}(\mathbf{z}) \leq |r|L_i + |r'|L_{i+1} < L_i.$$

This is a contradiction.

So $V_i \cap \mathbb{Z}^{d+1} = \langle \mathbf{x}_i, \mathbf{x}_{i+1} \rangle_{\mathbb{Z}}$ and thus

$$H(V_i) = \|\mathbf{x}_i \wedge \mathbf{x}_{i+1}\| \asymp X_{i+1} L_i.$$

Indeed, it is obvious that $\|\mathbf{x}_i \wedge \mathbf{x}_{i+1}\| \ll X_{i+1} L_i$. We will clarify that

$$\|\mathbf{x}_i \wedge \mathbf{x}_{i+1}\| \gg X_{i+1} L_i. \tag{2.10}$$

Set $\mathbf{u} = \mathbf{x}_i - x_{i,0}\boldsymbol{\theta}$ and $\mathbf{v} = \mathbf{x}_{i+1} - x_{i+1,0}\boldsymbol{\theta}$. Write $\mathbf{u} = (u_0, \ldots, u_d)$ and $\mathbf{v} = (v_0, \ldots, v_d)$. Then $L_i = |u_t|$ for some positive integer $1 \leq t \leq d$. Moreover, there exists $0 \leq l \leq d$ such that $|u_l - v_l| = \|\mathbf{u} - \mathbf{v}\| = L_{\boldsymbol{\theta}}(\mathbf{x}_{i+1} - \mathbf{x}_i) \geq L_i$ since $\|\mathbf{x}_{i+1} - \mathbf{x}_i\| < X_{i+1}$. We have

$$\|\mathbf{x}_i \wedge \mathbf{x}_{i+1}\| \geq |x_{i,0} v_t - x_{i+1,0} u_t| \geq x_{i+1,0} L_i - x_{i,0} L_{i+1} \geq (x_{i+1,0} - x_{i,0}) L_i.$$

In the other hand, we have

$$\begin{aligned} \|\mathbf{x}_i \wedge \mathbf{x}_{i+1}\| &\geq |x_{i,0} v_l - x_{i+1,0} u_l| = |x_{i,0}(v_l - u_l) + u_l(x_{i,0} - x_{i+1,0})| \\ &\geq x_{i,0} L_i - L_i(x_{i+1,0} - x_{i,0}). \end{aligned}$$

This yields

$$3\|\mathbf{x}_i \wedge \mathbf{x}_{i+1}\| \geq x_{i,0} L_i + (x_{i+1,0} - x_{i,0}) L_i = x_{i+1,0} L_i.$$

so we get (2.10). □

In the proof of Theorem 2.1.3, we will need another property of the above sequence of vector spaces $(V_i)_{i\in\mathbb{N}}$. We state it below in a very general form.

Lemma 2.2.3. *Let $(V_i)_{i\in\mathbb{N}}$ be a sequence of subspaces of $\mathbb{R}^{d+1}$ of dimension $t \le d$ defined over $\mathbb{Q}$. Suppose that the union of these spaces contains a sequence of non-zero points $(\mathbf{y}_i)_{i\in\mathbb{N}}$ in $\mathbb{R}^{d+1}$ converging to $\boldsymbol{\theta} = (1, \theta_1, \dots, \theta_d)$ projectively. Then the sequence $(V_i)_{i\in\mathbb{N}}$ contains infinitely many distinct vector spaces.*

Proof. Assume by contradiction that there exist only finitely many distinct vector spaces among the sequence $(V_i)_{i\in\mathbb{N}}$. Then there exists one of them V_{i_0} containing an infinite subsequence $(\mathbf{z}_n)_{n\in\mathbb{N}}$ of $(\mathbf{y}_i)_{i\in\mathbb{N}}$. Since $(\mathbf{y}_i)_{i\in\mathbb{N}}$ converges to $\boldsymbol{\theta}$ projectively, so does any of its subsequences. We deduce that $\boldsymbol{\theta} \in V_{i_0}$.

Since the vector space V_{i_0} is defined over $\mathbb{Q}$ and $\dim V_{i_0} \le d$, there exists a non-zero vector $u = (u_0, \dots, u_d) \in \mathbb{Q}^{d+1}$ orthogonal to V_{i_0}. So it is also orthogonal to $\boldsymbol{\theta}$. Then we have

$$u_0 + u_1\theta_1 + \cdots + u_d\theta_d = 0.$$

This contradicts the hypothesis that $1, \theta_1, \dots, \theta_d$ are linearly independent over $\mathbb{Q}$. □

For the last result of this section, we drop the condition that $\boldsymbol{\theta} = (1, \theta_1, \dots, \theta_d)$ has $\mathbb{Q}-$linearly independent coordinates. In fact, this result provides a criterion for the coordinates of $\boldsymbol{\theta}$ to be linearly independent over $\mathbb{Q}$.

Lemma 2.2.4. *Let $\boldsymbol{\theta} = (1, \theta_1, \dots, \theta_d)$ be an arbitrary point in $\mathbb{R}^{d+1}$. Assume that there exists a sequence of points $\mathbf{y}_n = (y_{n,0}, \dots, y_{n,d})$ in $\mathbb{Z}^{d+1}$ with $n \in \mathbb{N}^*$ such that*

(i) $\det(\mathbf{y}_n, \mathbf{y}_{n+1}, \dots, \mathbf{y}_{n+d}) \neq 0$ *for infinitely many integers n,*

(ii) $\lim_{n\to\infty} L_{\boldsymbol{\theta}}(\mathbf{y}_n) = 0$.

Then $1, \theta_1, \dots, \theta_d$ are $\mathbb{Q}$–linearly independent.

Proof. Assume on the contrary that $1, \theta_1, \dots, \theta_d$ are $\mathbb{Q}$–linearly dependent. WLOG, we may write $\theta_d = a_0 + a_1\theta_1 + \ldots + a_{d-1}\theta_{d-1}$ for some $a_0, a_1, \dots, a_{d-1}$ in $\mathbb{Q}$.

For each $n \in \mathbb{N}$, we have

$$\begin{aligned} x_{n,0}\theta_d - x_{n,d} &= x_{n,0}(a_0 + a_1\theta_1 + \cdots + a_{d-1}\theta_{d-1}) - x_{n,d} \\ &= a_1(x_{n,0}\theta_1 - x_{n,1}) + \cdots + a_{d-1}(x_{n,0}\theta_{d-1} - x_{n,d-1}) + R(n) \end{aligned}$$

where

$$R(n) = a_0x_{n,0} + a_1x_{n,1} + \cdots + a_{d-1}x_{n,d-1} - x_{n,d}.$$

Then we get

$$\begin{aligned} |R(n)| &\leq |x_{n,0}\theta_d - x_{n,d}| + |a_1(x_{n,0}\theta_1 - x_{n,1})| + \cdots + |a_{d-1}(x_{n,0}\theta_{d-1} - x_{n,d-1})| \\ &\ll L_{\boldsymbol{\theta}}(\mathbf{x}_n). \end{aligned}$$

Since $L_{\boldsymbol{\theta}}(\mathbf{x}_n)$ converges to 0 when n tends to infinity, so does $R(n)$. Since $R(n) \in \mathbb{Z}[a_0, a_1, \ldots, a_{d-1}]$ with $a_i \in \mathbb{Q}$ for all $i = 1, \ldots, d-1$, we deduce that $R(n) = 0$, namely

$$x_{n,d} = a_0x_{n,0} + a_1x_{n,1} + \cdots + a_{d-1}x_{n,d-1},$$

when n is sufficiently large. This implies that $\det(\mathbf{x}_n, \mathbf{x}_{n+1}, \mathbf{x}_{n+2}, \mathbf{x}_{n+3}) = 0$ when n is sufficiently large. This is a contradiction. So $1, \theta_1, \ldots, \theta_d$ are $\mathbb{Q}$–linearly independent. □

2.3 Construction of sequences of vector spaces

In this section, we fix a point of $\boldsymbol{\theta} = (1, \theta_1, \ldots, \theta_d) \in \mathbb{R}^{d+1}$ with $\mathbb{Q}$-linearly independent coordinates and fix a sequence of minimal points $(\mathbf{x}_i)_{i\geq 1}$ attached to $\boldsymbol{\theta}$. Let the notation X_i and L_i be as in Section 2.2.

Let i_0 be a positive integer. For each $t = 1, \ldots, d-1$, we denote by i_t the largest integer such that

$$\dim\langle \mathbf{x}_{i_0}, \mathbf{x}_{i_0+1}, \ldots, \mathbf{x}_{i_t} \rangle_{\mathbb{R}} = t + 1. \tag{2.11}$$

The existence of i_t follows from Lemma 2.2.3. Clearly, the property (2.11) also holds for $t = 0$. Moreover, we have

(i) $i_0 < i_1 < \ldots < i_{d-1}$,

(ii) $\dim\langle \mathbf{x}_{i_0}, \mathbf{x}_{i_0+1}, \ldots, \mathbf{x}_{i_t+1}\rangle_{\mathbb{R}} = t+2$ for $0 \le t \le d-1$,

(iii) $\mathbf{x}_{i_t+1} \notin \langle \mathbf{x}_{i_0}, \mathbf{x}_{i_0+1}, \ldots, \mathbf{x}_{i_t}\rangle_{\mathbb{R}}$ for $0 \le t \le d-1$.

By comparing dimensions, we deduce that

(iv) $\mathbb{R}^{d+1} = \langle \mathbf{x}_{i_0}, \mathbf{x}_{i_0+1}, \ldots, \mathbf{x}_{i_{d-1}+1}\rangle_{\mathbb{R}}$,

(v) $\langle \mathbf{x}_{i_0}, \mathbf{x}_{i_0+1}, \ldots, \mathbf{x}_{i_{t-1}+1}\rangle_{\mathbb{R}} = \langle \mathbf{x}_{i_0}, \mathbf{x}_{i_0+1}, \ldots, \mathbf{x}_{i_t}\rangle_{\mathbb{R}}$ for $0 < t \le d-1$.

For each $(t,k) \in \mathbb{N}^2$ with $0 \le t \le d-1$ and $1 \le k \le t+1$, let $s(t,k)$ be the largest integer $< i_t + 1$ such that

$$\dim\langle \mathbf{x}_{s(t,k)}, \mathbf{x}_{s(t,k)+1}, \ldots, \mathbf{x}_{i_t+1}\rangle_{\mathbb{R}} = k+1.$$

Then we get

$$s(t,1) = i_t > s(t,2) > \ldots > s(t,t+1) \ge i_0$$

Now we set

$$\begin{aligned} V_t^{k+1} &= \langle \mathbf{x}_{s(t,k)}, \mathbf{x}_{s(t,k)+1}, \ldots, \mathbf{x}_{i_t+1}\rangle_{\mathbb{R}}, \\ U_t^{k} &= \langle \mathbf{x}_{s(t,k)}, \mathbf{x}_{s(t,k)+1}, \ldots, \mathbf{x}_{i_t}\rangle_{\mathbb{R}}. \end{aligned}$$

By definition, we have

$$\dim V_t^{k+1} = k+1, \qquad U_t^k \subset V_t^{k+1}.$$

Moreover, for such (t,k), we have $U_t^k \subset \langle \mathbf{x}_{i_0}, \mathbf{x}_{i_0+1}, \ldots, \mathbf{x}_{i_t}\rangle_{\mathbb{R}}$. It follows from (iii) that $\mathbf{x}_{i_t+1} \notin U_t^k$. We deduce that

$$\dim U_t^k = k.$$

On the other hand, we have $\mathbf{x}_{i_t+1} \in V_t^k$ by the definition. Thus,

$$V_t^{k+1} = U_t^k + V_t^k \tag{2.12}$$

is the sum of two distinct k-dimensional vector spaces.

For $0 < t \leq d-1$ and $2 \leq k \leq t+1$, it is clear from the definition that U_t^{k-1} is a $(k-1)$-dimensional subspace of the two distinct k-dimensional vector spaces U_t^k and V_t^k. Hence, for such (t,k), we have

$$U_t^{k-1} = U_t^k \cap V_t^k. \tag{2.13}$$

For $t \geq 1$, note that U_t^{t+1} is by definition a $(t+1)$-dimensional subspace of $\langle \mathbf{x}_{i_0}, \mathbf{x}_{i_0+1}, \ldots \mathbf{x}_{i_t} \rangle_{\mathbb{R}}$. Since the latter has dimension $t+1$ by the choice of i_t, they coincide. Similarly, V_{t-1}^{t+1} is a $(t+1)$–dimensional subspace of $\langle \mathbf{x}_{i_0}, \mathbf{x}_{i_0+1}, \ldots, \mathbf{x}_{i_{t-1}+1} \rangle_{\mathbb{R}} = \langle \mathbf{x}_{i_0}, \mathbf{x}_{i_0+1}, \ldots, \mathbf{x}_{i_t} \rangle_{\mathbb{R}}$ so they coincide. Hence we have

$$U_t^{t+1} = \langle \mathbf{x}_{i_0}, \mathbf{x}_{i_0+1}, \ldots, \mathbf{x}_{i_{t-1}+1} \rangle_{\mathbb{R}} = V_{t-1}^{t+1}. \tag{2.14}$$

The following lemma relates the heights of $(U_j^k)_{k \leq j \leq d-1}$ and of $(V_j^{k+1})_{k-1 \leq j \leq d-1}$.

Lemma 2.3.1. *For each $k \in \mathbb{N}$ with $1 \leq k \leq d-1$, we have*

$$H(U_k^k)H(U_{k+1}^k)\cdots H(U_{d-1}^k) \ll H(V_{k-1}^{k+1})H(V_k^{k+1})\cdots H(V_{d-1}^{k+1}) \tag{2.15}$$

Proof. We proceed by descending induction on k.

By (iv), (2.12), and (2.14), we get

$$\mathbb{R}^{d+1} = V_{d-1}^{d+1} = U_{d-1}^d + V_{d-1}^d.$$

By (2.13), we have

$$U_{d-1}^{d-1} = U_{d-1}^d \cap V_{d-1}^d.$$

So it follows from Schmidt's inequality [24, Chap. 1, Lemma 8A] that

$$H(U_{d-1}^{d-1}) \ll H(U_{d-1}^d)H(V_{d-1}^d).$$

By (2.14), we have $H(U_{d-1}^d) = H(V_{d-2}^d)$. Thus,

$$H(U_{d-1}^{d-1}) \ll H(V_{d-2}^d)H(V_{d-1}^d).$$

So (2.15) holds for $k = d-1$.

Assume that (2.15) is true for some k with $1 < k \leq d-1$. For each index $t = k-1, \ldots, d-1$, by (2.12) and (2.13), we have

$$V_t^{k+1} = U_t^k + V_t^k, \qquad U_t^k \cap V_t^k = U_t^{k-1}.$$

Then, it follows from Schmidt's inequality that

$$H(V_t^{k+1}) \ll \frac{H(U_t^k)H(V_t^k)}{H(U_t^{k-1})}$$

for each $t = k-1, \ldots, d-1$. Combining this with the induction hypothesis, we get

$$H(U_k^k) \cdots H(U_{d-1}^k) \ll \frac{H(U_{k-1}^k)H(V_{k-1}^k)}{H(U_{k-1}^{k-1})} \cdots \frac{H(U_{d-1}^k)H(V_{d-1}^k)}{H(U_{d-1}^{k-1})}.$$

This leads to

$$H(U_{k-1}^{k-1}) \cdots H(U_{d-1}^{k-1}) \ll H(U_{k-1}^k)H(V_{k-1}^k) \cdots H(V_{d-1}^k).$$

By (2.14), we have $U_{k-1}^k = V_{k-2}^k$, we conclude that (2.15) is true with k replaced by $k-1$. By the induction principle, (2.15) is true for all $k = 1, \ldots, d-1$. □

Proposition 2.3.2. *Suppose that $\lambda > 0$ is an exponent of approximation to $\boldsymbol{\theta}$. Then we have*

$$X_{i_1} \cdots X_{i_{d-1}} \ll (X_{i_0+1}X_{i_1+1} \cdots X_{i_{d-1}+1})^{1-\lambda}.$$

Recall that $X_i = \|\mathbf{x}_i\|$ for each $i \geq 1$.

Proof. From the above lemma applied with $k = 1$, we get

$$H(U_1^1)H(U_2^1) \cdots H(U_{d-1}^1) \ll H(V_0^2)H(V_1^2) \cdots H(V_{d-1}^2)$$

where $V_t^2 = \langle \mathbf{x}_{i_t}, \mathbf{x}_{i_t+1} \rangle_{\mathbb{R}}$ and $U_t^1 = \langle \mathbf{x}_{i_t} \rangle_{\mathbb{R}}$ for $t = 0, \ldots, d-1$.

For $t = 0, \ldots, d-1$, we have

$$H(U_t^1) = \|\mathbf{x}_{i_t}\| = X_{i_t}.$$

It follows from Lemma 2.2.1 and Lemma 2.2.2 that

$$H(V_t^2) \asymp \|\mathbf{x}_{i_t} \wedge \mathbf{x}_{i_t+1}\| \asymp X_{i_t+1}L_{i_t} \ll X_{i_t+1}^{1-\lambda}.$$

This yields the required inequality. □

2.4 On the norms of minimal points

In this section, we fix a real number field K of degree $d \geq 2$ with basis $\{1, \theta_1, \dots, \theta_{d-1}\}$ over $\mathbb{Q}$ and fix $\xi \in \mathbb{R} \setminus K$. Set $\boldsymbol{\theta} = (1, \theta_1, \dots, \theta_{d-1}, \xi)$. We work with the two functions $L' : \mathbb{R}^d \longrightarrow \mathbb{R}$ and $L : \mathbb{R}^{d+1} \longrightarrow \mathbb{R}$ defined by

$$L'(\mathbf{y}) = L_{\boldsymbol{\theta}^-}(\mathbf{y}) \quad \text{for each } \mathbf{y} \in \mathbb{R}^d,$$
$$L(\mathbf{x}) = L_{\boldsymbol{\theta}}(\mathbf{x}) \quad \text{for each } \mathbf{x} \in \mathbb{R}^{d+1}.$$

We fix a sequence of minimal points $(\mathbf{x}_i)_{i \in \mathbb{N}}$ attached to $\boldsymbol{\theta}$. By construction, the norms $X_i = \|\mathbf{x}_i\|$ form a strictly increasing sequence while the values $L(\mathbf{x}_i)$ form a strictly decreasing sequence (see Section 2.2).

In this section, we will show that if λ is a uniform exponent of approximation to $\boldsymbol{\theta}$, then there exists a constant $c > 0$ such that

$$X_{i+1} \leq c X_i^{\frac{1}{(d-1)\lambda}} \quad \text{for all } i \in \mathbb{N}. \tag{2.16}$$

To verify this, we first establish the following estimate.

Proposition 2.4.1. *For any* $\mathbf{x} \in \mathbb{Z}^d \setminus \{0\}$, *we have*

$$L'(\mathbf{x}) \gg \|\mathbf{x}\|^{-\frac{1}{d-1}}.$$

Proof. Fix a real number $X \geq 1$. Consider the convex body

$$\mathcal{C}_X : \begin{cases} |x_0 + x_1\theta_1 + \cdots + x_{d-1}\theta_{d-1}| \leq X^{-(d-1)} \\ |x_1|, \dots, |x_{d-1}| \leq X \end{cases}$$

and its polar reciprocal parallelepiped

$$\mathcal{C}_X^* : \begin{cases} |x_0| \leq X^{d-1} \\ \max\limits_{1 \leq i < d} |x_0\theta_i - x_i| \leq X^{-1}. \end{cases}$$

Suppose first that $\nu\,\mathcal{C}_X$ contains a non-zero integer point $\mathbf{x}' = (x'_0, \dots, x'_{d-1})$ in $\mathbb{Z}^d$, for some $\nu > 0$. Then we have

$$\|\mathbf{x}'\| \leq \nu C X \qquad \text{with } C = 1 + |\theta_1| + \cdots + |\theta_{d-1}|.$$

Write

$$y = x'_0 + x'_1\theta_1 + \cdots + x'_{d-1}\theta_{d-1}.$$

Since $1, \theta_1, \ldots, \theta_d$ are $\mathbb{Q}$–linearly independent, we have $y \neq 0$. Upon choosing $m \in \mathbb{N}^*$ such that $m\theta_i \in \mathcal{O}_K$ for $i = 1, \ldots, d-1$, we get $m\,y \in \mathcal{O}_K \setminus \{0\}$ and so $N_{K/\mathbb{Q}}(m\,y) \in \mathbb{Z} \setminus \{0\}$. Let $\sigma_1, \ldots, \sigma_d$ denote the d distinct embeddings of K into $\mathbb{C}$, ordered so that σ_1 is the inclusion of K into $\mathbb{R}$. We find

$$\begin{aligned} |N_{K/\mathbb{Q}}(my)| &= m^d \prod_{i=1}^{d} |x'_0 + x'_1\sigma_i(\theta_1) + \cdots + x'_{d-1}\sigma_i(\theta_{d-1})| \\ &\leq m^d \nu X^{-(d-1)} \prod_{i=2}^{d} (C + |\sigma_i(\theta_1)| + \cdots + |\sigma_i(\theta_{d-1})|)\nu X \\ &\leq (C' m\nu)^d \end{aligned}$$

where $C' = \max_{2\leq i\leq d}(C + |\sigma_i(\theta_1)| + \cdots + |\sigma_i(\theta_{d-1})|)$. Since $N_{K/\mathbb{Q}}(m\mathbf{y}) \in \mathbb{Z} \setminus \{0\}$, we conclude that

$$1 \leq C' m\nu$$

and so $\nu \geq (C'm)^{-1}$. This shows that $\mu_1(\mathcal{C}_X) \geq (C'm)^{-1}$.

By Theorem B.4 in [4, Appendix], we have $\mu_1(\mathcal{C}_X) \cdot \mu_d(\mathcal{C}_X^*) \asymp 1$. This implies that

$$\mu_d(\mathcal{C}_X^*) \ll 1.$$

On the other hand, since $\mathrm{vol}(\mathcal{C}_X^*) = 2^d$, it follows from Minkowski's Second Convex Body Theorem that

$$\frac{1}{d!} \leq \mu_1(\mathcal{C}_X^*) \cdots \mu_d(\mathcal{C}_X^*) \leq 1.$$

Since $\mu_1(\mathcal{C}_X^*) \leq \mu_2(\mathcal{C}_X^*) \leq \cdots \leq \mu_d(\mathcal{C}_X^*)$, we deduce that

$$\mu_1(\mathcal{C}_X^*) \geq \frac{1}{d!\ \mu_d(\mathcal{C}_X^*)^{d-1}} > c$$

for some constant c that is independent of X, with $0 < c < 1$.

Now let $\mathbf{x} = (x_0, \ldots, x_{d-1}) \in \mathbb{Z}^d \setminus \{0\}$. We have

$$|x_0| \leq \|\mathbf{x}\| = cX^{d-1} \quad \text{with } X = (c^{-1}\|\mathbf{x}\|)^{\frac{1}{d-1}}.$$

Since $\mu_1(\mathcal{C}_X^*) > c$, the point $\mathbf{x}$ does not belong to $c\,\mathcal{C}_X^*$ and so

$$L'(\mathbf{x}) > cX^{-1} = c^{\frac{d}{d-1}}\|\mathbf{x}\|^{-\frac{1}{d-1}}. \qquad \square$$

Corollary 2.4.2. *Let $\lambda \in \mathbb{R}^+$ be a uniform exponent of approximation to $\boldsymbol{\theta}$. We have*

$$X_{i+1} \ll X_i^{\frac{1}{(d-1)\lambda}} \quad \textit{for all} \ \ i \in \mathbb{N}.$$

Proof. Fix an index i. Applying the above proposition to a minimal point $\mathbf{x}_i$, we get

$$L(\mathbf{x}_i) \geq L'(\mathbf{x}_i^-) \gg \|\mathbf{x}_i^-\|^{-\frac{1}{d-1}} \geq X_i^{-\frac{1}{d-1}}.$$

From Lemma 2.2.1, we have $L(\mathbf{x}_i) \ll X_{i+1}^{-\lambda}$. Thus we get

$$X_i^{-\frac{1}{d-1}} \ll X_{i+1}^{-\lambda},$$

from which the result follows. $\square$

The previous corollary provides a constraint on the norms of $(\mathbf{x}_i)_{i\in\mathbb{N}}$ which holds for any uniform exponent λ of approximation to $\boldsymbol{\theta}$. In the special case where $\lambda = \lambda_d$ is assumed to be an exponent of approximation to $\boldsymbol{\theta}$, we have the following result.

Theorem 2.4.3. *Let the notation be as in Theorem 2.1.3. Assume that λ_d is a uniform exponent of approximation to $\boldsymbol{\theta} = (1, \theta_1, \dots, \theta_{d-1}, \xi)$. Let $(\mathbf{x}_i)_{i\in\mathbb{N}}$ be a sequence of minimal points attached to $\boldsymbol{\theta}$. Then this sequence admits a subsequence $(\mathbf{y}_n)_{n\in\mathbb{N}^*}$ such that, for each $n \in \mathbb{N}$,*

(i) $|\det(\mathbf{y}_n, \mathbf{y}_{n+1}, \dots, \mathbf{y}_{n+d})| \asymp 1$,

(ii) $\|\mathbf{y}_n\| \asymp \|\mathbf{y}_{n+1}\|^{(d-1)\lambda_d}$,

(iii) $L(\mathbf{y}_n) \asymp L'(\mathbf{y}_n^-) \asymp \|\mathbf{y}_n\|^{-1/(d-1)}$.

This is a consequence of Theorem 2.1.3 and will be proved in the next section.

2.5 Proof of the main theorems

2.5.1 Proof of Theorem 2.1.3

Fix a sequence of minimal points $(\mathbf{x}_i)_{i\geq 1}$ in $\mathbb{Z}^{d-1}$ attached to $\boldsymbol{\theta} = (1, \theta_1, \theta_2, \dots, \theta_{d-1}, \xi)$. For each $i \geq 1$, we define $X_i = \|\mathbf{x}_i\|$ and $L_i = L_{\boldsymbol{\theta}}(\mathbf{x}_i)$ according to the general convention explained in Section 2.2.

Fix an arbitrary large integer i_0. For each $t = 1, \ldots, d-1$, we denote by i_t the largest integer $\geq i_0$ such that

$$\dim\langle \mathbf{x}_{i_0}, \mathbf{x}_{i_0+1}, \ldots, \mathbf{x}_{i_t} \rangle_{\mathbb{R}} = t + 1.$$

By Proposition 2.3.2, we get

$$X_{i_1} \cdots X_{i_{d-1}} \ll (X_{i_0+1} X_{i_1+1} \cdots X_{i_{d-1}+1})^{1-\lambda}.$$

The idea is to eliminate successively $X_{i_0+1}, X_{i_1}, X_{i_1+1}, X_{i_2}, \ldots$ from this equality.

Since $i_0 + 1 \leq i_1$, we first have $X_{i_0+1} \leq X_{i_1}$, hence the above inequality implies that

$$X_{i_1} \cdots X_{i_{d-1}} \ll (X_{i_1} X_{i_1+1} \cdots X_{i_{d-1}+1})^{1-\lambda} \tag{2.17}$$

which is equivalent to

$$X_{i_1}^{\lambda} X_{i_2} \cdots X_{i_{d-1}} \ll (X_{i_1+1} \cdots X_{i_{d-1}+1})^{1-\lambda}.$$

By Corollary 2.4.2, we have $X_{i_1} \gg X_{i_1+1}^{(d-1)\lambda}$. Using this to eliminate X_{i_1}, we get

$$X_{i_1+1}^{(d-1)\lambda^2} X_{i_2} \cdots X_{i_{d-1}} \ll (X_{i_1+1} \cdots X_{i_{d-1}+1})^{1-\lambda}. \tag{2.18}$$

Assume that

$$X_{i_{t-1}+1}^{(d-1)\lambda^2+\cdots+(d-1)^{t-1}\lambda^t} X_{i_t} \cdots X_{i_{d-1}} \ll (X_{i_{t-1}+1} \cdots X_{i_{d-1}+1})^{1-\lambda} \tag{2.19}$$

for some t with $1 < t < d$. We just proved (2.19) for $t = 2$. We will prove that (2.19) still holds when we replace t by $t + 1$.

The inequality (2.19) is equivalent to

$$X_{i_{t-1}+1}^{-1+\lambda+(d-1)\lambda^2+\cdots+(d-1)^{t-1}\lambda^t} X_{i_t} \cdots X_{i_{d-1}} \ll (X_{i_t+1} \cdots X_{i_{d-1}+1})^{1-\lambda}. \tag{2.20}$$

Upon noting that $\lambda \leq \hat{\lambda}(\boldsymbol{\theta}^-) = \dfrac{1}{d-1}$ (by Lemmas 2.1.1 and 2.1.2), we get

$$-1 + \lambda + (d-1)\lambda^2 + \cdots + (d-1)^{t-1}\lambda^t \leq -1 + \frac{t}{d-1} \leq 0. \tag{2.21}$$

So we can use the inequality $X_{i_{t-1}+1} \leq X_{i_t}$ to eliminate $X_{i_{t-1}+1}$ from (2.20). This gives

$$X_{i_t}^{\lambda+(d-1)\lambda^2+\cdots+(d-1)^{t-1}\lambda^t} X_{i_{t+1}} \cdots X_{i_{d-1}} \ll (X_{i_t+1} \cdots X_{i_{d-1}+1})^{1-\lambda}$$

Since $X_{i_t} \gg X_{i_t+1}^{(d-1)\lambda}$, we obtain

$$X_{i_t+1}^{(d-1)\lambda^2+\cdots+(d-1)^t\lambda^{t+1}} X_{i_{t+1}} \cdots X_{i_{d-1}} \ll (X_{i_t+1} \cdots X_{i_{d-1}+1})^{1-\lambda}$$

as required. By the induction principle, we deduce that the inequality (2.19) holds for all $t = 2, \dots, d$. Applying (2.19) with $t = d$, we get

$$X_{i_{d-1}+1}^{(d-1)\lambda^2+\cdots+(d-1)^{d-1}\lambda^d} \ll X_{i_{d-1}+1}^{1-\lambda} \tag{2.22}$$

This implies that λ satisfies

$$\lambda + (d-1)\lambda^2 + \cdots + (d-1)^{d-1}\lambda^d \leq 1.$$

Since $f(\lambda) = \lambda + (d-1)\lambda^2 + \cdots + (d-1)^{d-1}\lambda^d$ is an increasing function on $\mathbb{R}^+$, we deduce that $\lambda \leq \lambda_d$.

2.5.2 Proof of Theorem 2.4.3

Note that if there exists a subsequence $(\mathbf{y}_n)_{n\in\mathbb{N}^*}$ of $(\mathbf{x}_i)_{i\in\mathbb{N}}$ in which any $d+1$ consecutive points are linearly independent and if this sequence satisfies the properties (ii), (iii) of Theorem 2.4.3 for any $n \in \mathbb{N}$ then we have

$$\begin{aligned} 1 \leq |\det(\mathbf{y}_n, \mathbf{y}_{n+1}, \dots, \mathbf{y}_{n+d})| &\ll \|\mathbf{y}_{n+d}\| L(\mathbf{y}_n) \cdots L(\mathbf{y}_{n+d-1}) \\ &\ll \|\mathbf{y}_{n+d}\|^{1-\lambda_d-(d-1)\lambda_d^2-\cdots-(d-1)^{d-1}\lambda_d^d} = 1, \end{aligned}$$

so the property (i) holds.

Therefore it is enough to establish the existence of a subsequence $(\mathbf{y}_n)_{n\in\mathbb{N}}$ in which any $d+1$ consecutive points are linearly independent and for which the properties (ii) and (iii) hold. We start with two general observations.

a) Consider an arbitrarily large integer i. For each $t = 0, \dots, d-1$, let i_t be the largest integer $\geq i$ such that

$$\dim\langle \mathbf{x}_i, \mathbf{x}_{i+1}, \dots, \mathbf{x}_{i_t}\rangle_{\mathbb{R}} = t+1.$$

In particular, we note that $i_0 = i$. We will show that

$$X_{i_{t-1}+1} \asymp X_{i_t} \asymp X_{i_t+1}^{(d-1)\lambda_d}, \quad L(\mathbf{x}_{i_t}) \asymp L(\mathbf{x}_{i_t}^-) \asymp X_{i_t}^{-\frac{1}{d-1}} \tag{2.23}$$

for $t = 1, \dots, d-1$.

To this end, consider the proof of Theorem 2.1.3. In our case where $\lambda = \lambda_d$, we get an equality in (2.22). Therefore, throughout the proof, we can replace all symbols $\ll$ and $\gg$ by $\asymp$. Otherwise, if in some inequality, one side is much larger than the other, this would carry to all subsequent estimates, and so we could not have an equality in (2.22). This uses the fact that for $\lambda = \lambda_d$, the first inequality in (2.21) is strict for $t = 1, \dots, d-1$. We conclude that

$$X_{i_{t-1}+1} \asymp X_{i_t} \asymp X_{i_t+1}^{(d-1)\lambda_d} \quad \text{for all } t = 1, \dots, d-1 \tag{2.24}$$

where the implied constants do not depend on the choice of i made at the beginning of Step 1.

Since $(d-1)\lambda_d < 1$, this means that, for each $t = 1, \dots, d-1$, the numbers $X_{i_{t-1}+1}, X_{i_{t-1}+2}, \dots, X_{i_t}$ are about the same size while X_{i_t+1} is much larger. More precisely, there exists a constant $c > 1$, independent of the choice of i, such that, if i is large enough, then

$$\begin{aligned} i_1 &= \min\{k \in \mathbb{N};\ \ k > i_0,\ X_{k+1} > cX_k\}, \\ i_2 &= \min\{k \in \mathbb{N};\ \ k > i_1,\ X_{k+1} > cX_k\}, \\ &\cdots \\ i_{d-1} &= \min\{k \in \mathbb{N};\ \ k > i_{d-2},\ X_{k+1} > cX_k\}. \end{aligned} \tag{2.25}$$

Moreover, going back to the proof of Corollary 2.4.2, the estimates (2.24) imply that

$$L(\mathbf{x}_{i_t}) \asymp L'(\mathbf{x}_{i_t}^-) \asymp X_{i_t}^{-\frac{1}{d-1}}$$

for all $t = 1, \dots, d-1$, where the implied constants are again independent of the choice of the initial integer i.

b) With the above notation, take $j = i_1$. For each $t = 0, \dots, d-1$, let j_t be the largest integer such that

$$\dim\langle \mathbf{x}_j, \mathbf{x}_{j+1}, \dots, \mathbf{x}_{j_t}\rangle_{\mathbb{R}} = t+1.$$

We will show that $j_t = i_{t+1}$ for $t = 0, \dots, d-2$ provided that i is large enough. This is true for $t = 0$ since $j_0 = j = i_1$. Assume that $j_0 = i_1, \dots, j_{t-1} = i_t$ for some t with $1 \le t < d-1$. By part a) and the induction hypothesis, we have

$$\begin{aligned} j_t &= \min\{k \in \mathbb{N};\quad k > j_{t-1},\ X_{k+1} > cX_k\} \\ &= \min\{k \in \mathbb{N};\quad k > i_t,\ X_{k+1} > cX_k\}, \end{aligned}$$

and so $j_t = i_{t+1}$. By the induction principle, we get

$$j_t = i_{t+1} \qquad \text{for } \ t = 0, \dots, d-2.$$

Set $i_d = j_{d-1}$. Then we have

$$\begin{aligned} i_d = j_{d-1} &= \min\{k \in \mathbb{N};\quad k > j_{d-2},\ X_{k+1} > cX_k\} \\ &= \min\{k \in \mathbb{N};\quad k > i_{d-1},\ X_{k+1} > cX_k\}. \end{aligned} \tag{2.26}$$

We claim that the point $\mathbf{x}_{i_0}$ is $\mathbb{R}$–linearly independent from the d points $\mathbf{x}_{i_1}, \mathbf{x}_{i_2}, \dots, \mathbf{x}_{i_d}$. To verify this, we first note that

$$\begin{aligned} \mathbb{R}^{d+1} &= \langle \mathbf{x}_{i_0}, \mathbf{x}_{i_0+1}, \dots, \mathbf{x}_{i_{d-1}+1}\rangle_{\mathbb{R}} \\ &= \langle \mathbf{x}_{i_0}, \mathbf{x}_{i_0+1}, \dots, \mathbf{x}_{i_1}\rangle_{\mathbb{R}} + \langle \mathbf{x}_{i_1}, \mathbf{x}_{i_1+1}, \dots, \mathbf{x}_{i_{d-1}+1}\rangle_{\mathbb{R}}. \end{aligned}$$

Since $\langle \mathbf{x}_{i_0}, \mathbf{x}_{i_0+1}, \dots, \mathbf{x}_{i_1}\rangle_{\mathbb{R}}$ has dimension 2, and since the two points $\mathbf{x}_{i_0}, \mathbf{x}_{i_1}$ are primitive with unequal norms, we get

$$\langle \mathbf{x}_{i_0}, \mathbf{x}_{i_0+1}, \dots, \mathbf{x}_{i_1}\rangle_{\mathbb{R}} = \langle \mathbf{x}_{i_0}, \mathbf{x}_{i_1}\rangle_{\mathbb{R}}.$$

Moreover, since $i_{t+1} = j_t$ for all $t = 0, \dots, d-1$, we also have

$$\langle \mathbf{x}_{i_1}, \mathbf{x}_{i_1+1}, \dots, \mathbf{x}_{i_{d-1}+1}\rangle_{\mathbb{R}} = \langle \mathbf{x}_{j_0}, \mathbf{x}_{j_0+1}, \dots, \mathbf{x}_{j_{d-2}+1}\rangle_{\mathbb{R}}.$$

By definition of j_{d-2}, this vector space has dimension d. By definition of j_{d-1}, we also have

$$\begin{aligned}\langle \mathbf{x}_{j_0}, \mathbf{x}_{j_0+1}, \dots, \mathbf{x}_{j_{d-2}+1}\rangle_{\mathbb{R}} &= \langle \mathbf{x}_{j_0}, \mathbf{x}_{j_0+1}, \dots, \mathbf{x}_{j_{d-1}}\rangle_{\mathbb{R}} \\ &= \langle \mathbf{x}_{i_1}, \mathbf{x}_{i_1+1}, \dots, \mathbf{x}_{i_d}\rangle_{\mathbb{R}}.\end{aligned}$$

Therefore, the $(d+1)$–dimensional vector space

$$\begin{aligned}\mathbb{R}^{d+1} &= \langle \mathbf{x}_{i_0}, \mathbf{x}_{i_1}\rangle_{\mathbb{R}} + \langle \mathbf{x}_{i_1}, \mathbf{x}_{i_1+1}, \dots, \mathbf{x}_{i_d}\rangle_{\mathbb{R}} \\ &= \langle \mathbf{x}_{i_0}\rangle_{\mathbb{R}} + \langle \mathbf{x}_{i_1}, \mathbf{x}_{i_1+1}, \dots, \mathbf{x}_{i_d}\rangle_{\mathbb{R}}\end{aligned}$$

is the sum of a 1-dimensional vector space and a d–dimensional vector space. We deduce that $\mathbf{x}_{i_0} \notin \langle \mathbf{x}_{i_1}, \mathbf{x}_{i_1+1}, \dots, \mathbf{x}_{i_d}\rangle_{\mathbb{R}}$. A fortiori, this proves the claim.

c) **Construction of $(\mathbf{y}_n)_{n\in\mathbb{N}}$:** Let the constant c be as in part a), and let $k_0 \in \mathbb{N}$ be sufficiently large so that (2.25) holds for any choice of i with $i \geq k_0$. Define recursively an increasing sequence of integers $(k_n)_{n\in\mathbb{N}}$ by

$$k_{n+1} = \min\{k \in \mathbb{N};\quad k > k_n,\ X_{k+1} > cX_k\},$$

and put

$$\mathbf{y}_n = \mathbf{x}_{k_n}$$

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

If we apply the construction of parts a) and b) with $i = k_n$ for some $n \geq 0$, then the integers $i_0, i_1, \dots, i_d$ become $k_n, k_{n+1}, \dots, k_{n+d}$ because of (2.25) and (2.26). Note that the estimates (2.23) of part a) not only hold for $t = 1, \dots, d-1$, but also for $t = d$ because of the construction of i_d in part b). Considering the cases $t = 1$ and $t = 2$, we have

$$X_{k_{n+1}} \asymp X_{k_{n+1}+1}^{(d-1)\lambda}, \quad X_{k_{n+1}+1} \asymp X_{k_{n+2}},$$

and

$$L(\mathbf{x}_{k_{n+1}}) \asymp L'(\mathbf{x}_{k_{n+1}}^-) \asymp X_{k_{n+1}}^{-1/(d-1)}.$$

So we have

$$\|\mathbf{y}_{n+1}\| \asymp \|\mathbf{y}_{n+2}\|^{(d-1)\lambda_d}, \quad L(\mathbf{y}_{n+1}) \asymp L'(\mathbf{y}_{n+1}^-) \asymp \|\mathbf{y}_{n+1}\|^{-1/(d-1)}$$

for all $n \geq 0$, showing that the sequence $(\mathbf{y}_n)_{n\in\mathbb{N}^*}$ fulfills the properties (ii) and (iii) of Theorem 2.4.3.

Finally, if we again choose $i = k_n$ in part a), then the main result of part b) states that $\mathbf{y}_n$ is $\mathbb{R}$–linearly independent of the d successors $\mathbf{y}_{n+1}, \mathbf{y}_{n+2}, \ldots, \mathbf{y}_{n+d}$. This being true for all $n \geq 0$, it shows that any $d+1$ consecutive points of the sequence $(\mathbf{y}_n)_{n\in\mathbb{N}}$ are linearly independent. So $(\mathbf{y}_n)_{n\in\mathbb{N}^*}$ fulfills all the required properties.

2.6 The polynomials φ and Φ

Fix a real number field K of degree $d \geq 2$. Then there exists an algebraic integer α of degree d such that $K = \mathbb{Q}(\alpha)$. Then $\{1, \alpha, \ldots, \alpha^{d-1}\}$ is a basis of K over $\mathbb{Q}$. Set $\boldsymbol{\theta} = (1, \alpha, \ldots, \alpha^{d-1})$.

Using geometry of numbers, we proved in Proposition 2.4.1 that for any $\mathbf{x} \in \mathbb{Z}^d$, we have

$$L_{\boldsymbol{\theta}}(\mathbf{x}) \gg \|\mathbf{x}\|^{-\frac{1}{d-1}}. \tag{2.27}$$

In this section, we provide an algebraic proof of this result based on properties of a symmetric d-linear form $\Phi(\mathbf{X}_1, \ldots, \mathbf{X}_d) \in \mathbb{Z}[\mathbf{X}_1, \ldots, \mathbf{X}_d]$ which we will construct below, where $\mathbf{X}_j = (X_{j,0}, \ldots, X_{j,d-1})$ is a $d-$tuple of variables for $j = 1, \ldots, d$.

Firstly, we need an auxiliary lemma.

Lemma 2.6.1. *There exists a unique choice of $a_0, a_1, \ldots, a_{d-1}$ in K with $a_{d-1} = 1$ such that every embedding $\tau : K \hookrightarrow \mathbb{C}$ distinct from the inclusion map satisfies*

$$\tau(a_0) + \tau(a_1)\alpha + \cdots + \tau(a_{d-1})\alpha^{d-1} = 0. \tag{2.28}$$

These numbers $a_0, a_1 \ldots, a_{d-1}$ are $\mathbb{Q}$-linearly independent algebraic integers.

Proof. Let F be a normal closure of K over $\mathbb{Q}$. Set $G = \mathrm{Gal}(F/\mathbb{Q})$ and $H = \mathrm{Gal}(F/K)$. Any embedding τ of K into $\mathbb{C}$ such that $\tau \neq Id_K$ can be extended to an automorphism $\bar{\tau}$ of F and then $\bar{\tau} \in G \setminus H$. Conversely, the restriction to K of any element σ of $G \setminus H$ yields an embedding from K into $\mathbb{C}$ distinct from the inclusion. Therefore, condition (2.28) for all $\tau \neq Id_K$ is equivalent to

$$\sigma(a_0) + \sigma(a_1)\alpha + \cdots + \sigma(a_{d-1})\alpha^{d-1} = 0 \quad \text{for all } \sigma \in G \setminus H. \tag{2.29}$$

Since H is a subgroup of G, we have $\sigma \in G \setminus H$ if and only if $\sigma^{-1} \in G \setminus H$. Applying σ^{-1} to both sides of the equation associated σ, it becomes

$$a_0 + a_1\sigma^{-1}(\alpha) + \cdots + a_{d-1}\sigma^{-1}(\alpha^{d-1}) = 0 \quad \text{for all } \sigma \in G \setminus H,$$

and thus the conditions (2.29) are equivalent to

$$a_0 + a_1\sigma(\alpha) + \cdots + a_{d-1}(\sigma(\alpha))^{d-1} = 0 \quad \text{for all } \sigma \in G \setminus H \tag{2.30}$$

By definition of G and H, the set of numbers $\tau(\alpha)$ with $\tau \in G \setminus H$ consists of all the conjugates of α but α. Therefore, condition (2.30) is equivalent to asking that the polynomial

$$p(T) = a_0 + a_1T + \cdots + a_{d-2}T^{d-2} + T^{d-1}$$

has roots $\alpha_1, \ldots, \alpha_{d-1}$ where $\alpha_1, \ldots, \alpha_{d-1}$ denote all the conjugates of α which are different from α. Namely, it asks that

$$p(T) = (T - \alpha_1)(T - \alpha_2)\cdots(T - \alpha_{d-1}) = \frac{\min(\alpha, \mathbb{Q})}{T - \alpha}. \tag{2.31}$$

Since $\alpha \in \mathcal{O}_K$, we can write

$$\min(\alpha, \mathbb{Q}) = T^d + t_{d-1}T^{d-1} + \cdots + t_0$$

for some integers $t_0, \ldots, t_{d-1}$. Then (2.31) is equivalent to the following equation

$$(T^{d-1} + a_{d-2}T^{d-2} + \cdots + a_0)(T - \alpha) = T^d + t_{d-1}T^{d-1} + \cdots + t_0.$$

By comparing coefficients on both sides, we get

$$t_i = a_{i-1} - a_i\alpha \qquad \text{for } \; i = 1, \ldots, d-1,$$

and so

$$\begin{aligned} a_{d-2} &= t_{d-1} + \alpha, \\ a_{d-3} &= t_{d-2} + a_{d-2}\alpha = t_{d-2} + t_{d-1}\alpha + \alpha^2, \\ &\cdots \\ a_0 &= t_1 + t_2\alpha + \cdots + \alpha^{d-1}. \end{aligned} \tag{2.32}$$

This proves the existence and unicity of $a_0, \dots, a_{d-1}$ in $\mathbb{Q}(\alpha)$ satisfying (2.28). Since $\alpha \in \mathcal{O}_K$ and $t_0, \dots, t_{d-1} \in \mathbb{Z}$, we get $a_i \in \mathcal{O}_K$ for all $i = 0, \dots, d-2$. On the other hand, since α has degree d, the elements $1, \alpha, \dots, \alpha^{d-1}$ form a basis of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$. Moreover, the above formulas show that each a_i with $i = 0, \dots, d-1$ is a monic polynomial in α of degree $d - i - 1$. Hence the elements $a_0, \dots, a_{d-1}$ form another basis of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$. In particular, they are $\mathbb{Q}-$linearly independent. □

Proposition 2.6.2. *Let $a_0, \dots, a_{d-1}$ be as in the above lemma. There exists a symmetric d-linear form $\Phi(\mathbf{X}_1, \dots, \mathbf{X}_d) \in \mathbb{Z}[\mathbf{X}_1, \dots, \mathbf{X}_d]$ such that*

(i) $\Phi(\boldsymbol{\theta}, \boldsymbol{\theta}, \mathbf{X}_3, \dots, \mathbf{X}_d) = 0$,

(ii) the polynomial $\varphi(\mathbf{X}_1) = \frac{1}{d!}\Phi(\mathbf{X}_1, \dots, \mathbf{X}_1)$ *satisfies*

$$\varphi(\mathbf{x}) = N_{K/\mathbb{Q}}(a_0x_0 + \cdots + a_{d-1}x_{d-1}) \in \mathbb{Z} \setminus \{0\}$$

for all $\mathbf{x} = (x_0, \dots, x_{d-1}) \in \mathbb{Z}^d \setminus \{0\}$.

Proof.

(i) Let F be a normal closure of $K/\mathbb{Q}$ and set $G = \mathrm{Gal}(F/\mathbb{Q})$. Then G acts on $F[\mathbf{X}_1, \dots, \mathbf{X}_d]$ by

$$\sigma\left(\sum a_{\mathbf{i}_1,\cdots,\mathbf{i}_d}\mathbf{X}_1^{\mathbf{i}_1}\cdots\mathbf{X}_d^{\mathbf{i}_d}\right) = \sum \sigma(a_{\mathbf{i}_1,\dots,\mathbf{i}_d})\mathbf{X}_1^{\mathbf{i}_1}\cdots\mathbf{X}_d^{\mathbf{i}_d} \qquad \text{for } \sigma \in G,$$

where $\mathbf{X}_j^{\mathbf{i}}$ denotes the monomial $X_{j,0}^{i_0}\cdots X_{j,d-1}^{i_{d-1}}$ for each $\mathbf{i} = (i_0, \dots, i_{d-1}) \in \mathbb{N}^d$.

Let $\tau_1, \dots, \tau_d$ be all the d embeddings of K into $\mathbb{C}$ ordered so that $\tau_d = Id_K$. Set

$$\ell_j(\mathbf{X}) = \tau_j(a_0)X_0 + \cdots + \tau_j(a_{d-1})X_{d-1} \qquad \text{for } j = 1, \dots, d,$$

and set

$$\Phi(\mathbf{X}_1, \dots, \mathbf{X}_d) = \sum_{\nu \in S_d} \ell_{\nu(1)}(\mathbf{X}_1)\cdots\ell_{\nu(d)}(\mathbf{X}_d).$$

It is clear that Φ is a symmetric d-linear form. By the previous lemma, we have $a_i \in \mathcal{O}_K$ for all $i = 0, \dots, d-1$, and so $\Phi \in \mathcal{O}_F[\mathbf{X}_1, \dots, \mathbf{X}_d]$. Moreover, we have $\sigma(\Phi(\mathbf{X}_1, \dots, \mathbf{X}_d)) = \Phi(\mathbf{X}_1, \dots, \mathbf{X}_d)$ for any $\sigma \in G$ since σ permutes $\ell_1, \dots, \ell_d$. We deduce that

$$\Phi \in \mathcal{O}_F^G[\mathbf{X}_1, \dots, \mathbf{X}_d] = \mathbb{Z}[\mathbf{X}_1^{\mathbf{i}_1} \dots \mathbf{X}_d^{\mathbf{i}_d}].$$

By the same lemma, we have $\ell_j(\boldsymbol{\theta}) = 0$ for $j = 1, \dots, d-1$. This implies that

$$\ell_{\nu(1)}(\boldsymbol{\theta}) \cdot \ell_{\nu(2)}(\boldsymbol{\theta}) = 0$$

for all $\nu \in S_d$, so we get (i).

(ii) Since $a_0, \dots, a_{d-1}$ are $\mathbb{Q}$- linearly independent algebraic integers, we have

$$a_0 x_0 + \dots + a_{d-1} x_{d-1} \in \mathcal{O}_K \setminus \{0\}$$

for all $\mathbf{x} = (x_0, \dots, x_{d-1}) \in \mathbb{Z}^d \setminus \{0\}$. For those points, we conclude that

$$\begin{aligned} \varphi(\mathbf{x}) =& \prod_{i=1}^{d} \tau_i(a_0 x_0 + \ldots + a_{d-1} x_{d-1}) \\ =& N_{K/\mathbb{Q}}(a_0 x_0 + \ldots + a_{d-1} x_{d-1}) \end{aligned}$$

is a non-zero integer. □

Now we are able to give an alternative proof of Proposition 2.4.1.

Proof of Proposition 2.4.1. Fix $\mathbf{x} = (x_0, \dots, x_{d-1}) \in \mathbb{Z}^d \setminus \{0\}$ and write this point in the form $\mathbf{x} = x_0\boldsymbol{\theta} + \Delta$ with $\Delta \in \mathbb{R}^d$. Then we have $L_{\boldsymbol{\theta}}(\mathbf{x}) = \|\Delta\|$. With Φ and φ as in Proposition 2.6.2, we find

$$\begin{aligned} \varphi(\mathbf{x}) &= \frac{1}{d!}\Phi(x_0\boldsymbol{\theta} + \Delta, \dots, x_0\boldsymbol{\theta} + \Delta) \\ &= \frac{1}{d!}\big(\Phi(\Delta, \dots, \Delta) + d x_0 \Phi(\boldsymbol{\theta}, \Delta, \dots, \Delta)\big) \end{aligned}$$

since $\Phi(x_0\boldsymbol{\theta}, x_0\boldsymbol{\theta}, \Delta, \dots, \Delta) = x_0^2 \Phi(\boldsymbol{\theta}, \boldsymbol{\theta}, \Delta, \dots, \Delta) = 0$. Since $\varphi(\mathbf{x}) \in \mathbb{Z} \setminus \{0\}$, we conclude that

$$1 \le |\varphi(\mathbf{x})| \ll \|\mathbf{x}\| \cdot L_{\boldsymbol{\theta}}(\mathbf{x})^{d-1} \tag{2.33}$$

and so $L_{\boldsymbol{\theta}}(\mathbf{x}) \gg \|\mathbf{x}\|^{-1/(d-1)}$. □

2.7 The morphism Ψ

As we said before, we don't know if there exists a point $\boldsymbol{\theta} \in \mathbb{R}^{d+1}$ as in Theorem 2.1.3 such that $\hat{\lambda}(\boldsymbol{\theta}) = \lambda_d$. However, if such $\boldsymbol{\theta}$ exists, then there exists a sequence of primitve points $(\mathbf{y}_n)_{n\in\mathbb{N}^*}$ satisfying conditions (i)–(iii) of Theorem 2.4.3 for each $n > 0$. In this section, we construct explicit algebraic relations between the points of such a sequence. We hope that these relations will be useful for further study of this topic.

Let the notation d, K, α, φ and Φ be as in Section 2.6. We fix $\xi \in \mathbb{R} \setminus \mathbb{Q}(\alpha)$ and set $\boldsymbol{\theta} = (1, \alpha, \dots, \alpha^{d-1}, \xi)$.

For any $\mathbf{x}, \mathbf{y} \in \mathbb{R}^{d+1}$, we define

$$\Psi(\mathbf{x}, \mathbf{y}) = \varphi(\mathbf{x}^-)\mathbf{y} - \frac{1}{(d-1)!}\Phi(\mathbf{x}^-, \dots, \mathbf{x}^-, \mathbf{y}^-)\mathbf{x} \qquad \in \mathbb{R}^{d+1}.$$

and set $L(\mathbf{x}) = L_{\boldsymbol{\theta}}(\mathbf{x})$.

Theorem 2.7.1. *Suppose that there exists a sequence of primitive points $(\mathbf{y}_n)_{n\in\mathbb{N}^*}$ satisfying conditions (i)–(iii) of Theorem 2.4.3 for each n. Set $\mathbf{z}_n = \Psi(\mathbf{y}_{n+d}, \mathbf{y}_{n+d+1})$ for each $n \in \mathbb{N}^*$. Then we have*

(i) $(d-1)!\,\mathbf{z}_n \in \mathbb{Z}^{d+1} \setminus \{0\}$ *for each* $n > 0$,

(ii) $\|\mathbf{z}_n\| \ll \|\mathbf{y}_{n+d}\|^{\frac{d-r}{d-1}}, \quad L(\mathbf{z}_n) \ll \|\mathbf{y}_{n+d}\|^{r-\frac{d}{d-1}} \asymp L(\mathbf{y}_i)$ *for each* $n > 0$,

(iii) $\det(\mathbf{y}_n, \mathbf{y}_{n+1}, \dots, \mathbf{y}_{n+d-1}, \Psi(\mathbf{y}_{n+d}, \mathbf{y}_{n+d+1})) = 0$ *when n is sufficiently large.*

Condition (i) of Theorem 2.4.3 implies that any $d+1$ consecutive points of $(\mathbf{y}_n)_{n\in\mathbb{N}^*}$ form a basis of $\mathbb{R}^{d+1}$. Therefore, each point $\mathbf{y}_{n+d+1}$ with $n > 0$ is a linear combination of its $d+1$ predecessors $\mathbf{y}_n, \dots, \mathbf{y}_{n+d}$. The following corollary provides us with the coefficient of $\mathbf{y}_{n+d}$ in such a linear combination.

Corollary 2.7.2. *Let the assumption and the notation be as in the Theorem 2.7.1. We have*

$$\varphi(\mathbf{y}_{n+d}^-)\mathbf{y}_{n+d+1} - \frac{1}{(d-1)!}\Phi(\mathbf{y}_{n+d}^-, \dots, \mathbf{y}_{n+d}^-, \mathbf{y}_{n+d+1}^-)\mathbf{y}_{n+d} \in \langle \mathbf{y}_n, \dots, \mathbf{y}_{n+d-1} \rangle_{\mathbb{R}}.$$

To prove Theorem 2.7.1, we establish the following result.

Proposition 2.7.3. *Let* $\mathbf{x}, \mathbf{y} \in \mathbb{R}^{d+1}$ *such that*

$$L(\mathbf{y}) \leq L(\mathbf{x}) \leq \|\mathbf{x}\| \leq \|\mathbf{y}\|. \tag{2.34}$$

Then we have

(i) $L(\Psi(\mathbf{x}, \mathbf{y})) \ll \|\mathbf{y}\| L(\mathbf{x})^d$,

(ii) $\|\Psi(\mathbf{x}, \mathbf{y})\| \ll \|\mathbf{x}\|^2 L(\mathbf{x})^{d-2} L(\mathbf{y}) + \|\mathbf{y}\| L(\mathbf{x})^d$.

Proof. Write $\mathbf{x}^- = x_0 \boldsymbol{\theta}^- + \Delta\mathbf{x}$. Then we have

$$\|\Delta\mathbf{x}\| \leq L_{\boldsymbol{\theta}^-}(\mathbf{x}^-) \leq L(\mathbf{x}).$$

Similarly, write $\mathbf{y}^- = y_0 \boldsymbol{\theta}^- + \Delta\mathbf{y}$ and so $\|\Delta\mathbf{y}\| \leq L(\mathbf{y})$.

Using the multilinearity of Φ and Proposition 2.6.2 (i), we find that

$$\begin{aligned} \Phi(\mathbf{x}^-, \dots, \mathbf{x}^-, \mathbf{y}^-) &= \Phi(x_0\boldsymbol{\theta}^- + \Delta\mathbf{x}, \dots, x_0\boldsymbol{\theta}^- + \Delta\mathbf{x}, y_0\boldsymbol{\theta}^- + \Delta\mathbf{y}) \\ &= (d-1)x_0\Phi(\boldsymbol{\theta}^-, \Delta\mathbf{x}, \dots, \Delta\mathbf{x}, \Delta\mathbf{y}) \\ &\quad + y_0\Phi(\boldsymbol{\theta}^-, \Delta\mathbf{x}, \dots, \Delta\mathbf{x}) + \Phi(\Delta\mathbf{x}, \dots, \Delta\mathbf{x}, \Delta\mathbf{y}). \end{aligned} \tag{2.35}$$

We deduce from (2.34) that

$$\begin{aligned} |\Phi(\mathbf{x}^-, \dots, \mathbf{x}^-, \mathbf{y}^-)| &\ll \|\mathbf{x}\| L(\mathbf{x})^{d-2} L(\mathbf{y}) + \|\mathbf{y}\| L(\mathbf{x})^{d-1} + L(\mathbf{x})^{d-1} L(\mathbf{y}) \\ &\ll \|\mathbf{y}\| L(\mathbf{x})^{d-1}. \end{aligned} \tag{2.36}$$

On the other hand, using the definition of φ in Proposition 2.6.2 (ii), we find that

$$\varphi(\mathbf{x}^-) = \frac{1}{d!}\Phi(\mathbf{x}^-, \dots, \mathbf{x}^-) = \frac{1}{(d-1)!} x_0 \Phi(\boldsymbol{\theta}^-, \Delta\mathbf{x}, \dots, \Delta\mathbf{x}) + \varphi(\Delta\mathbf{x}), \tag{2.37}$$

and so, by (2.34), we get

$$|\varphi(\mathbf{x}^-)| \ll \|\mathbf{x}\| L(\mathbf{x})^{d-1}. \tag{2.38}$$

It follows from the definition of Ψ and equalities (2.35), (2.37) that

$$\begin{aligned}\Psi(\mathbf{x},\mathbf{y})_0 &= y_0\,\varphi(\mathbf{x}^-) - \frac{1}{(d-1)!}x_0\Phi(\mathbf{x}^-,\dots,\mathbf{x}^-,\mathbf{y}^-)\\ &= y_0\,\varphi(\Delta\mathbf{x}) - \frac{1}{(d-2)!}x_0^2\Phi(\boldsymbol{\theta}^-,\Delta\mathbf{x},\dots,\Delta\mathbf{x},\Delta\mathbf{y})\\ &\quad - \frac{1}{(d-1)!}x_0\Phi(\Delta\mathbf{x},\dots,\Delta\mathbf{x},\Delta\mathbf{y}).\end{aligned}$$

Thus we get

$$\begin{aligned}|\Psi(\mathbf{x},\mathbf{y})_0| &\ll \|\mathbf{y}\|L(\mathbf{x})^d + \|\mathbf{x}\|^2L(\mathbf{x})^{d-2}L(\mathbf{y}) + \|\mathbf{x}\|L(\mathbf{x})^{d-1}L(\mathbf{y})\\ &\ll \|\mathbf{y}\|L(\mathbf{x})^d + \|\mathbf{x}\|^2L(\mathbf{x})^{d-2}L(\mathbf{y})\end{aligned}$$

since $\|\mathbf{x}\| \geq L(\mathbf{x})$.

On the other hand, we deduce from the inequalities (2.36) and (2.38) that

$$\begin{aligned}L(\Psi(\mathbf{x},\mathbf{y})) &= L\left(\varphi(\mathbf{x}^-)\mathbf{y} - \frac{1}{(d-1)!}\Phi(\mathbf{x}^-,\dots,\mathbf{x}^-,\mathbf{y}^-)\mathbf{x}\right)\\ &\ll |\varphi(\mathbf{x}^-)|L(\mathbf{y}) + |\Phi(\mathbf{x}^-,\dots,\mathbf{x}^-,\mathbf{y}^-)|L(\mathbf{x})\\ &\ll \|\mathbf{x}\|L(\mathbf{x})^{d-1}L(\mathbf{y}) + \|\mathbf{y}\|L(\mathbf{x})^d\\ &\ll \|\mathbf{y}\|L(\mathbf{x})^d,\end{aligned}$$

Therefore, we obtain

$$\begin{aligned}\|\Psi(\mathbf{x},\mathbf{y})\| &= \|\Psi(\mathbf{x},\mathbf{y})_0\boldsymbol{\theta} + (\Psi(\mathbf{x},\mathbf{y}) - \Psi(\mathbf{x},\mathbf{y})_0\boldsymbol{\theta})\|\\ &\ll |\Psi(\mathbf{x},\mathbf{y})_0| + L(\Psi(\mathbf{x},\mathbf{y}))\\ &\ll \|\mathbf{x}\|^2L(\mathbf{x})^{d-2}L(\mathbf{y}) + \|\mathbf{y}\|L(x)^d.\end{aligned}$$ □

Proof of Theorem 2.7.1. (i) By definition of Ψ, we have $(d-1)!\,\mathbf{z}_n \in \mathbb{Z}^{d+1}$ for all n. Since any two consecutive minimal points are linearly independent and since $\varphi(\mathbf{y}_{n+d}) \neq 0$ for each $n \geq 1$ (by Proposition 2.6.2 (ii)), we deduce that $\mathbf{z}_n \neq 0$.

(ii) For any $n \in \mathbb{N}^*$, the conditions (ii) and (iii) of Theorem 2.4.3 give

$$\|\mathbf{y}_{n+1}\| \asymp \|\mathbf{y}_n\|^r, \quad L(\mathbf{y}_n) \asymp \|\mathbf{y}_n\|^{-1/(d-1)},$$

with $r = 1/((d-1)\lambda_d)$.

Fix a large integer n. We deduce from Proposition 2.7.3 that

$$L(\mathbf{z}_n) \ll \|\mathbf{y}_{n+d+1}\| L(\mathbf{y}_{n+d})^d \asymp \|\mathbf{y}_{n+d}\|^{r-\frac{d}{d-1}} \asymp \|\mathbf{y}_n\|^{(r-\frac{d}{d-1})r^d}.$$

Since λ_d is a positive root of (2.5), we get

$$\frac{1}{r} + \cdots + \frac{1}{r^d} = d-1,$$

and so

$$d\,r^d = (d-1)r^d + r^d = 1 + r + \cdots + r^{d-1} + r^d. \tag{2.39}$$

Thus we have

$$\begin{aligned}\left(r - \frac{d}{d-1}\right) r^d &= \frac{1}{d-1}\big((d-1)r^{d+1} - (1 + r + \cdots + r^d)\big) \\ &= \frac{1}{d-1}\Big(-1 + r\big((d-1)r^d - (1 + r + \cdots + r^{d-1})\big)\Big) \\ &= \frac{-1}{d-1}.\end{aligned}$$

This leads to

$$L(\mathbf{z}_n) \ll \|\mathbf{y}_{n+d}\|^{r-\frac{d}{d-1}} \asymp \|\mathbf{y}_n\|^{\frac{-1}{d-1}} \asymp L(\mathbf{y}_n). \tag{2.40}$$

By Proposition 2.7.3 (ii), we get

$$\begin{aligned}\|\mathbf{z}_n\| &\ll \|\mathbf{y}_{n+d}\|^2 L(\mathbf{y}_{n+d})^{d-2} L(\mathbf{y}_{n+d+1}) + \|\mathbf{y}_{n+d+1}\| L(\mathbf{y}_{n+d})^d \\ &\asymp \|\mathbf{y}_{n+d}\|^{2-\frac{d-2}{d-1}-\frac{r}{d-1}} + \|\mathbf{y}_{n+d}\|^{r-\frac{d}{d-1}}.\end{aligned}$$

We deduce from the estimates (2.40) that $\|\mathbf{y}_{n+d}\|^{r-\frac{d}{d-1}}$ converges to 0 as n tends to ∞, and since $\|\mathbf{z}_n\| \geq 1$, we obtain

$$\|\mathbf{z}_n\| \ll \|\mathbf{y}_{n+d}\|^{\frac{d-r}{d-1}}.$$

(iii) Set $D_n = \det(\mathbf{y}_n, \mathbf{y}_{n+1}, \ldots, \mathbf{y}_{n+d-1}, \mathbf{z}_n)$ for each $n > 0$.

By part (i), we get $(d-1)!\, D_n \in \mathbb{Z}$ for all $n > 0$. So, it is enough to prove that D_n converges to 0 when n tends to infinity.

From part (ii), we deduce that

$$\begin{aligned}
D_n &\ll \|\mathbf{y}_{n+d-1}\| L(\mathbf{y}_n)\cdots L(\mathbf{y}_{n+d-2}) L(\mathbf{z}_n) + \|\mathbf{z}_n\| L(\mathbf{y}_n)\cdots L(\mathbf{y}_{n+d-1}) \\
&\ll L(\mathbf{y}_n)\cdots L(\mathbf{y}_{n+d-2})(\|\mathbf{y}_{n+d-1}\| L(\mathbf{z}_n) + \|\mathbf{z}_n\| L(\mathbf{y}_{n+d-1})) \\
&\ll (\|\mathbf{y}_n\|\cdots\|\mathbf{y}_{n+d-2}\|)^{-\frac{1}{d-1}} \left(\|\mathbf{y}_{n+d}\|^{\frac{1}{r}+r-\frac{d}{d-1}} + \|\mathbf{y}_{n+d}\|^{\frac{d-r}{d-1}-\frac{1}{(d-1)r}} \right) \\
&\ll \|\mathbf{y}_n\|^{-\frac{1}{d-1}(1+r+\cdots+r^{d-2})} \|\mathbf{y}_{n+d}\|^{\frac{1}{r}+r-\frac{d}{d-1}} \\
&\ll \|\mathbf{y}_n\|^{g(r)},
\end{aligned}$$

where

$$g(r) = -\frac{1}{d-1}(1+r+\cdots+r^{d-2}) + r^d\left(\frac{1}{r}+r-\frac{d}{d-1}\right).$$

By (2.39), we get

$$\begin{aligned}
g(r) &= -\frac{1}{d-1}\left((d-1)r^d - r^{d-1}\right) + \left(r^{d-1}+r^{d+1}-\frac{d}{d-1}r^d\right) \\
&= r^{d-1}\left(r^2 - \frac{2d-1}{d-1}r + \frac{d}{d-1}\right).
\end{aligned}$$

Note that $1/d < \lambda_d < 1/(d-1)$ and so $1 < r < d/(d-1)$. We deduce that $g(r) < 0$. Since $\|\mathbf{y}_n\|$ grows very fast, D_n converges to 0 when n tends to infinity. □

2.8 An explicit construction of a point with exponent of approximation $\geq 1/3$

It would be nice to know if the exponent λ_d given by Theorem 2.1.3 is optimal for some integer $d \geq 3$, namely if there exists a real algebraic number α of degree d and a real number $\xi \notin \mathbb{Q}(\alpha)$ such that $\hat{\lambda}(1,\alpha,\ldots,\alpha^{d-1},\xi) = \lambda_d$. If such numbers exist, then Theorem 2.4.3 provides us with a sequence of primitive points $\mathbf{x}_n = (x_{n,0},\ldots,x_{n,d-1})$ in $\mathbb{Z}^{d+1}$ satisfying

(i) $|\det(\mathbf{x}_n,\mathbf{x}_{n+1},\ldots,\mathbf{x}_{n+d})| \asymp 1$,

(ii) $\|\mathbf{x}_{n+1}\| \asymp \|\mathbf{x}_n\|^r$ with $r = 1/((d-1)\lambda_d)$,

(iii) $L(\mathbf{x}_n) \asymp L'(\mathbf{x}_n^-) \asymp \|\mathbf{x}_n\|^{-1/(d-1)}$,

where $\boldsymbol{\theta} = (1,\alpha,\ldots,\alpha^{d-1},\xi)$ and $L = L_{\boldsymbol{\theta}}$, $L' = L_{\boldsymbol{\theta}^-}$.

Then by (2.33), the property $L'(\mathbf{x}_n) \asymp \|\mathbf{x}_n\|^{-1/(d-1)}$ implies that

(iv) $|\varphi(\mathbf{x}_n^-)| \asymp 1$

where φ is the polynomial associated to α defined in Section 2.6.

In this section, we choose $d = 3$ and $\alpha = \sqrt[3]{2}$ and prove the following result.

Theorem 2.8.1. *There exist a real number $\xi \notin \mathbb{Q}(\alpha)$ and a sequence of primitive points $(\mathbf{x}_n)_{n\in\mathbb{N}^*}$ in $\mathbb{Z}^4$ satisfying*

(i)' $\det(\mathbf{x}_n, \mathbf{x}_{n+1}, \mathbf{x}_{n+2}, \mathbf{x}_{n+3}) \neq 0$,

(ii)' $\|\mathbf{x}_{n+1}\| \asymp \|\mathbf{x}_n\|^{3/2}$,

(iii)' $L'(\mathbf{x}_n^-) \asymp \|\mathbf{x}_n\|^{-1/2}$ *and* $L(\mathbf{x}_n) \ll c^n \|\mathbf{x}_n\|^{-1/2}$,

(iv)' $\varphi(\mathbf{x}_n^-) = 1$,

where $c = 180\,000$ *and* $L = L_{\boldsymbol{\theta}}$, $L' = L_{\boldsymbol{\theta}^-}$ *with* $\boldsymbol{\theta} = (1, \alpha, \alpha^2, \xi)$.

It is interesting to compare the conditions (i)'–(iv)' with the conditions (i)–(iv) for $d = 3$.

The condition (iv)' is very restrictive because, as we will see below, it implies that $x_{n,0}\alpha^2 + x_{n,1}\alpha + x_{n,2}$ is a unit of $\mathbb{Z}[\alpha]$, and these units are sparse since the unit group of $\mathbb{Z}[\alpha]$ has rank 1. However, it is not much more restrictive than condition (iv) which requests the norm of $x_{n,0}\alpha^2 + x_{n,1}\alpha + x_{n,2}$ to be bounded. So conditions (iv) and (iv)' are essentially the same.

Consider condition (iii)'. We deduce from the condition (ii)' on the growth of $\|\mathbf{x}_n\|$ that, for each $\epsilon > 0$, there exists an integer n_0 such that

$$c^n \leq \|\mathbf{x}_n\|^{\epsilon} \qquad \text{for all } n \geq n_0.$$

Therefore, conditions (iii)' and (iii) for $d = 3$ are also essentially the same. The condition (i)' is much weaker than (i) but strong enough to yield that $\xi \notin \mathbb{Q}(\alpha)$ as we will see below.

The main difference is condition (ii)' which shows that $\|\mathbf{x}_n\|$ grows much faster than we would like in comparison with (ii) because for $d = 3$, we have $r \approx 1.234$.

Now let ξ and $(\mathbf{x}_n)_{n\in\mathbb{N}^*}$ be as in Theorem 2.8.1. Fix $\epsilon \in \mathbb{R}$ with $0 < \epsilon < 1/6$. For each sufficiently large value of X, condition (ii)' ensures the existence of a positive integer n such that

$$\|\mathbf{x}_n\| \le X < \|\mathbf{x}_{n+1}\|, \quad c^n \le \|\mathbf{x}_{n+1}\|^{\epsilon/3}.$$

Then for $\mathbf{x} = \mathbf{x}_n$, we have $\|\mathbf{x}\| \le X$, moreover, it follows from conditions (ii)' and (iii)' that

$$L_{\boldsymbol{\theta}}(\mathbf{x}) \ll c^n\|\mathbf{x}_n\|^{-1/2} \asymp c^n\|\mathbf{x}_{n+1}\|^{-1/3} \le \|\mathbf{x}_{n+1}\|^{-(1-\epsilon)/3} < X^{-(1-\epsilon)/3}.$$

Therefore, $\lambda = (1-\epsilon)/3$ is a uniform exponent of approximation to $\boldsymbol{\theta} = (1, \alpha, \alpha^2, \xi)$. Since $\epsilon > 0$ can be choosen arbitrarily small, we deduce that $\hat{\lambda}(\boldsymbol{\theta}) \ge 1/3$, a result which is true for any ξ by the box principle (see Lemma 2.1.2 (i)).

On the other hand, if X is sufficiently large and satisfies

$$\|\mathbf{x}_n\| \le X < \|\mathbf{x}_{n+1}\|^{1-2\epsilon}$$

for some n, then we have

$$L_{\boldsymbol{\theta}}(\mathbf{x}) \ll \|\mathbf{x}_{n+1}\|^{-(1-\epsilon)/3} \le X^{-\frac{1-\epsilon}{3(1-2\epsilon)}}.$$

This is meaningful because $\frac{1-\epsilon}{3(1-2\epsilon)} > 1/3$ and so we cannot construct such a point by the box principle.

One more thing significant here is that if we could improve the condition (ii)' and get $\|\mathbf{x}_{n+1}\| \asymp \|\mathbf{x}_n\|^r$ with $1/2 \le r < 3/2$, then by condition (iii)', this would give

$$L_{\boldsymbol{\theta}}(\mathbf{x}_n) \ll c^n\|\mathbf{x}_n\|^{-\frac{1}{2}} \asymp c^n\|\mathbf{x}_{n+1}\|^{-\frac{1}{2r}} \ll \|\mathbf{x}_{n+1}\|^{-(\frac{1}{2r}-\epsilon)}$$

for any fixed $\epsilon > 0$. Then $\lambda = 1/(2r) - \epsilon$ would be a uniform exponent of approximation to $\boldsymbol{\theta}$ for any $\epsilon > 0$ and so

$$\hat{\lambda}(\boldsymbol{\theta}) \ge \frac{1}{2r} > 1/3.$$

In order to prove Theorem 2.8.1, we will construct a number ξ and a sequence $(\mathbf{x}_n)_{n\in\mathbb{N}^*}$ satisfying all the conditions required in the theorem. To do this, we start with the following observations.

Assume that points $\mathbf{x}_n = (x_{n,0}, \ldots, x_{n,3}) \in \mathbb{Z}^4$ satisfy the condition (iv)'. By Proposition 2.6.2, it implies that

$$N_{K/\mathbb{Q}}(a_0x_{n,0} + a_1x_{n,1} + a_2x_{n,2}) = 1$$

with $a_0, a_1, a_2 \in \mathbb{Q}(\alpha)$ given by (2.32) in Lemma 2.6.1. Since $\min(\alpha, \mathbb{Q}) = T^3 - 2$, we get

$$a_0 = \alpha^2, \quad a_1 = \alpha, \quad a_2 = 1.$$

So we find

$$\alpha^2x_{n,0} + \alpha x_{n,1} + x_{n,2} \in \mathcal{O}_K^*.$$

Since K has one real embedding and two complex conjugate embeddings into $\mathbb{C}$, it follows from Dirichlet's Unit Theorem that $\mathcal{O}_K^*$ has rank 1. One can show that

$$\mathcal{O}_K^* = \{\pm\varepsilon^m, \ m \in \mathbb{Z}\}$$

where $\varepsilon = \alpha^2 + \alpha + 1$. So for each $n \in \mathbb{N}$, we have

$$\alpha^2x_{n,0} + \alpha x_{n,1} + x_{n,2} = \pm\varepsilon^{s_n}$$

for some $s_n \in \mathbb{Z}$.

Note that for each $n \in \mathbb{Z}$, there exists a unique triple (a_n, b_n, c_n) in $\mathbb{Z}^3$ such that

$$\varepsilon^n = a_n\alpha^2 + b_n\alpha + c_n.$$

Therefore, the points $\mathbf{x}_n$ must have the form

$$\mathbf{x}_n = \pm(A_n, B_n, C_n, y_n) \tag{2.41}$$

for some $y_n \in \mathbb{Z}$ and $A_n = a_{s_n}, B_n = b_{s_n}, C_n = c_{s_n}$.

We need more information about the powers of ε. To derive them, we denote the three conjugates of α by

$$\alpha, \quad \alpha_1 = \rho\sqrt[3]{2}, \quad \alpha_2 = \bar{\alpha}_1 = \rho^2\sqrt[3]{2}.$$

where $\rho = e^{\frac{2\pi}{3}i}$. Hence the three conjugates of ε^n are

$$\varepsilon^n, \quad \varepsilon_1^n = a_n\alpha_1^2 + b_n\alpha_1 + c_n, \quad \varepsilon_2^n = a_n\alpha_2^2 + b_n\alpha_2 + c_n.$$

Moreover, we have

$$\varepsilon_1 = \varepsilon^{-\frac{1}{2}}e^{i\zeta}, \ \varepsilon_2 = \varepsilon^{-\frac{1}{2}}e^{-i\zeta}$$

with $\zeta \approx -0.5899$.

Proposition 2.8.2. *For any $n \in \mathbb{N}^*$, the number ε^n has the following properties:*

(*i*) $N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\varepsilon^n) = 1, \ \gcd(a_n, b_n, c_n) = 1,$

(*ii*) $|a_n\alpha - b_n| \leq \varepsilon^{-\frac{n}{2}}, \quad |a_n\alpha^2 - c_n| \leq \frac{3}{2}\varepsilon^{-\frac{n}{2}},$

(*iii*) $\frac{1}{6}\varepsilon^n < a_n < \frac{1}{3}\varepsilon^n.$

Proof. The property (i) follows immediately from the fact that ε is a unit of $\mathbb{Z}[\alpha]$ of norm 1.

(ii) We have

$$\begin{aligned}\varepsilon_1^n - \varepsilon_2^n &= a_n(\alpha_1^2 - \alpha_2^2) + b_n(\alpha_1 - \alpha_2)\\ &= (\alpha_2 - \alpha_1)(a_n\alpha - b_n).\end{aligned}$$

So

$$|a_n\alpha - b_n| = \frac{|\varepsilon_1^n - \varepsilon_2^n|}{|\alpha_2 - \alpha_1|} \leq \frac{2\varepsilon^{-n/2}}{|\alpha_2 - \alpha_1|} \leq \varepsilon^{-\frac{n}{2}}.$$

For the second inequality, we use

$$\begin{aligned}\varepsilon_1^n + \varepsilon_2^n &= a_n(\alpha_1^2 + \alpha_2^2) + b_n(\alpha_1 + \alpha_2) + 2c_n\\ &= -a_n\alpha^2 - b_n\alpha + 2c_n\\ &= 2(c_n - a_n\alpha^2) - \alpha(b_n - a_n\alpha),\end{aligned}$$

and get

$$\begin{aligned}|c_n - a_n\alpha^2| = \frac{1}{2}|(\varepsilon_1^n + \varepsilon_2^n) + \alpha(b_n - a_n\alpha)| &= \frac{1}{2}\left|(\varepsilon_1^n + \varepsilon_2^n) + \alpha\frac{\varepsilon_1^n - \varepsilon_2^n}{\alpha_1 - \alpha_2}\right|\\ &\leq \frac{1}{2}\left(\left|1 + \frac{\alpha}{\alpha_1 - \alpha_2}\right| + \left|1 - \frac{\alpha}{\alpha_1 - \alpha_2}\right|\right)\varepsilon^{-n/2}\\ &\leq \frac{3}{2}\varepsilon^{-n/2}.\end{aligned}$$

(iii) We have

$$\begin{aligned}\varepsilon^n &= a_n\alpha^2 + b_n\alpha + c_n\\ &= 3a_n\alpha^2 + \alpha(b_n - a_n\alpha) + (c_n - a_n\alpha^2).\end{aligned}$$

It is clear by definition that $a_n > 0$ for all $n > 0$. From (ii), we deduce that

$$\frac{\varepsilon^n}{6} < \frac{\varepsilon^n - (\alpha + \frac{3}{2})\varepsilon^{-\frac{n}{2}}}{3\alpha^2} \le a_n \le \frac{\varepsilon^n + (\alpha + \frac{3}{2})\varepsilon^{-\frac{n}{2}}}{3\alpha^2} < \frac{\varepsilon^n}{3} \quad \text{for} \quad n > 1.$$

When $n = 1$, we have $a_n = 1$ so it is clear that $\frac{1}{6}\varepsilon < a_n < \frac{1}{3}\varepsilon$. □

For each $n \ge 1$, we request that $s_n > 0$. Since $\mathbf{x}_n$ has form (2.41), the above proposition gives

$$\varphi(\mathbf{x}_n^-) = 1, \quad \|\mathbf{x}_n^-\| \asymp A_n \asymp \varepsilon^{s_n}, \quad L'(\mathbf{x}_n^-) \ll \varepsilon^{-s_n/2} \asymp \|\mathbf{x}_n^-\|^{-1/2}. \tag{2.42}$$

By Proposition 2.4.1, we get $L'(\mathbf{x}_n) \gg \|\mathbf{x}_n^-\|^{-1/2}$ and so

$$L'(\mathbf{x}_n) \asymp \|\mathbf{x}_n^-\|^{-1/2}.$$

Hence $(\mathbf{x}_n)_{n\in\mathbb{N}^*}$ satisfies the condition (iv)' and half of (iii)' in Theorem 2.8.1 for any choice of y_n and $s_n > 0$. We have the freedom of choosing y_n and s_n such that the remaining conditions are fulfilled.

Since we want the first coordinate of $\mathbf{x}_n$ to be positive, we will assume that in (2.41) we have the sign + so that $\mathbf{x}_n = (A_n, B_n, C_n, y_n)$

Note that

$$L(\mathbf{x}_n) = \max\{L'(\mathbf{x}_n^-), |A_n\xi - y_n|\}$$

holds for any choice of y_n and ξ. Moreover, we have

$$L'(\mathbf{x}_n^-) \ll \|\mathbf{x}_n^-\|^{-1/2}.$$

So asking that $L(\mathbf{x}_n) \ll c^n\|\mathbf{x}_n\|^{-1/2}$ is equivalent to asking that

$$|A_n\xi - y_n| \ll c^n\|\mathbf{x}_n\|^{-1/2},$$

which leads to

$$\left|\xi - \frac{y_n}{A_n}\right| \ll c^n A_n^{-3/2}. \tag{2.43}$$

Set

$$\xi_n = \frac{y_n}{A_n} \qquad \text{for } n \in \mathbb{N}^*.$$

Then the conditioon (2.43) implies that

$$\begin{aligned} |\xi_n - \xi_{n-1}| &\leq |\xi_n - \xi| + |\xi_{n-1} - \xi| \\ &\ll c^n A_n^{-3/2} + c^{n-1} A_{n-1}^{-3/2} \\ &\ll c^{n-1} A_{n-1}^{-3/2}. \end{aligned} \tag{2.44}$$

To utilise this, we introduce some new notation.

For each $n \in \mathbb{N}^*$, we denote by $[\varepsilon^n] = (a_n, b_n, c_n)^T$ the coordinates of ε^n in the basis $\{1, \alpha, \alpha^2\}$ of $\mathcal{O}_K$.

For each $n \geq 4$, we also denote by D_n the determinant of the matrix

$$M_n = (\mathbf{x}_n^T \;\; \mathbf{x}_{n-1}^T \;\; \mathbf{x}_{n-2}^T \;\; \mathbf{x}_{n-3}^T)$$

and denote by $D_{n,i}$ the determinant of the matrix obtained by removing the last row and the $(i+1)$–th column from matrix M_n for each $i = 0, 1, 2, 3$.

We have

$$\begin{aligned} D_n &= \begin{vmatrix} [\varepsilon^{s_n}] & [\varepsilon^{s_{n-1}}] & [\varepsilon^{s_{n-2}}] & [\varepsilon^{s_{n-3}}] \\ y_n - \xi_{n-1}A_n & 0 & y_{n-2} - \xi_{n-1}A_{n-2} & y_{n-3} - \xi_{n-1}A_{n-3} \end{vmatrix} \\ &= (\xi_n - \xi_{n-1})A_n D_{n,0} + (\xi_{n-2} - \xi_{n-1})A_{n-2}D_{n,2} + (\xi_{n-3} - \xi_{n-1})A_{n-3}D_{n,3}. \end{aligned}$$

Suppose that $\mathbf{x}_{n-1}, \mathbf{x}_{n-2}, \mathbf{x}_{n-3}$ have been constructed and that $D_{n,0} \neq 0$. We get

$$|\xi_n - \xi_{n-1}| \leq \frac{|D_n| + |(\xi_{n-2} - \xi_{n-1})A_{n-2}D_{n,2}| + |(\xi_{n-3} - \xi_{n-1})A_{n-3}D_{n,3}|}{|A_n D_{n,0}|}. \tag{2.45}$$

We want $|\xi_n - \xi_{n-1}| \leq c^{n-1} A_{n-1}^{-3/2}$. However, as we will see below, for any positive integers m, n, p with $m < n < p$, we have

$$\left|\det\left([\varepsilon^m]^T \;\; [\varepsilon^n]^T \;\; [\varepsilon^p]^T\right)\right| \leq \frac{1}{\sqrt{3}} \varepsilon^{p - \frac{m+n}{2}},$$

which is an optimal upper bound. Therefore, we want $|D_{n,0}|$ as large as possible and want $|D_n|$ as small as possible, but not zero (because of (i)').

We find a case where $\left|\det\left([\varepsilon^m]^T\ [\varepsilon^n]^T\ [\varepsilon^p]^T\right)\right| \asymp \frac{1}{\sqrt{3}}\varepsilon^{p-\frac{m+n}{2}}$. The following lemma ensures the existence of m, n, p in this case.

Lemma 2.8.3. *Among any two consecutive integers, there is one integer n for which $|\sin(n\zeta)| > 1/4$.*

Proof. Assume that $|\sin(n\zeta)| \leq 1/4$. We will show that $|\sin((n+1)\zeta)| > 1/4$. Indeed, by noting that $|\cos(n\zeta)| \geq \frac{\sqrt{15}}{4}$, we have

$$\begin{aligned}|\sin((n+1)\zeta)| &= |\sin(\zeta)\cos(n\zeta) + \cos(\zeta)\sin(n\zeta)|\\ &\geq |\sin(\zeta)\cos(n\zeta)| - |\cos(\zeta)\sin(n\zeta)|\\ &\geq \frac{\sqrt{15}}{4}|\sin\zeta| - \frac{1}{4}|\cos\zeta|\\ &> 1/4\end{aligned}$$

where the last inequality is a direct computation using $\zeta \approx -0.5899$ □

Lemma 2.8.4. *Let $K = \mathbb{Q}(\alpha)$. Let m, n, p be integers such that $1 \leq m < n < p$ and*

$$|\sin(n-m)\zeta| \geq 1/4.$$

Then we have

$$\frac{1}{36\sqrt{3}}\varepsilon^{p-\frac{m+n}{2}} < |\det([\varepsilon^m], [\varepsilon^n], [\varepsilon^p])| < \frac{1}{\sqrt{3}}\varepsilon^{p-\frac{m+n}{2}}. \tag{2.46}$$

Proof. Let $\sigma_0, \sigma_1, \sigma_2$ be all the embeddings of K into $\mathbb{C}$ ordered so that

$$\sigma_0(\alpha) = \alpha, \quad \sigma_1(\alpha) = \alpha_1, \quad \sigma_2(\alpha) = \alpha_2.$$

Consider the canonical embedding

$$\begin{aligned}f : K &\longrightarrow \mathbb{C}^3\\ x &\longmapsto (\sigma_0(x), \sigma_1(x), \sigma_2(x)).\end{aligned}$$

For each $x \in K$, we have $f(x)^T = M[x]$ where

$$M = \begin{pmatrix} 1 & \alpha & \alpha^2 \\ 1 & \alpha_1 & \alpha_1^2 \\ 1 & \alpha_2 & \alpha_2^2 \end{pmatrix}$$

and where $[x]$ denotes the coordinates of x in the basis $\{1, \alpha, \alpha^2\}$.

So, for any $x, y, z \in K$, we have

$$\begin{aligned} |\det(f(x)^T, f(y)^T, f(z)^T)| = & \ |\det(M) \det([x], [y], [z])| \\ = & \ 6\sqrt{3}\ |\det([x], [y], [z])|. \end{aligned}$$

In particular, we deduce that

$$|\det([\varepsilon^m], [\varepsilon^n], [\varepsilon^p])| = \frac{|A|}{6\sqrt{3}}$$

where

$$A = \det\left(f(\varepsilon^m)^T, f(\varepsilon^n)^T, f(\varepsilon^p)^T\right) = \begin{vmatrix} \varepsilon^m & \varepsilon^n & \varepsilon^p \\ \varepsilon_1^m & \varepsilon_1^n & \varepsilon_1^p \\ \varepsilon_2^m & \varepsilon_2^n & \varepsilon_2^p \end{vmatrix}.$$

Since $|\varepsilon_1| = |\varepsilon_2| = \varepsilon^{-\frac{1}{2}}$ and $m < n < p$, we get

$$|A| \leq 6|\varepsilon^p \varepsilon_1^n \varepsilon_2^m| \leq 6\varepsilon^{p - \frac{m+n}{2}},$$

which proves the upper bound for the absolute value of the determinant in (2.46).

Now for the lower bound, we use

$$\begin{aligned} |A| &\geq |\varepsilon^p(\varepsilon_1^m \varepsilon_2^n - \varepsilon_1^n \varepsilon_2^m)| - |\varepsilon^n(\varepsilon_1^m \varepsilon_2^p - \varepsilon_1^p \varepsilon_2^m)| - |\varepsilon^m(\varepsilon_1^p \varepsilon_2^n - \varepsilon_1^n \varepsilon_2^p)| \\ &\geq \varepsilon^p |(\varepsilon_1^m \varepsilon_2^m)(\varepsilon_2^{n-m} - \varepsilon_1^{n-m})| - 2\varepsilon^{n - \frac{m+p}{2}} - 2\varepsilon^{m - \frac{n+p}{2}} \\ &\geq \varepsilon^{p-m} |2\,\mathrm{Im}(\varepsilon_1^{\mathrm{n-m}})| - 2\varepsilon^{n - \frac{m+p}{2}} - 2\varepsilon^{m - \frac{n+p}{2}} \\ &\geq 2\ |\sin((n-m)\zeta)| \varepsilon^{p - \frac{m+n}{2}} - 2\varepsilon^{n - \frac{m+p}{2}} - 2\varepsilon^{m - \frac{n+p}{2}}. \end{aligned}$$

Since $|\sin(n-m)\zeta| \geq 1/4$ and $p > n > m$, we obtain that

$$\begin{aligned} |A| &> \varepsilon^{p - \frac{n+m}{2}} \left(\frac{1}{2} - 2\varepsilon^{-\frac{3}{2}(p-n)} - 2\varepsilon^{-\frac{3}{2}(p-m)} \right) \\ &\geq \frac{1}{6} \varepsilon^{p - \frac{m+n}{2}}, \end{aligned}$$

so this completes the proof of (2.46). □

In view of the above lemma, we ask that

$$|\sin((s_n - s_{n-1})\zeta)| > 1/4 \tag{2.47}$$

for all $n > 1$ in order to make $D_{n,0}$ large.

Note that condition (iii)' implies that $\|\mathbf{x}_n\| \asymp \|\mathbf{x}_n^-\| \asymp \varepsilon^{s_n}$. Hence condition (ii)' requires

$$s_{n+1} = \frac{3}{2}s_n + \mathcal{O}(1). \tag{2.48}$$

As we will see below, it is easy to construct a sequence $(s_n)_{n\in\mathbb{N}^*}$ for which conditions (2.47) and (2.48) are satisfied.

To construct y_n, we consider D_n as a linear form in y_n. Since the coefficient of y_n is $D_{n,0}$, as we will see below, we can choose $y_n \in \mathbb{Z}$ such that

$$0 < |D_n| \le |D_{n,0}|. \tag{2.49}$$

Now we give the details.

Proof of Theorem 2.8.1. We construct the sequence $(\mathbf{x}_n)_{n\in\mathbb{N}^*}$ and the number ξ so that they satisfy all the required conditions.

Step 1. We construct recursively a sequence of positive integers $(s_n)_{n\in\mathbb{N}^*}$.

Set $s_1 = 1$. For $n > 1$, we assume that s_{n-1} is constructed and choose s_n to be one of the two consecutive integers $\lfloor (3/2)^n \rfloor$ and $\lceil (3/2)^n \rceil$ for which

$$|\sin((s_n - s_{n-1})\zeta)| > 1/4$$

is satisfied (see (2.47)). This is possible because of Lemma 2.8.3. Then, for each $n \ge 1$, we find

$$\left| s_{n+1} - \frac{3}{2}s_n \right| \le \left| s_{n+1} - \left(\frac{3}{2}\right)^{n+1} \right| + \frac{3}{2}\left| s_n - \left(\frac{3}{2}\right)^n \right| < \frac{5}{2}\,. \tag{2.50}$$

(The condition (2.48) is therefore fulfilled.)

Set

$$\mathbf{x}_n^- = [\varepsilon^{s_n}]^T \quad \text{for each } n > 1.$$

Then, from the previous discussion, we deduce that, for each $n > 0$, we have

$$\varphi(\mathbf{x}_n^-) = 1, \qquad L'(\mathbf{x}_n^-) \asymp \|\mathbf{x}_n^-\|^{-1/2},$$

$$\|\mathbf{x}_{n+1}^-\| \asymp A_{n+1} \asymp \varepsilon^{s_{n+1}} \asymp A_n^{3/2} \asymp \|\mathbf{x}_n^-\|^{3/2},$$

and

$$\frac{1}{36\sqrt{3}}\varepsilon^{s_{n-1}-\frac{1}{2}(s_{n-2}+s_{n-3})} \le |D_{n,0}| \le \frac{1}{\sqrt{3}}\varepsilon^{s_{n-1}-\frac{1}{2}(s_{n-2}+s_{n-3})} \quad \text{if } n > 4. \tag{2.51}$$

Step 2. We construct recursively a sequence of integers $(y_n)_{n\in\mathbb{N}^*}$.

For $n = 1, 2, 3$, we set $y_n = A_n$. Assume that $y_{n-1}, y_{n-2}, y_{n-3}$ have been choosen for some $n > 3$. Let t be a real number such that $D_n(t) = 0$ where

$$\begin{aligned} D_n(t) = &\begin{vmatrix} (\mathbf{x}_n^-)^T & (\mathbf{x}_{n-1}^-)^T & (\mathbf{x}_{n-2}^-)^T & (\mathbf{x}_{n-3}^-)^T \\ t & y_{n-1} & y_{n-2} & y_{n-3} \end{vmatrix} \\ = &- tD_{n,0} + y_{n-1}D_{n,1} - y_{n-2}D_{n,2} + y_{n-3}D_{n,3}. \end{aligned}$$

Set

$$y_n = \begin{cases} t+1 & \text{if } t \in \mathbb{Z}, \\ \lfloor t \rfloor & \text{if } t \notin \mathbb{Z}. \end{cases}$$

Then we obtain that $0 \neq |D_n| \le |D_{n,0}|$ for all $n > 3$.

For each $n > 0$, we define

$$\mathbf{x}_n = (\mathbf{x}_n^-, y_n).$$

Step 3. We construct $\xi \notin \mathbb{Q}(\alpha)$ and show that the sequence $(\mathbf{x}_n)_{n\in\mathbb{N}^*}$ has all the required properties.

Set $\xi_n = y_n/A_n$ for each $n \ge 1$.

We first prove by induction that the sequence $(\xi_n)_{n\in\mathbb{N}^*}$ satisfies

$$|\xi_n - \xi_{n-1}| \le c^{n-1}A_{n-1}^{-3/2} \tag{2.52}$$

for all $n > 1$.

This is true when $n = 2$ or 3 since $\xi_1 = \xi_2 = \xi_3 = 1$. Assume that

$$|\xi_{n-1} - \xi_{n-2}| \le c^{n-2}A_{n-2}^{-3/2}, \quad |\xi_{n-2} - \xi_{n-3}| \le c^{n-3}A_{n-3}^{-3/2} \tag{2.53}$$

for some $n > 3$. We will show that

$$|\xi_n - \xi_{n-1}| \le c^{n-1} A_{n-1}^{-3/2}.$$

Note that, by Proposition 2.8.2 (iii), we get

$$\frac{1}{6}\varepsilon^{s_m} < A_m < \frac{1}{3}\varepsilon^{s_m} \quad \text{for any } m \in \mathbb{N}^*. \tag{2.54}$$

Since $s_{n-2} > s_{n-3}$, this implies that

$$\frac{A_{n-2}}{A_{n-3}} > \frac{1}{2}\varepsilon^{s_{n-2}-s_{n-3}} > \varepsilon/2.$$

By the assumption (2.53), this leads to

$$\begin{aligned} |\xi_{n-3} - \xi_{n-1}| &\le |\xi_{n-3} - \xi_{n-2}| + |\xi_{n-2} - \xi_{n-1}| \\ &\le c^{n-2} A_{n-3}^{-3/2} \left(\frac{1}{c} + \left(\frac{A_{n-2}}{A_{n-3}} \right)^{-3/2} \right) \\ &\le c^{n-2} A_{n-3}^{-3/2}. \end{aligned} \tag{2.55}$$

By the choice of y_n, we have $0 \ne |D_{n,0}| < |D_n|$. So it follows from the main inequality (2.45) that

$$|\xi_n - \xi_{n-1}| \le \frac{|D_{n,0}| + |(\xi_{n-2} - \xi_{n-1}) A_{n-2} D_{n,2}| + |(\xi_{n-3} - \xi_{n-1}) A_{n-3} D_{n,3}|}{|A_n D_{n,0}|}.$$

It follows from (2.50) and (2.54) that

$$A_n > \frac{1}{6}\varepsilon^{s_n} > \frac{1}{6}\varepsilon^{\frac{3}{2}s_{n-1}-\frac{5}{2}} > \frac{1}{6\varepsilon^{5/2}}(3A_{n-1})^{3/2} > \frac{1}{35}A_{n-1}^{3/2}.$$

So we deduce that

$$|\xi_n - \xi_{n-1}| \le 35 A_{n-1}^{-3/2} \left(1 + \frac{|(\xi_{n-2} - \xi_{n-1}) A_{n-2} D_{n,2}| + |(\xi_{n-3} - \xi_{n-1}) A_{n-3} D_{n,3}|}{|D_{n,0}|} \right).$$

Applying Lemma 2.8.4 together wit the estimates (2.53), (2.54), we find

$$\begin{aligned} |(\xi_{n-2} - \xi_{n-1}) A_{n-2} D_{n,2}| &\le c^{n-2} A_{n-2}^{-1/2} \frac{1}{\sqrt{3}} \varepsilon^{s_n - \frac{1}{2}(s_{n-1}+s_{n-3})} \\ &\le c^{n-2} \left(\frac{1}{6}\varepsilon^{s_{n-2}} \right)^{-1/2} \frac{1}{\sqrt{3}} \varepsilon^{s_n - \frac{1}{2}(s_{n-1}+s_{n-3})} \\ &\le \sqrt{2}\, c^{n-2} \varepsilon^{s_n - \frac{1}{2}(s_{n-1}+s_{n-2}+s_{n-3})}. \end{aligned}$$

Similarly, using (2.55), we also find

$$|(\xi_{n-3} - \xi_{n-1})A_{n-3}D_{n,3}| \le \sqrt{2}\, c^{n-2} \varepsilon^{s_n - \frac{1}{2}(s_{n-1}+s_{n-2}+s_{n-3})}.$$

Substituting the estimates in the upper bound for $|\xi_n - \xi_{n-1}|$ and using the lower bound for $D_{n,0}$ given by (2.51), we deduce that

$$\begin{aligned} |\xi_n - \xi_{n-1}| &\le 35 A_{n-1}^{-3/2}(1 + 72\sqrt{6}\, c^{n-2}\varepsilon^{s_n - \frac{3}{2}s_{n-1}}) \\ &< (35 + 6173\, c^{n-2}\varepsilon^{5/2})A_{n-1}^{-3/2} && (\text{ by } (2.48)) \\ &< c^{n-1} A_{n-1}^{-3/2} && (\text{since } \ c = 180\,000). \end{aligned}$$

By the induction principle, we conclude that (2.52) holds for any integer $n > 1$.

This result shows that $(\xi_n)_{n\in\mathbb{N}^*}$ is a Cauchy sequence, so it converges. Set

$$\xi = \lim_{n\to\infty} \xi_n.$$

By (2.44), we deduce that, for any $n \in \mathbb{N}^*$, we have

$$|\xi_n - \xi| \ll c^n A_n^{-3/2},$$

and thus

$$|A_n\xi - y_n| \ll c^n A_n^{-1/2}. \tag{2.56}$$

By Step 1, this implies that

$$\|\mathbf{x}_{n+1}\| \asymp \|\mathbf{x}_{n+1}^-\| \asymp \|\mathbf{x}_n^-\|^{3/2} \asymp \|\mathbf{x}_n\|^{3/2},$$

and that

$$L(\mathbf{x}_n) = \max\{L'(\mathbf{x}_n^-), |A_n\xi - y_n|\} \ll c^n A_n^{-1/2} \ll c^n \|\mathbf{x}_n\|^{-1/2}.$$

Note that $\lim_{n\to\infty} L(\mathbf{x}_n) = 0$ and $D_n \ne 0$ for all $n > 3$. By Lemma 2.2.4, this implies that $\xi \notin \mathbb{Q}(\alpha)$. So ξ and $(\mathbf{x}_n)_{n\in\mathbb{N}^*}$ satisfy all the required conditions. □

Remark 2.8.5. If we replace $3/2$ by a real number r with $1 < r < 3/2$ in the construction of $(s_n)_{n\in\mathbb{N}^*}$ in Step 1 and argue as Steps 2, 3, then we obtain a sequence $(\mathbf{x}_n)_{n\in\mathbb{N}^*}$ in $\mathbb{Z}^4$ and a number $\xi \notin \mathbb{Q}(\alpha)$ satisfying (i)" $\det(\mathbf{x}_n, \ldots, \mathbf{x}_{n+3}) \neq 0$,

(ii)" $\|\mathbf{x}_{n+1}\| \asymp \|\mathbf{x}_n\|^r$,

(iii)" $L'(\mathbf{x}_n^-) \asymp \|\mathbf{x}_n^-\|^{-1/2}$ and $L(\mathbf{x}_n) \ll c'^n A_n^{-(r-1)} \ll c'^n \|\mathbf{x}_n\|^{-(r-1)}$,

(iv)" $\varphi(\mathbf{x}_n^-) = 1$,

where the constant c' only depends on r.

The property (iii)" derives from

$$|\xi_n - \xi_{n-1}| \ll A_{n-1}^{-r} \left(\left| \frac{D_n}{D_{n,0}} \right| + c'^{n-2} \varepsilon^{s_n - \frac{3}{2} s_{n-1}} \right) \ll A_{n-1}^{-r},$$

using $|D_n| < |D_{n,0}|$. Therefore, if we could make $\left|\frac{D_n}{D_{n,0}}\right|$ much smaller than 1 for some $r < 3/2$, then we could improve on (iii)" or (iii)'.

Chapter 3

On the dual Diophantine problem

3.1 Introduction

Let $\boldsymbol{\theta} = (1, \theta_1, \dots, \theta_d) \in \mathbb{R}^{d+1}$. We denote by $\hat{\tau}(\boldsymbol{\theta})$ the supremum of the real numbers τ for which there exists a constant $c > 0$ such that the convex body

$$\mathcal{C}^*_{c,X,\tau} : \begin{cases} |x_0 + x_1\theta_1 + \cdots + x_d\theta_d| \leq cX^{-\tau} \\ |x_1|, \dots, |x_d| \leq X \end{cases} \tag{3.1}$$

contains a non-zero point $(x_0, x_1, \dots, x_d) \in \mathbb{Z}^{d+1}$ for any sufficiently large value of X. Note that

$$\mathrm{vol}(\mathcal{C}^*_{c,X,\tau}) = c2^{d+1}X^{d-\tau}.$$

By Minkowski's First Convex Body Theorem, we deduce that if $\tau = d$ and $c = 1$, then the convex body $\mathcal{C}^*_{c,X,\tau}$ contains a non-zero point in $\mathbb{Z}^{d+1}$ for each $X > 0$. This implies that

$$\hat{\tau}(\boldsymbol{\theta}) \geq d.$$

The main goal of this chapter is to prove the following result.

Theorem 3.1.1. *Let α be an algebraic number of degree $d \geq 2$ and let $\xi \in \mathbb{R} \setminus \mathbb{Q}(\alpha)$.*

Let $\tau, c > 0$. Suppose that the inequalities

$$\begin{cases} |x_0 + x_1\alpha + \cdots + x_{d-1}\alpha^{d-1} + x_d\xi| \le cX^{-\tau} \\ |x_1|, \dots, |x_d| \le X \end{cases} \tag{3.2}$$

admit a solution $\mathbf{x} = (x_0, \dots, x_d) \in \mathbb{Z}^{d+1} \setminus \{0\}$ for any sufficiently large value of X. Then we have

$$\tau \le \tau_d := \frac{1+\sqrt{5}}{2}(d-1) + 1.$$

In the notation introduced above, this means that

$$\hat{\tau}(\boldsymbol{\theta}) \le \tau_d \quad \text{where} \quad \boldsymbol{\theta} = (1, \alpha, \dots, \alpha^{d-1}, \xi).$$

In fact, when $d = 2$, the estimate $\hat{\tau}(1, \alpha, \xi) \le \tau_2 = \gamma^2$ can be deduced from the upper bound $\hat{\lambda}(1, \alpha, \xi) \le \lambda_2 = 1/\gamma$ from Chapter 2. Indeed, Jarník's transference principle ([11]) gives

$$\hat{\tau}(1, \alpha, \xi) = \frac{1}{1 - \hat{\lambda}(1, \alpha, \xi)} \le \frac{1}{1 - 1/\gamma} = \gamma^2.$$

Moreover, it is shown in [22] that, given a quadratic number α, there exists $\xi \in \mathbb{R} \setminus \mathbb{Q}(\alpha)$ such that $\hat{\lambda}(1, \alpha, \xi) = 1/\gamma$ and so $\hat{\tau}(1, \alpha, \xi) = \gamma^2$. Therefore, the estimate $\hat{\tau}(\boldsymbol{\theta}) \le \tau_d$ is optimal for $d = 2$. We don't know if it is best possible for $d \ge 3$.

Based on the main result of Y. Bugeaud and M. Laurent in [3], arguing as in Section 3.2, we obtain the following result.

Corollary 3.1.2. *Let the notation be as in Theorem 3.1.1. Assume that $\tau > \tau_d$. Then, for any $\boldsymbol{\eta} = (\eta_0, \dots, \eta_d) \in \mathbb{R}^{d+1}$, there are arbitrarily large real numbers X such that the inequalities*

$$\begin{cases} |x_0\alpha^i - x_i - \eta_i| \ll X^{-1/\tau} \quad (1 \le i < d), \\ |x_0\xi - x_d - \eta_d| \ll X^{-1/\tau}, \\ \|\mathbf{x}\| \le X \end{cases}$$

have a non-zero solution $\mathbf{x} = (x_0, \dots, x_d)$ in $\mathbb{Z}^{d+1}$.

To prove our main result, we start, as in Chapter 2, with the construction of a sequence of minimal points $(\mathbf{x}_i)_{i\in\mathbb{N}}$ attached to the point $\boldsymbol{\theta} = (1, \alpha, \dots, \alpha^{d-1}, \xi)$ or more precisely to its associated map $T_{\boldsymbol{\theta}}(\mathbf{x}) = |\mathbf{x}\cdot\boldsymbol{\theta}|$ for each $\mathbf{x} \in \mathbb{Z}^{d+1}$. We then establish some basic properties of this sequence, assuming that the system (3.2) has a non-zero integer solution for each sufficiently large real number X and some fixed $\tau > 0$. This is similar to [6] and occupies Section 3.2. However, by contrast to [6], it is not so easy to show there exist infinitely many indices $i \in \mathbb{N}$ such that $\mathbf{x}_i$, $\mathbf{x}_{i+1}$ and $\mathbf{x}_{i+2}$ are linearly independent over $\mathbb{Q}$. To prove this, we require that $\tau > 1$. Then we denote by I the infinite set of all those indices i, and endow it with the natural ordering of integers.

The proof of the theorem itself uses three main estimates. Two of them are obtained in a similar way, by working with several linearly independent minimal points to produce a polynomial in α with small non-zero absolute value and then by using Liouville's inequality to bound from below this absolute value. For two points, this is done in Section 3.2 through an explicit construction. The result is an upper bound for the norm of any minimal point in terms of the norm of the preceding point. For three points however, our construction is not explicit as we obtain it through an application of Dirichlet's box principle. The resulting estimate is established in Section 3.3. The triples of points that we use for this purpose are of the form $(\mathbf{x}_{i+1}, \mathbf{x}_{j+1}, \mathbf{x}_{j+2})$ for consecutive elements $i < j$ in I, such triples being linearly independent. The last ingredient that we need uses the fact that, for such pairs (i, j), we have $\langle \mathbf{x}_{i+1}, \mathbf{x}_{i+2}\rangle_{\mathbb{Z}} = \langle \mathbf{x}_j, \mathbf{x}_{j+1}\rangle_{\mathbb{Z}}$ and so $\|\mathbf{x}_{i+1} \wedge \mathbf{x}_{i+2}\| = \|\mathbf{x}_j \wedge \mathbf{x}_{j+1}\|$. A useful inequality then follows by estimating these norms.

The estimates obtained in Section 3.2 already imply a first upper bound for $\hat{\tau}(\boldsymbol{\theta})$, namely $\hat{\tau}(\boldsymbol{\theta}) \le 2d - 1$. Combining the estimates of Section 3.2 with those of Section 3.3, we prove in Section 3.4 the stronger estimate $\hat{\tau}(\boldsymbol{\theta}) \le \tau_d$ of Theorem 3.1.1.

In the last section, we obtain one more general estimate through the construction of explicit non-zero polynomial maps from $(\mathbb{Q}^{d+1})$ to $\mathbb{Q}$ which do not vanish simultaneously on any triple of linearly independent points in $\mathbb{Q}^d \times \{0\}$. Using this estimate (in place of an estimate constructed in Section 3.3), we obtain an alternative proof for Theorem 3.1.1 in the case where $d = 3$.

Notation. For any $\mathbf{x} = (x_0, x_1, \ldots, x_d)$ in $\mathbb{R}^{d+1}$, we define $\mathbf{x}^- = (x_0, \ldots, x_{d-1})$ and $\mathbf{x}^+ = (x_1, \ldots, x_d)$. For each point $\boldsymbol{\theta} = (\theta_0, \ldots, \theta_d)$ in $\mathbb{R}^{d+1}$, we define a function $T_{\boldsymbol{\theta}} : \mathbb{R}^{d+1} \longrightarrow \mathbb{R}$ by

$$T_{\boldsymbol{\theta}}(\mathbf{x}) = |\mathbf{x} \cdot \boldsymbol{\theta}| = |x_0\theta_0 + x_1\theta_1 + \cdots + x_d\theta_d|.$$

3.2 Sequences of minimal points associated to $T_{\boldsymbol{\theta}}$

Fix a point $\boldsymbol{\theta} = (1, \theta_1, \ldots, \theta_d)$ of $\mathbb{R}^{d+1}$ with $\mathbb{Q}$–linearly independent coordinates. Replacing $L_{\boldsymbol{\theta}}$ by $T_{\boldsymbol{\theta}}$ in the construction of minimal points in section 2 of chapter 2, we obtain a sequence of points $(\mathbf{x}_i)_{i\in\mathbb{N}} \subset \mathbb{Z}^{d+1}$ such that

(a) $\mathbf{x}_i$ is primitive for each $i \in \mathbb{N}$,

(b) the norms $X_i = \|\mathbf{x}_i\|$ form a strictly increasing sequence,

(c) the positive real numbers $T_i = T_{\boldsymbol{\theta}}(\mathbf{x}_i)$ form a strictly decreasing sequence,

(d) if a non-zero point $\mathbf{x} \in \mathbb{Z}^{d+1}$ satisfies $T_{\boldsymbol{\theta}}(\mathbf{x}) < T_i$ for some $i \geq 1$ then $\|\mathbf{x}\| \geq X_{i+1}$.

The sequences of minimal points associated to $T_{\boldsymbol{\theta}}$ are uniquely determined up to the choice of their first points. We fix such a sequence $(\mathbf{x}_i)_{i\in\mathbb{N}}$ and denote by $(x_{i,0}, \ldots, x_{i,d})$ the coordinates of $\mathbf{x}_i$ for each i.

Arguing as Daverport and Schmidt in [7, Lemma 2], we also find that, for each i, the points $\mathbf{x}_i, \mathbf{x}_{i+1}$ constitute an integral basis for all integer points in the plane through the origin and these two points. More precisely, we have the following result.

Lemma 3.2.1. *For each index i, the two points $\mathbf{x}_i$ and $\mathbf{x}_{i+1}$ are $\mathbb{R}$-linearly independent and satisfy*

$$\langle \mathbf{x}_i, \mathbf{x}_{i+1} \rangle_{\mathbb{R}} \cap \mathbb{Z}^{d+1} = \langle \mathbf{x}_i, \mathbf{x}_{i+1} \rangle_{\mathbb{Z}}.$$

Proof. Since $\mathbf{x}_i$ and $\mathbf{x}_{i+1}$ are primitive integer points with different norms, they are $\mathbb{R}$-linearly independent.

Assume that $\langle \mathbf{x}_i, \mathbf{x}_{i+1} \rangle_{\mathbb{R}} \cap \mathbb{Z}^{d+1} \neq \langle \mathbf{x}_i, \mathbf{x}_{i+1} \rangle_{\mathbb{Z}}$. Then there exists a point of the form $\mathbf{y} = r\mathbf{x}_i + s\mathbf{x}_{i+1} \in \langle \mathbf{x}_i, \mathbf{x}_{i+1} \rangle_{\mathbb{R}} \cap \mathbb{Z}^{d+1}$ for some $(r, s) \in \mathbb{R} \setminus \{0\}$ with $|r|, |s| \leq 1/2$. This implies that

$$\|\mathbf{y}\| \leq |r|X_i + |s|X_{i+1} < X_{i+1}, \qquad T_{\boldsymbol{\theta}}(\mathbf{y}) \leq |r|T_i + |s|T_{i+1} < T_i,$$

which is impossible because of property (d) of the sequence $(\mathbf{x}_i)_{i \in \mathbb{N}}$. □

The next lemma is also a basic result to which we will refer repeatedly in the following.

Lemma 3.2.2. *Let the notation be as above and let $\tau, c > 0$. Assume that the system*

$$\begin{cases} |x_0 + x_1\theta_1 + \cdots + x_d\theta_d| \leq cX^{-\tau} \\ |x_1|, \ldots, |x_d| \leq X \end{cases} \tag{3.3}$$

admits a solution $\mathbf{x} = (x_0, \ldots, x_d) \in \mathbb{Z}^{d+1} \setminus \{0\}$ for any sufficiently large value of X.

(i) We have

$$T_i \ll X_{i+1}^{-\tau} \quad \textit{for all } i \geq 1.$$

(ii) If $\tau > 1$, then there exist infinitely many integers i such that the three points $\mathbf{x}_i, \mathbf{x}_{i+1}, \mathbf{x}_{i+2}$ are linearly independent over $\mathbb{R}$.

As we will see below, the proof of part (i) is quite standard following for example [6, page 399]. The proof of part (ii) however is more delicate.

Proof. (i) Set $c_0 = |\theta_1| + \cdots + |\theta_d| + c + 1$, and choose X_0 such that system (3.3) has a non-zero solution in $\mathbb{Z}^{d+1}$ for each $X \geq X_0$.

Fix an index i and a real number X with $X_0 \leq X < c_0^{-1}X_{i+1}$. Let $\mathbf{x} = (x_0, \ldots, x_d) \in \mathbb{Z}^{d+1} \setminus \{0\}$ be a solution to (3.3). Then we have

$$|x_1|, \ldots, |x_d| \leq X, \qquad T_{\boldsymbol{\theta}}(\mathbf{x}) \leq cX^{-\tau},$$

and so

$$\begin{aligned} \|\mathbf{x}\| &= \max\{|x_0|, |x_1|, \ldots, |x_d|\} \\ &\leq \max\{|x_1\theta_1| + \cdots + |x_d\theta_d| + cX^{-\tau}, X\} \\ &\leq c_0 X < X_{i+1}. \end{aligned}$$

Since the sequence $(\mathbf{x}_i)_{i\in\mathbb{N}}$ has property (d) , we deduce that

$$T_i \le T_{\boldsymbol{\theta}}(\mathbf{x}) \le cX^{-\tau}.$$

Since we can choose X arbitrarily close to $c_0^{-1}X_{i+1}$, we conclude that

$$T_i \le c(c_0^{-1}X_{i+1})^{-\tau}.$$

(ii) Assume on the contrary that there exists an integer n such that $\mathbf{x}_i, \mathbf{x}_{i+1}, \mathbf{x}_{i+2}$ are $\mathbb{R}$–linearly dependent for all $i \ge n$.

For each $i \ge n$, set $V_i = \langle \mathbf{x}_i, \mathbf{x}_{i+1}, \mathbf{x}_{i+2}\rangle_{\mathbb{R}}$. Then we have

$$\dim_{\mathbb{R}} V_i \le 2 \qquad \text{for} \quad i \ge n.$$

Since any two consecutive points of the sequence $(\mathbf{x}_i)_{i\in\mathbb{N}}$ are $\mathbb{R}$–linearly independent, we deduce that

$$V_i = \langle \mathbf{x}_{i+1}, \mathbf{x}_{i+2}\rangle_{\mathbb{R}} = V_{i+1} \qquad \text{for} \quad i \ge n.$$

So we find

$$V_n = V_{n+1} = V_{n+2} = \cdots$$

There exists a vector $\mathbf{y} \in V_n \setminus \{0\}$ such that $\mathbf{y} \cdot \boldsymbol{\theta} = 0$. Since $\boldsymbol{\theta}$ has $\mathbb{Q}$–linearly independent coordinates, we deduce that $\mathbf{y} \notin \langle \mathbf{x}_n \rangle_{\mathbb{R}}$ and thus $\{\mathbf{y}, \mathbf{x}_n\}$ is a basis of V_n.

Fix an index $i \ge n$. Since $\mathbf{x}_i \in V_i = V_n$, we can write

$$\mathbf{x}_i = a_i\mathbf{y} + b_i\mathbf{x}_n$$

for some $a_i, b_i \in \mathbb{R}$ with

$$\max\{|a_i|, |b_i|\} \asymp \|\mathbf{x}_i\| = X_i,$$

where the implied constants only depend on $\mathbf{y}$ and $\mathbf{x}_n$. Then we get

$$\mathbf{x}_i \wedge \mathbf{x}_{i+1} = \begin{vmatrix} a_i & b_i \\ a_{i+1} & b_{i+1} \end{vmatrix} (\mathbf{y} \wedge \mathbf{x}_n).$$

Moreover, we have

$$T_i = |\mathbf{x}_i \cdot \boldsymbol{\theta}| = |a_i(\mathbf{y} \cdot \boldsymbol{\theta}) + b_i(\mathbf{x}_n \cdot \boldsymbol{\theta})| \asymp |b_i|.$$

We deduce that

$$1 \ll \|\mathbf{x}_i \wedge \mathbf{x}_{i+1}\| \ll |a_{i+1}b_i - a_i b_{i+1}| \ll X_{i+1}T_i + X_i T_{i+1} \ll X_{i+1}T_i.$$

Since $T_i \ll X_{i+1}^{-\tau}$, we get $1 \ll X_{i+1}^{1-\tau}$. This is impossible if $\tau > 1$ and if i is large enough. This shows that there exist infinitely many i such that $\mathbf{x}_i, \mathbf{x}_{i+1}, \mathbf{x}_{i+2}$ are linearly independent over $\mathbb{R}$. □

Considering pairs of consecutive points of $(\mathbf{x}_i)_{i\in\mathbb{N}}$ and applying Liouville's inequality, we get the following result.

Lemma 3.2.3. *Suppose that $\boldsymbol{\theta} = (1, \alpha, \ldots, \alpha^{d-1}, \xi)$ where α is an algebraic number of degree $d \geq 2$ and where $\xi \in \mathbb{R} \setminus \mathbb{Q}(\alpha)$. Let $c > 0$ and $\tau > d-1$. Assume that the system*

$$\begin{cases} |x_0 + x_1\alpha + \cdots + x_{d-1}\alpha^{d-1} + x_d\xi| \leq cX^{-\tau}, \\ |x_1|, \ldots, |x_d| \leq X \end{cases}$$

admits a solution $\mathbf{x} = (x_0, \ldots, x_d) \in \mathbb{Z}^{d+1} \setminus \{0\}$ for any sufficiently large value of X. Then we have $\tau \leq 2d-1$ and $\mathbf{x}_i^- \neq 0$, $x_{i,d} \neq 0$ for each sufficiently large index i. Moreover, if $\tau > d$, then we have $X_{i+1} \ll X_i^{\frac{d-1}{\tau-d}}$.

Proof. We first note, by Lemma 3.2.2 (i), that there exists a constant $c_1 = c_1(\alpha, \xi) > 0$ such that

$$T_{\boldsymbol{\theta}}(\mathbf{x}_i) = |x_{i,0} + x_{i,1}\alpha + \cdots + x_{i,d-1}\alpha^{d-1} + x_{i,d}\xi| \leq c_1 X_{i+1}^{-\tau}$$

for all $i \in \mathbb{N}$. If $\mathbf{x}_i^- = 0$, we find

$$|x_{i,d}| = X_i, \qquad |x_{i,d}\xi| \leq c_1 X_{i+1}^{-\tau},$$

and so i is bounded from above. Hence, there exists an integer N such that $\mathbf{x}_i^- \neq 0$ for all $i \geq N$. By Liouville's inequality, there exists a constant $c_2 = c_2(\alpha) > 0$ such that

$$|x_{i,0} + x_{i,1}\alpha + \cdots + x_{i,d-1}\alpha^{d-1}| \geq c_2\|\mathbf{x}_i^-\|^{-(d-1)} \geq c_2 X_i^{-(d-1)} \qquad \text{for } i \geq N.$$

Therefore, for any sufficiently large integer $i \geq N$, we get

$$\begin{aligned}|x_{i,d}\xi| &\geq |x_{i,0} + x_{i,1}\alpha + \cdots + x_{i,d-1}\alpha^{d-1}| - |x_{i,0} + x_{i,1}\alpha + \cdots + x_{i,d-1}\alpha^{d-1} + x_{i,d}\xi| \\ &\geq c_2 X_i^{-(d-1)} - c_1 X_{i+1}^{-\tau} > 0\end{aligned}$$

since $\tau > d-1$ and $X_i < X_{i+1}$. This means that $x_{i,d} \neq 0$ when i is sufficiently large. We deduce that there exists an integer N_0 such that

$$\mathbf{x}_i^- \neq 0, \quad x_{i,d} \neq 0 \quad \text{for each } i \geq N_0.$$

Fix an index $i \geq N_0$. We have $\mathbf{x}_i^- \neq 0,\ x_{i,d} \neq 0$ and $\mathbf{x}_{i+1}^- \neq 0,\ x_{i+1,d} \neq 0$. Since $\mathbf{x}_i, \mathbf{x}_{i+1}$ are linearly independent , we deduce that $x_{i+1,d}\mathbf{x}_i^- - x_{i,d}\mathbf{x}_{i+1}^- \neq 0$.

Set

$$D_i = (x_{i+1,d}\mathbf{x}_i^- - x_{i,d}\mathbf{x}_{i+1}^-) \cdot \boldsymbol{\theta}^-.$$

Then

$$D_i = (x_{i+1,d}x_{i,0} - x_{i,d}x_{i+1,0}) + \cdots + (x_{i+1,d}x_{i,d-1} - x_{i,d}x_{i+1,d-1})\alpha^{d-1}$$

is a non-zero polynomial in α with integer coefficients of absolute value $\ll X_i X_{i+1}$. Applying Liouville's inequality, we then deduce that

$$|D_i| \gg (X_{i+1}X_i)^{-(d-1)}.$$

On the other hand, we have

$$|D_i| = |x_{i+1,d}(\mathbf{x}_i \cdot \boldsymbol{\theta}) - x_{i,d}(\mathbf{x}_{i+1} \cdot \boldsymbol{\theta})| \leq T_i X_{i+1} + T_{i+1} X_i \ll T_i X_{i+1}.$$

Therefore, we get

$$(X_{i+1}X_i)^{-(d-1)} \ll T_i X_{i+1} \ll X_{i+1}^{-(\tau-1)},$$

using Lemma 3.2.2 (i), and so

$$X_{i+1}^{\tau-d} \ll X_i^{d-1}.$$

Since $X_{i+1} > X_i$, this implies that $\tau - d \leq d-1$, *i.e.*, $\tau \leq 2d-1$. In particular, if $\tau > d$, then $X_{i+1} \ll X_i^{(d-1)/(\tau-d)}$. □

3.3 The set I

Fix an integer $d \geq 2$ and a point $\boldsymbol{\theta} = (\theta_0, \dots, \theta_d)$ in $\mathbb{R}^{d+1}$ with $\mathbb{Q}$-linearly independent coordinates. We fix a sequence of minimal points $(\mathbf{x}_i)_{i\in\mathbb{N}}$ attached to $T_{\boldsymbol{\theta}}$ with norms X_i and $T_i = T_{\boldsymbol{\theta}}(\mathbf{x}_i)$(see section 2). Let $\tau > 1$, and $c > 0$. Assume that the system

$$\begin{cases} |x_0 + x_1\theta_1 + \cdots + x_d\theta_d| \leq cX^{-\tau} \\ |x_1|, \dots, |x_d| \leq X \end{cases}$$

admits a solution $\mathbf{x} = (x_0, \dots, x_d) \in \mathbb{Z}^{d+1} \setminus \{0\}$ for any sufficiently large value of X. Then it follows from Lemma 3.2.2 (ii) that the set

$$I = \{i \in \mathbb{N};\ \mathbf{x}_i, \mathbf{x}_{i+1}, \mathbf{x}_{i+2} \text{ are } \mathbb{R}\text{-linearly independent } \}$$

is infinite.

We endow I with the natural ordering of integers. Let $i < j$ be consecutive elements in I. For each index t with $i+1 \leq t < j$, the points $\mathbf{x}_t, \mathbf{x}_{t+1}, \mathbf{x}_{t+2}$ are $\mathbb{R}$-linearly dependent. Since any two distinct points of $(\mathbf{x}_i)_{i\in\mathbb{N}}$ are $\mathbb{R}$-linearly independent, for such t, we find that

$$\langle \mathbf{x}_t, \mathbf{x}_{t+1} \rangle_{\mathbb{R}} = \langle \mathbf{x}_{t+1}, \mathbf{x}_{t+2} \rangle_{\mathbb{R}}.$$

This means that

$$\langle \mathbf{x}_{i+1}, \mathbf{x}_{i+2} \rangle_{\mathbb{R}} = \cdots = \langle \mathbf{x}_j, \mathbf{x}_{j+1} \rangle_{\mathbb{R}}. \tag{3.4}$$

Then, Lemma 3.2.1 gives that

$$\langle \mathbf{x}_{i+1}, \mathbf{x}_{i+2} \rangle_{\mathbb{Z}} = \cdots = \langle \mathbf{x}_j, \mathbf{x}_{j+1} \rangle_{\mathbb{Z}}.$$

On the other hand, it follows from (3.4) that

$$\langle \mathbf{x}_{i+1}, \dots, \mathbf{x}_{j+1} \rangle_{\mathbb{R}} = \langle \mathbf{x}_\ell, \mathbf{x}_{\ell'} \rangle_{\mathbb{R}} \tag{3.5}$$

for any $\ell, \ell' \in \mathbb{N}$ such that $i+1 \leq \ell < \ell' \leq j+1$. We deduce that $\mathbf{x}_i,\ \mathbf{x}_\ell, \mathbf{x}_{\ell'}$ are linearly independent and so are $\mathbf{x}_\ell, \mathbf{x}_{\ell'}, \mathbf{x}_{j+2}$ for any $\ell, \ell' \in \mathbb{N}$ such that $i+1 \leq \ell < \ell' \leq j+1$.

The following lemma allows us to exploit the properties (3.5).

Lemma 3.3.1. *Let $\mathbf{y}_1, \mathbf{y}_2, \mathbf{y}_3, \mathbf{y}_4$ be primitive points in $\mathbb{Z}^{d+1}$ and let $\eta > 1$ such that* *(i)* $\eta\|\mathbf{y}_1\| < \|\mathbf{y}_2\| \le \|\mathbf{y}_3\| < \|\mathbf{y}_4\|$,

(ii) $|\mathbf{y}_1 \cdot \boldsymbol{\theta}| > |\mathbf{y}_2 \cdot \boldsymbol{\theta}| \ge |\mathbf{y}_3 \cdot \boldsymbol{\theta}| > |\mathbf{y}_4 \cdot \boldsymbol{\theta}|$,

(iii) $\langle \mathbf{y}_1, \mathbf{y}_2 \rangle_{\mathbb{Z}} = \langle \mathbf{y}_3, \mathbf{y}_4 \rangle_{\mathbb{Z}}$.

Then we have

$$\|\mathbf{y}_2\||\mathbf{y}_1 \cdot \boldsymbol{\theta}| \ll_\eta \|\mathbf{y}_4\||\mathbf{y}_3 \cdot \boldsymbol{\theta}|.$$

Proof. Since $\mathbf{y}_1, \mathbf{y}_2$ are primitive and have distinct norms, they are $\mathbb{R}$-linearly independent. So it follows from condition (iii) that

$$\langle \mathbf{y}_1, \mathbf{y}_2 \rangle_{\mathbb{R}} = \langle \mathbf{y}_3, \mathbf{y}_4 \rangle_{\mathbb{R}} =: V$$

has dimension 2. Then there exists a point $\mathbf{y} \in V$ such that $\mathbf{y} \cdot \boldsymbol{\theta} = 0$. Since $\boldsymbol{\theta}$ has $\mathbb{Q}$-linearly independent coordinates, we get $\mathbf{y}_1 \cdot \boldsymbol{\theta} \neq 0$ and so $\mathbf{y} \notin \langle \mathbf{y}_1 \rangle_{\mathbb{R}}$. This shows that

$$V = \langle \mathbf{y}, \mathbf{y}_1 \rangle_{\mathbb{R}}.$$

For each $t = 2, 3, 4$, we write

$$\mathbf{y}_t = a_t \mathbf{y} + b_t \mathbf{y}_1$$

for some $a_t,\ b_t \in \mathbb{R}$. Then we get

$$\mathbf{y}_t \cdot \boldsymbol{\theta} = b_t(\mathbf{y}_1 \cdot \boldsymbol{\theta}),$$

and so

$$|b_t| = \frac{|\mathbf{y}_t \cdot \boldsymbol{\theta}|}{|\mathbf{y}_1 \cdot \boldsymbol{\theta}|}. \tag{3.6}$$

Since $|\mathbf{y}_1 \cdot \boldsymbol{\theta}| > |\mathbf{y}_t \cdot \boldsymbol{\theta}|$, we get $|b_t| < 1$ and thus $\|b_t \mathbf{y}_1\| < \|\mathbf{y}_1\| < \|\mathbf{y}_t\|$. So we get

$$\left(1 - \frac{1}{\eta}\right) \|\mathbf{y}_t\| \le \|\mathbf{y}_t\| - \|\mathbf{y}_1\| \le \|a_t \mathbf{y}\| \le \|\mathbf{y}_t\| + \|\mathbf{y}_1\| \le 2\|\mathbf{y}_t\|$$

and therefore, we find

$$|a_t| \asymp_\eta \frac{\|\mathbf{y}_t\|}{\|\mathbf{y}\|}. \tag{3.7}$$

Since $\langle \mathbf{y}_1,\ \mathbf{y}_2 \rangle_{\mathbb{Z}} = \langle \mathbf{y}_3,\ \mathbf{y}_4 \rangle_{\mathbb{Z}}$, we have

$$\|\mathbf{y}_1 \wedge \mathbf{y}_2\| = \|\mathbf{y}_3 \wedge \mathbf{y}_4\|.$$

We also have

$$\mathbf{y}_1 \wedge \mathbf{y}_2 = \mathbf{y}_1 \wedge (a_2\mathbf{y} + b_2\mathbf{y}_1) = a_2(\mathbf{y}_1 \wedge \mathbf{y}).$$

and

$$\mathbf{y}_3 \wedge \mathbf{y}_4 = -\begin{vmatrix} a_3 & b_3 \\ a_4 & b_4 \end{vmatrix} (\mathbf{y}_1 \wedge \mathbf{y})$$

This implies that

$$|a_2| = |a_3b_4 - a_4b_3| \leq |a_3b_4| + |a_4b_3|.$$

Using (3.6) and (3.7), we deduce that

$$\frac{\|\mathbf{y}_2\|}{\|\mathbf{y}_1\|} \ll_\eta \frac{\|\mathbf{y}_3\|}{\|\mathbf{y}_1\|} \cdot \frac{|\mathbf{y}_4 \cdot \boldsymbol{\theta}|}{|\mathbf{y}_1 \cdot \boldsymbol{\theta}|} + \frac{\|\mathbf{y}_4\|}{\|\mathbf{y}_1\|} \cdot \frac{|\mathbf{y}_3 \cdot \boldsymbol{\theta}|}{|\mathbf{y}_1 \cdot \boldsymbol{\theta}|} \leq 2\frac{\|\mathbf{y}_4\|}{\|\mathbf{y}_1\|} \cdot \frac{|\mathbf{y}_3 \cdot \boldsymbol{\theta}|}{|\mathbf{y}_1 \cdot \boldsymbol{\theta}|},$$

which proves the required inequality. □

The following lemma provides an estimate which can be applied to any triple of linearly independent points of $(\mathbf{x}_i)_{i\in\mathbb{N}}$.

Lemma 3.3.2. *Suppose that $\boldsymbol{\theta} = (1, \alpha, \dots, \alpha^{d-1}, \xi)$ where α is an algebraic number of degree d and $\xi \notin \mathbb{Q}(\alpha)$. Let $\mathbf{x}, \mathbf{y}, \mathbf{z}$ be linearly independent points in $\mathbb{Z}^{d+1}$. Assume that*

$$\|\mathbf{x}\| \leq \|\mathbf{y}\| \leq \|\mathbf{z}\|$$

$$|\mathbf{x} \cdot \boldsymbol{\theta}| \geq |\mathbf{y} \cdot \boldsymbol{\theta}| \geq |\mathbf{z} \cdot \boldsymbol{\theta}|$$

Then we have

$$\|\mathbf{x}\| \ll (\|\mathbf{x}\| \cdot \|\mathbf{y}\| \cdot \|\mathbf{z}\|)^{d/2} \, |\mathbf{x} \cdot \boldsymbol{\theta}|.$$

Proof. Put $M = 9(\|\mathbf{x}\| \cdot \|\mathbf{y}\| \cdot \|\mathbf{z}\|)^{1/2}$. We consider the set

$$S = \left\{ (a, b, c) \in \mathbb{Z}^3; 0 \leq a \leq \frac{M}{3\|\mathbf{x}\|}, 0 \leq b \leq \frac{M}{3\|\mathbf{y}\|}, 0 \leq c \leq \frac{M}{3\|\mathbf{z}\|} \right\}.$$

Its cardinality is

$$\begin{aligned} |S| &= \left(\left\lfloor \frac{M}{3\|\mathbf{x}\|} \right\rfloor + 1 \right) \left(\left\lfloor \frac{M}{3\|\mathbf{y}\|} \right\rfloor + 1 \right) \left(\left\lfloor \frac{M}{3\|\mathbf{z}\|} \right\rfloor + 1 \right) \\ &\geq \frac{M^3}{27\|\mathbf{x}\| \cdot \|\mathbf{y}\| \cdot \|\mathbf{z}\|}. \end{aligned}$$

For each $(a,b,c) \in S$, we have

$$ax_d + by_d + cz_d \in W := \{-M, -M+1, \dots, M\}.$$

Consider the map

$$\begin{array}{rccl} f: & S & \longrightarrow & W \\ & (a,b,c) & \longmapsto & ax_d + by_d + cz_d. \end{array}$$

Since $M = 9(\|\mathbf{x}\| \cdot \|\mathbf{y}\| \cdot \|\mathbf{z}\|)^{1/2}$, we have

$$|S| \geq \frac{M^3}{27\|\mathbf{x}\| \cdot \|\mathbf{y}\| \cdot \|\mathbf{z}\|} = 3M > 2M+1 = |W|.$$

We deduce that there exist at least two points of S, (a',b',c') and (a'',b'',c''), which have the same image under f. Set

$$(a,b,c) = (a',b',c') - (a'',b'',c'') \in \mathbb{Z}^3 \setminus \{0\}.$$

Then we find

$$ax_d + by_d + cz_d = 0. \tag{3.8}$$

Since $\mathbf{x}, \mathbf{y}, \mathbf{z}$ are linearly independent, we observe that

$$a\mathbf{x}^- + b\mathbf{y}^- + c\mathbf{z}^- \neq 0.$$

Set

$$P(T) = (ax_0 + by_0 + cz_0) + \cdots + (ax_{d-1} + by_{d-1} + cz_{d-1})T^{d-1}.$$

Then we get $P \in \mathbb{Z}[T]_{\leq d-1} \setminus \{0\}$. Since $0 \leq a', a'' \leq M/(3\|\mathbf{x}\|)$, we obtain that

$$|a| = |a' - a''| \leq \frac{M}{3\|\mathbf{x}\|}.$$

Similarly, we also get

$$|b| \leq \frac{M}{3\|\mathbf{y}\|}\ , \quad |c| \leq \frac{M}{3\|\mathbf{z}\|}.$$

This implies that

$$\|P\| = \|a\mathbf{x}^- + b\mathbf{y}^- + c\mathbf{z}^-\| \leq M.$$

Applying Liouville's inequality to $P(\alpha)$, we deduce that

$$M^{-(d-1)} \ll |P(\alpha)|.$$

On the other hand, using (3.8), we get

$$\begin{aligned}|P(\alpha)| &= |(a\mathbf{x}^- + b\mathbf{y}^- + c\mathbf{z}^-)\cdot\boldsymbol{\theta}^- + (ax_d + by_d + cz_d)\xi| \\ &= |a(\mathbf{x}\cdot\boldsymbol{\theta}) + b(\mathbf{y}\cdot\boldsymbol{\theta}) + c(\mathbf{z}\cdot\boldsymbol{\theta})| \\ &\le \frac{M}{3\|\mathbf{x}\|}|\mathbf{x}\cdot\boldsymbol{\theta}| + \frac{M}{3\|\mathbf{y}\|}|\mathbf{y}\cdot\boldsymbol{\theta}| + \frac{M}{3\|\mathbf{z}\|}|\mathbf{z}\cdot\boldsymbol{\theta}| \\ &\le \frac{M}{\|\mathbf{x}\|}|\mathbf{x}\cdot\boldsymbol{\theta}|.\end{aligned}$$

So we conclude that

$$M^{-(d-1)} \ll \frac{M}{\|\mathbf{x}\|}|\mathbf{x}\cdot\boldsymbol{\theta}|,$$

which leads to

$$\|\mathbf{x}\| \ll M^d|\mathbf{x}\cdot\boldsymbol{\theta}| \asymp (\|\mathbf{x}\|\cdot\|\mathbf{y}\|\cdot\|\mathbf{z}\|)^{d/2}|\mathbf{x}\cdot\boldsymbol{\theta}|.$$ □

Applying the above lemmas to points of our sequence $(\mathbf{x}_i)_{i\in\mathbb{N}}$, we obtain the following result which summarizes the crucial properties that we need for the proof of Theorem 3.1.1.

Proposition 3.3.3. *Suppose that $\boldsymbol{\theta} = (1, \alpha, \dots, \alpha^{d-1}, \xi)$ where α is an algebraic number of degree d and $\xi \notin \mathbb{Q}(\alpha)$. Let $i < j$ be two consecutive indices in I. Then we have*

(i) $X_{i+1} \ll (X_{i+1}X_{i+2}X_{j+2})^{d/2}T_{i+1}$,

(ii) $X_{i+2}T_{i+1} \ll X_{j+1}T_j$ *if* $\tau > (3/2)d - 1$.

Proof. Since $i < j$ are consecutive indices in I, we have

$$\langle \mathbf{x}_{i+1}, \mathbf{x}_{i+2}\rangle_{\mathbb{R}} = \cdots = \langle \mathbf{x}_j, \mathbf{x}_{j+1}\rangle_{\mathbb{R}} := V \qquad \text{(see (3.4))}.$$

Moreover, $\mathbf{x}_j, \mathbf{x}_{j+1}, \mathbf{x}_{j+2}$ are $\mathbb{R}$–linearly independent and thus $\mathbf{x}_{i+1}, \mathbf{x}_{i+2}, \mathbf{x}_{j+2}$ are $\mathbb{R}$–linearly independent. Applying Lemma 3.3.2 to $\mathbf{x}_{i+1}, \mathbf{x}_{i+2}, \mathbf{x}_{j+2}$, we get (i).

To prove assertion (ii), we first note that

$$V \cap \mathbb{Z}^{d+1} = \langle \mathbf{x}_{i+1}, \mathbf{x}_{i+2} \rangle_{\mathbb{Z}} = \langle \mathbf{x}_j, \mathbf{x}_{j+1} \rangle_{\mathbb{Z}},$$

according to Lemma 3.2.1. Now, suppose that there exist infinitely many $i \in I$ such that

$$X_{i+2} \leq 2X_{i+1}.$$

Then, for such i, applying Lemma 3.3.2 to the $\mathbb{R}$–linearly independent points $\mathbf{x}_i, \mathbf{x}_{i+1}, \mathbf{x}_{i+2}$ and using $X_i < X_{i+1}, T_i \leq X_{i+1}^{-\tau}$, we get

$$1 \ll X_i^{d/2-1} X_{i+1}^{d/2} X_{i+2}^{d/2} T_i \ll X_{i+1}^{-1-\tau+(3/2)d}.$$

Since this holds for infinitely many i, we deduce that $\tau \leq (3/2)d - 1$. So if $\tau > (3/2)d - 1$, we get $X_{i+2} > 2X_{i+1}$ for each sufficiently large $i \in I$. Then we may apply Lemma 3.3.1 to $\mathbf{x}_{i+1}, \mathbf{x}_{i+2}, \mathbf{x}_j, \mathbf{x}_{j+1}$ with $\eta = 2$ and this yields the inequality in (ii). □

3.4 Proof of Theorem 3.1.1

Assume that $\tau > (3/2)d - 1$. We will show that $\tau \leq \tau_d$.

First of all, we fix a sequence of minimal points $(\mathbf{x}_i)_{i \in \mathbb{N}}$ in $\mathbb{Z}^{d+1}$ attached to $T_{\boldsymbol{\theta}}$. We know that the corresponding set I is infinite. Set

$$\rho = \inf\{r \geq 1; X_{i+2} \leq X_{i+1}^r \text{ for all sufficiently large } i \in I\}.$$

Lemma 3.2.3 gives

$$X_{i+1} \ll X_i^{(d-1)/(\tau-d)} \quad \text{for each } i \in \mathbb{N}.$$

So we find

$$1 \leq \rho \leq \frac{d-1}{\tau - d}. \tag{3.9}$$

Now fix a real number ε with $0 < \varepsilon < \rho$. Then by the definition of ρ, there exist infinitely many $i \in I$ such that

$$X_{i+2} \geq X_{i+1}^{\rho-\varepsilon}. \tag{3.10}$$

Fix such an index i and let j be the next element in I. By the definition of ρ, we get

$$X_{j+2} \le X_{j+1}^{\rho+\varepsilon} \tag{3.11}$$

if i is large enough. Combining Proposition 3.3.3 with the above two inequalities, we get

$$\begin{aligned}
1 &\ll X_{i+1}^{d/2-1} X_{i+2}^{d/2} X_{j+2}^{d/2} T_{i+1} \\
&\ll X_{i+2}^{(d/2-1)(1/(\rho-\varepsilon))} X_{i+2}^{d/2-1} X_{j+2}^{d/2} (X_{i+2} T_{i+1}) \\
&\ll X_{i+2}^{(d/2-1)(1/(\rho-\varepsilon)+1)} X_{j+2}^{d/2} (X_{j+1} T_j) \\
&\ll X_{i+2}^{(d/2-1)(1/(\rho-\varepsilon)+1)} X_{j+1}^{(d/2)(\rho+\varepsilon)+1-\tau} \qquad \text{(using } T_j \le X_{j+1}^{-\tau}\text{)},
\end{aligned}$$

thus

$$X_{j+1}^{\tau-1-(d/2)(\rho+\varepsilon)} \ll X_{i+2}^{(d/2-1)(1/(\rho-\varepsilon)+1)}.$$

This holds for infinitely many $i \in I$. Since $(X_i)_{i\in I}$ is strictly increasing and since $j+1 \le i+2$, we deduce that

$$\tau - 1 - \frac{d}{2}(\rho+\varepsilon) \le \left(\frac{d}{2} - 1\right)\left(\frac{1}{\rho-\varepsilon} + 1\right).$$

Since ε can be chosen arbitrarily small, we conclude that

$$\tau - 1 - \frac{d}{2}\rho \le \left(\frac{d}{2} - 1\right)\left(\frac{1}{\rho} + 1\right).$$

This implies that

$$\tau - \frac{d}{2} \le \frac{d}{2}\rho + \left(\frac{d}{2} - 1\right)\frac{1}{\rho}$$

Noting that ρ belongs to $[1, (d-1)/(\tau-d)]$ and that the right hand side of the above estimate is an increasing function of ρ on $[1, \infty)$, we get

$$\tau - \frac{d}{2} \le \frac{d(d-1)}{2(\tau-d)} + \left(\frac{d}{2} - 1\right)\frac{\tau-d}{d-1}.$$

Since $\tau > (3/2)d - 1 \ge d$, this yields

$$\tau^2 - (d+1)\tau - d^2 + 3d - 1 \le 0,$$

which implies that $\tau \le \tau_d$.

3.5 Alternative approach using polynomials

Let α be an algebraic integer of degree $d \geq 3$ and let $\xi \in \mathbb{R} \setminus \mathbb{Q}(\alpha)$. Set $\boldsymbol{\theta} = (1, \alpha, \dots, \alpha^{d-1}, \xi)$. We fix a sequence of minimal points $(\mathbf{x}_i)_{i \in \mathbb{N}}$ attached to $T_{\boldsymbol{\theta}}$ and set $X_i = \|\mathbf{x}_i\|$ and $T_i = T_{\boldsymbol{\theta}}(\mathbf{x}_i)$.

Recall that, in Section 3.3, we defined the set

$$I = \{i \in \mathbb{N};\ \mathbf{x}_i, \mathbf{x}_{i+1}, \mathbf{x}_{i+2} \text{ are linearly independent}\}.$$

We showed that this set is infinite if $\hat{\tau}(\boldsymbol{\theta}) > 1$ (Lemma 3.2.2). Moreover, by using Dirichlet's Box principle, we proved that

$$X_{i+1} \ll (X_{i+1} X_{i+2} X_{j+2})^{d/2} T_{i+1} \tag{3.12}$$

for any consecutive elements $i < j$ in I. This was the crucial estimate in the proof of Theorem 3.1.1.

In this section, we construct non-zero polynomial maps from $(\mathbb{Q}^{d+1})^3$ to $\mathbb{Q}$ which are defined over $\mathbb{Z}$ and do not simultaneously vanish on any triple of linearly independent points of $\mathbb{Q}^d \times \{0\}$. Looking at the values of these polynomials at $(\mathbf{x}_{i+1}, \mathbf{x}_{i+2}, \mathbf{x}_{j+2})$ where i, j are consecutive elements of I, we will show that

$$1 \ll X_{i+1}^{d-2} X_{i+2}^{d-1} X_{j+2} T_{i+1}.$$

Using this estimate instead of (3.12), we will then provide an alternative proof for Theorem 3.1.1 in the case where $d = 3$.

To construct the polynomial maps, we first note that, for each $j \in \mathbb{N}$, and each $\mathbf{y} \in \mathbb{Q}^d \times \{0\}$, we have

$$\alpha^j (\mathbf{y} \cdot \boldsymbol{\theta}) \in \mathbb{Q}(\alpha).$$

Fix $j \in \mathbb{N}$. Since $\{1, \alpha, \dots, \alpha^{d-1}\}$ is a basis of $\mathbb{Q}(\alpha)$, there exists a unique point $\mathbf{y}_j \in \mathbb{Q}^d \times \{0\}$ such that

$$\alpha^j (\mathbf{y} \cdot \boldsymbol{\theta}) = \mathbf{y}_j \cdot \boldsymbol{\theta}.$$

In particular, if $\mathbf{y} \in \mathbb{Z}^d \times \{0\}$, then

$$\alpha^j (\mathbf{y} \cdot \boldsymbol{\theta}) \in \langle 1, \alpha, \dots, \alpha^{d-1} \rangle_{\mathbb{Z}}$$

since α is an algebraic integer, and so $\mathbf{y}_j \in \mathbb{Z}^d \times \{0\}$.

To estimate the norm of $\mathbf{y}_j$, we consider the map

$$\begin{aligned} \mathcal{T}_j : \mathbb{Q}^d \times \{0\} &\longrightarrow \mathbb{Q}^d \times \{0\} \\ \mathbf{y} &\longmapsto \mathbf{y}_j. \end{aligned}$$

Since this is a bijective linear map, there exist constants $c_j, c'_j > 0$ such that

$$c'_j \|\mathbf{y}\| \le \|\mathbf{y}_j\| = \|\mathcal{T}_j(\mathbf{y})\| \le c_j \|\mathbf{y}\| \qquad \text{for each } \mathbf{y} \in \mathbb{Q}^d \times \{0\}.$$

Then, for any $\mathbf{y} \in \mathbb{Q}^d \times \{0\}$ and any $j \in \{0, \dots, d-1\}$, we have

$$c'\|\mathbf{y}\| \le \|\mathbf{y}_j\| \le c\|\mathbf{y}\|$$

where $c = \max\{c_0, \dots, c_{d-1}\}$ and $c' = \min\{c'_0, \dots, c'_{d-1}\}$ depend only on α.

We can now construct the desired polynomial maps. They are the determinants given in the following proposition.

Proposition 3.5.1. *Let $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbb{Z}^{d+1}$ be linearly independent. Assume that the last coordinates x_d and y_d of $\mathbf{x}$ and $\mathbf{y}$ (respectively) are not both zero. Set*

$$E_0 = x_d\mathbf{y} - y_d\mathbf{x} \quad \textit{and} \quad E_i = \mathcal{T}_i(E_0) \quad \textit{for} \quad i = 1, \dots, d-1.$$

For each $j = 0, 1$, put

$$D_j = \begin{cases} \det(\mathbf{x}, \mathbf{y}, \mathbf{z}, E_{1+j}) & \textit{if} \quad d = 3, \\ \det(\mathbf{x}, \mathbf{y}, \mathbf{z}, E_1, \dots, E_{d-3}, E_{d-2+j}) & \textit{if} \quad d > 3. \end{cases}$$

Then, D_0 and D_1 are not both zero. Moreover, if

$$\|\mathbf{x}\| \le \|\mathbf{y}\| \le \|\mathbf{z}\| \quad \textit{and} \quad |\mathbf{x} \cdot \boldsymbol{\theta}| \ge |\mathbf{y} \cdot \boldsymbol{\theta}| \ge |\mathbf{z} \cdot \boldsymbol{\theta}|,$$

then we have

$$1 \le \|\mathbf{x}\|^{d-2} \|\mathbf{y}\|^{d-1} \|\mathbf{z}\| \, |\mathbf{x} \cdot \boldsymbol{\theta}|. \tag{3.13}$$

Proof. Set

$$V = \begin{cases} \langle \mathbf{x}, \mathbf{y}, \mathbf{z} \rangle_{\mathbb{Q}} & \text{if} \quad d = 3, \\ \langle \mathbf{x}, \mathbf{y}, \mathbf{z}, E_1, \ldots, E_{d-3} \rangle_{\mathbb{Q}} & \text{if} \quad d > 3. \end{cases}$$

Then $\dim_{\mathbb{Q}} V \leq d$. Assume on contrary that $D_0 = D_1 = 0$. This implies that E_{d-1} and E_{d-2} are contained in V. By definition, we have

$$E_0 \in \langle \mathbf{x}, \mathbf{y} \rangle_{\mathbb{Q}} \cap \left(\mathbb{Q}^d \times \{0\} \right) \subset V \cap \left(\mathbb{Q}^d \times \{0\} \right).$$

We conclude that

$$U := \langle E_0, \ldots E_{d-1} \rangle_{\mathbb{Q}} \subset V \cap \left(\mathbb{Q}^d \times \{0\} \right). \tag{3.14}$$

Since $\mathbf{x}, \mathbf{y}$ are linearly independent and x_d, y_d are not both zero, we get $E_0 \neq 0$. Note that $\boldsymbol{\theta} = (1, \alpha, \ldots, \alpha^{d-1}, \xi)$ has $\mathbb{Q}$-linearly independent coordinates. This implies that $E_0 \cdot \boldsymbol{\theta} \neq 0$, and moreover,

$$E_0 \cdot \boldsymbol{\theta},\ \alpha(E_0 \cdot \boldsymbol{\theta}), \ldots,\ \alpha^{d-1}(E_0 \cdot \boldsymbol{\theta})$$

are $\mathbb{Q}$-linearly independent. As $\alpha^i(E_0 \cdot \boldsymbol{\theta}) = E_i \cdot \boldsymbol{\theta}$ for each $i = 1, \ldots, d-1$, we deduce that $E_0, \ldots, E_{d-1}$ are also linearly independent. Hence, we get $\dim_{\mathbb{Q}} U = d \geq \dim_{\mathbb{Q}} V$. By (3.14), this implies that

$$U = V = \mathbb{Q}^d \times \{0\}.$$

Hence we get $\mathbf{x}, \mathbf{y} \in \mathbb{Q}^d \times \{0\}$, which is impossible as x_d and y_d are not both zero. This contradiction shows that D_0 and D_1 are not both 0.

Now assume that

$$\|\mathbf{x}\| \leq \|\mathbf{y}\| \leq \|\mathbf{z}\| \quad \text{and} \quad |\mathbf{x} \cdot \boldsymbol{\theta}| \geq |\mathbf{y} \cdot \boldsymbol{\theta}| \geq |\mathbf{z} \cdot \boldsymbol{\theta}|.$$

By definition, we have

$$D_j = \det \begin{pmatrix} \mathbf{x} \cdot \boldsymbol{\theta} & \mathbf{y} \cdot \boldsymbol{\theta} & \cdots & E_{d-2+j} \cdot \boldsymbol{\theta} \\ \mathbf{x}^+ & \mathbf{y}^+ & \cdots & E_{d-2+j}^+ \end{pmatrix} \qquad (j = 0, 1).$$

By the construction, we get

$$\|E_i\| = \|\mathcal{T}_i(E_0)\| \asymp \|E_0\| \ll \|\mathbf{x}\| \|\mathbf{y}\|$$

and

$$|E_i \cdot \boldsymbol{\theta}| = |\alpha^i (E_0 \cdot \boldsymbol{\theta})| \ll \|\mathbf{x}\| \, |\mathbf{y} \cdot \boldsymbol{\theta}| + \|\mathbf{y}\| \, |\mathbf{x} \cdot \boldsymbol{\theta}|$$
$$\ll \|\mathbf{y}\| \, |\mathbf{x} \cdot \boldsymbol{\theta}|$$

for all $i = 0, \ldots, d-1$. Combining the above estimates, we find that

$$|D_j| \ll \|\mathbf{x}\|\|\mathbf{y}\|\|\mathbf{z}\|(\|\mathbf{x}\|\|\mathbf{y}\|)^{d-3}(\|\mathbf{y}\||\mathbf{x} \cdot \boldsymbol{\theta}|) + |\mathbf{x} \cdot \boldsymbol{\theta}|\|\mathbf{y}\|\|\mathbf{z}\|(\|\mathbf{x}\|\|\mathbf{y}\|)^{d-2}$$
$$\ll \|\mathbf{x}\|^{d-2}\|\mathbf{y}\|^{d-1}\|\mathbf{z}\||\mathbf{x} \cdot \boldsymbol{\theta}|.$$

On the other hand, as α is an algebraic integer, we have $E_i \in \mathbb{Z}^{d+1}$for each $i = 1, \ldots, d-1$, and thus $D_0,\ D_1 \in \mathbb{Z}$. Since D_0 and D_1 are not both zero, we get

$$1 \le \max\{|D_0|, |D_1|\} \ll \|\mathbf{x}\|^{d-2}\|\mathbf{y}\|^{d-1}\|\mathbf{z}\||\mathbf{x} \cdot \boldsymbol{\theta}|. \qquad \square$$

As we discussed in Section 3.3, if $i < j$ are consecutive elements of I, then the points $\mathbf{x}_{i+1}, \mathbf{x}_{i+2}, \mathbf{x}_{j+2}$ are linearly independent. On the other hand, if the hypothesis of Lemma 3.2.3 are satisfied, then, for each sufficiently large index i, the last coordinate of $\mathbf{x}_i$ is not zero. Therefore, we deduce from the above proposition the following result.

Corollary 3.5.2. *Let $c > 0$ and $\tau > d-1$. Assume that the system*

$$\begin{cases} |x_0 + x_1\alpha + \cdots + x_{d-1}\alpha^{d-1} + x_d\xi| \le cX^{-\tau}, \\ |x_1|, \ldots, |x_d| \le X \end{cases}$$

admits a solution $\mathbf{x} = (x_0, \ldots, x_d) \in \mathbb{Z}^{d+1} \setminus \{0\}$ for any sufficiently large value of X. Then, for any consecutive indices $i < j$ of I, we have

$$1 \ll X_{i+1}^{d-2} X_{i+2}^{d-1} X_{j+2} T_{i+1}.$$

We now provide an alternative proof of Theorem 3.1.1 in the case where $d = 3$. The argument is the same as the one of the proof in Section 3.4. The difference is that we use the estimate given in Corollary 3.5.2 instead of Proposition 3.3.3 (i).

Alternative proof of Theorem 3.1.1 in the case where $d = 3$.

Let $(\mathbf{x}_i)_{i\in\mathbb{N}}, I, \rho$ be as in the proof of Theorem 3.1.1 in Section 3.4 for $d = 3$. Assume that $\tau > (3/2)d - 1 = 7/2$. We show that $\tau \leq \tau_3 = 2 + \sqrt{5}$. Fix a real number ε with $0 \leq \varepsilon < \rho$. As in the proof of Section 3.4, there exist infinitely many $i \in I$ satisfying (3.10). Fix such an index i and let j be the next element in I. Then, if i is sufficiently large, the inequality (3.11) holds for this pair (i, j). We now apply Corollary 3.5.2 (in place of Proposition 3.3.3 (i)) and get

$$\begin{aligned} 1 &\ll X_{i+1}\, X_{i+2}^2\, X_{j+2}\, T_{i+1} \\ &= X_{i+1}X_{i+2}\, X_{j+2}\, (X_{i+2}\, T_{i+1}) \\ &\ll X_{i+2}^{(1/(\rho-\varepsilon)+1)}\, X_{j+2}\, (X_{j+1}\, T_j) && \text{by (3.10) and Proposition 3.3.3 (ii)} \\ &\ll X_{i+2}^{(1/(\rho-\varepsilon)+1)}\, X_{j+1}^{(\rho+\varepsilon)+1-\tau} && \text{(using } T_j \leq X_{j+1}^{-\tau} \text{ and (3.11)).} \end{aligned}$$

We conclude that

$$X_{j+1}^{\tau-1-\rho-\varepsilon} \ll X_{i+2}^{1/(\rho+\varepsilon)+1}$$

holds for infinitely many $i \in I$ for each $0 < \varepsilon < \rho$. So we deduce that

$$\tau - 1 - \rho \leq \frac{1}{\rho} + 1.$$

This implies that

$$\tau \leq \frac{1}{\rho} + \rho + 2.$$

Since $1 \leq \rho \leq \frac{d-1}{\tau-d} = \frac{2}{\tau-3}$ and since the right hand side of the above estimate is an increasing function of ρ on $[1, \infty)$, we get

$$\tau \leq \frac{\tau-3}{2} + \frac{2}{\tau-3} + 2,$$

which implies $\tau \leq \tau_3 = 2 + \sqrt{5}$.

Bibliography

[1] A. Baker, *Transcendental number theory*, Cambridge University Press (1975).

[2] Y. Bugeaud and M. Laurent, *Exponents of Diophantine Approximation and Sturmian Continued Fractions* **55** (2005), 773-804.

[3] Y. Bugeaud and M. Laurent, *On exponents of homogeneous and inhomogeneous Diophantine approximation*, Mosc. Math. J. **5** (2005), no. 4, 747–766, 927.

[4] Y. Bugeaud, *Approximation by Algebraic numbers*, Cambridge Tracts in Math. 160, Cambridge Univ. Press, 2004.

[5] W. D. Brownawell and D. W. Masser, *Multiplicity estimates for analytic functions II*, Duke Math. J. **47** (1980), 273–295.

[6] H. Davenport and W. M. Schmidt, *Approximation to real numbers by algebraic integers*, Acta Arith. **15** (1968/1969), 393–416.

[7] H. Davenport and W. M. Schmidt, *Approximation to real numbers by quadratic irrationals*, Acta Arith. **13** (1967/1968), 169–176.

[8] G. Diaz, *Grand degrés de transcendance pour des familles d'exponentielles*, J. Number Theory **31** (1989), 1–23.

[9] A.O. Gel'fond, *On the algebraic independence of algebraic powers of algebraic numbers*, Doklady Akad. Nauk SSSR (N.S.) **64** (1949), 277–280.

[10] A.O. Gel'fond, *Transcendental and Algebraic Numbers*, Moscow, 1952; English translation: Dover Publ., 1960.

[11] V. Jarník, *Zum Khintchineschen Übertragungssatz*, Trudy Tbilisskogo mathematicheskogo instituta im. A. M. Razmadze = Travaux de l'Institut mathématique de Tbilissi **3** (1938), 193–212.

[12] S. Lang, *Introduction to Transcendental Numbers*, Addison -Wesley, 1966.

[13] M. Laurent, *Simultaneous rational approximation to the successive powers of a real number*, Indag. Math. (N.S.) **11** (2003), 45–53.

[14] M. Laurent and D. Roy, *Criteria of algebraic independence with multiplicities and approximation by hyper-surfaces*, J. reine angew. Math. **536** (2001), 65–114

[15] S. Lozier and D. Roy, *Simultaneous approximation to a real number and to its cube by rational numbers*, Acta Arith. **156** (2012), no. 1, 39–73.

[16] P. Philippon, *Critères pour l'indépendance algébrique,* Pub. Math. IHES, **64** (1986), 5–52.

[17] D. Roy, *An arithmetic criterion for the values of the exponential function*, Acta Arithmetica, XCVII.2 (2001), 183 -194.

[18] D. Roy, *Approximation to real numbers by cubic algebraic integers I*, Proc. London Math. Soc. (3) **88** (2004), 42–62.

[19] D. Roy, *On simultaneous rational approximations to a real number, its square, and its cube*, Acta Arith. **133** (2008), no. 2, 185–197.

[20] D. Roy, *Philippon's Criterion for Algebraic Independence*, Lectures 3 and 4, Fields' off-site summer school at the University of Ottawa, Analytic Number Theory and Diophantine Approximation, June 30 - July 11, 2008.

[21] D. Roy, *A small value estimate for* $\mathbb{G}_a \times \mathbb{G}_m$, Mathematika **59** (2013), 333–363.

[22] D. Roy, *Rational approximation to real points on conics*, Ann. Inst. Fourier (Grenoble), 13pp, to appear.

[23] B.L. van der Waerden, *Modern Algebra*, Frederick Ungar Publishing Co., New York, Vol II (1950).

[24] W. M. Schmidt, *Diophantine Approximations and Diophantine Equations*, Lecture notes in Math. 1467, Springer, 1991.