Multiplicities of Linear Recurrence Sequences

by

Patrick Brodie Allen

A thesis
presented to the University of Waterloo
in fulfilment of the
thesis requirement for the degree of
Master of Mathematics
in
Pure Mathematics

Waterloo, Ontario, Canada, 2006

Declaration

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.
I understand that my thesis may be made electronically available to the public.

Abstract

In this report we give an overview of some of the major results concerning the multiplicities of linear recurrence sequences. We first investigate binary recurrence sequences where we exhibit a result due to Beukers and a result due to Brindza, Pintér and Schmidt. We then investigate ternary recurrences and exhibit a result due to Beukers building on work of Beukers and Tijdeman. The last two chapters deal with a very important result due to Schmidt in which we bound the zero-multiplicity of a linear recurrence sequence of order t by a function involving t alone. Moreover we improve on Schmidt's bound by making some minor changes to his argument.

Acknowledgements

I would like to acknowledge my supervisor University Professor Cameron L. Stewart for giving me a thoroughly interesting thesis topic as well as for all his help in the preparation of this document. I would also like to acknowledge Professors Kevin Hare and Wentang Kuo for being part of my thesis committee.

Dedication

This thesis is dedicated to Deepa, my Mom, my Dad and my brothers.

Contents

List of Tables

Chapter 1

Introduction

1.1 Definitions and zero-multiplicity

A sequence of complex numbers $\{u_n\}_{n\in\mathbb{Z}}$ is called a *linear recurrence sequence* if there exists a positive integer t and $c_1, \ldots, c_t \in \mathbb{C}$, with $c_t \neq 0$, such that

$$u_n = c_1 u_{n-1} + \cdots + c_t u_{n-t} \tag{1.1}$$

for all $n \in \mathbb{Z}$. The recurrence sequence is said to be of *order* t if it satisfies (1.1) but no such relation with fewer than t summands. We say that the zero sequence, i.e. $u_n = 0$ for all $n \in \mathbb{Z}$, has order 0 and it is the only recurrence sequence with order 0. We claim that if a recurrence sequence $\{u_n\}_{n\in\mathbb{Z}}$ is of order $t > 0$ then its recurrence relation (1.1) is unique. Indeed suppose $\{u_n\}_{n\in\mathbb{Z}}$ satisfies (1.1) as well as

$$u_n = d_1 u_{n-1} + \cdots + d_t u_{n-t}$$

for some $d_1, \ldots, d_t \in \mathbb{C}$ with $d_t \neq 0$ and some $c_i \neq d_i$, $1 \leq i \leq t$. Let $r = \min\{i : c_i \neq d_i\}$. If $r = t$ then we have $c_t u_{n-t} = d_t u_{n-t}$ for all $n \in \mathbb{Z}$, hence $u_{n-t} = 0$ for all $n \in \mathbb{Z}$ which is a contradiction since we assumed $t > 0$. Assume $r < t$, then we have

$$u_{n-r} = \frac{c_{n-r-1} - d_{n-r-1}}{d_{n-r} - c_{n-r}} u_{n-r-1} + \cdots + \frac{c_{n-t} - d_{n-t}}{d_{n-r} - c_{n-r}} u_{n-t}$$

for all $n \in \mathbb{Z}$. This is a relation with fewer than t summands, which is contradiction.

A recurrence is called *algebraic* if the sequence as well as the recurrence coefficients $c_1, \ldots, c_t$ in (1.1) are algebraic. *Rational* and *integral* recurrences are defined similarly. Note that a sequence of algebraic, rational or integral numbers may satisfy a recurrence relation

that is not algebraic, rational or integral, respectively. For example the sequence $\{1\}_{n\in\mathbb{Z}}$ satisfies the recurrence relation $u_n = \pi u_{n-1} + (1-\pi)u_{n-2}$. Note however that this is not the minimal recurrence relation for this sequence. It can be shown that if a recurrence sequence belongs to a field K then its minimal recurrence relation has coefficients belonging to K. Let $\{u_n\}_{n\in\mathbb{Z}} \subseteq K$ be a recurrence sequence with minimal recurrence relation

$$u_n = c_1 u_{n-1} + \cdots + c_t u_{n-t}$$

for all $n \in \mathbb{Z}$, where $c_1, \ldots, c_t$ belong to some field which contains K. Consider the system of t linear equations in t variables $x_1, \ldots, x_t$,

$$\begin{aligned} u_t &= x_1 u_{t-1} + \cdots + x_t u_0 \\ &\vdots \\ u_{2t-1} &= x_1 u_{2t-2} + \cdots + x_t u_{t-1}. \end{aligned} \tag{1.2}$$

It is not hard to show, by induction, that any solution, $x_1, \ldots, x_t$, to (1.2) will satisfy

$$u_n = x_1 u_{n-1} + \cdots + x_t u_{n-t}$$

for all $n \in \mathbb{Z}$. Since our sequence is of order t there is a unique solution to this system of equations and thus the determinant of the coefficient matrix of (1.2) cannot vanish. We can then apply Cramer's rule and express the x_i in terms of $u_0, \ldots, u_{2t-1}$.

For a recurrence sequence satisfying (1.1) its *companion polynomial* is defined as

$$\mathcal{P}(z) = z^t - c_1 z^{t-1} - \cdots - c_t. \tag{1.3}$$

Say (1.3) has distinct roots $\alpha_1, \ldots, \alpha_k$, each with multiplicity t_i, $1 \le i \le k$, i.e.

$$\mathcal{P}(z) = \prod_{i=1}^{k} (z - \alpha_i)^{t_i}. \tag{1.4}$$

We call these α_i the *roots* of the recurrence. Note that they are all nonzero since $c_t \neq 0$. If each α_i is a simple root we say that the recurrence is *simple*. The following result is fundamental to the theory of linear recurrences.

Theorem 1.1. *Let $\{u_n\}_{n\in\mathbb{Z}}$ be a recurrence relation satisfying* (1.1) *with companion polynomial that factors as* (1.4)*. Then, for $1 \le i \le k$, there exists polynomials $P_i(x) \in \mathbb{C}[x]$ with $\deg P_i < t_i$, such that for all $n \in \mathbb{Z}$,*

$$u_n = P_1(n)\alpha_1^n + \cdots + P_k(n)\alpha_k^n. \tag{1.5}$$

Moreover if $\{u_n\}_{n\in\mathbb{Z}}$ *is of order* t *than* $\deg P_i = t_i - 1$ *for each* $1 \le i \le k$.

Conversely, suppose $\alpha_1, \ldots, \alpha_k$ *are distinct nonzero complex numbers and* $P_1(x), \ldots, P_k(x)$ *are nonzero polynomials in* $\mathbb{C}[x]$. *For* $1 \le i \le k$, *let* t_i *be an integer strictly greater than* $\deg P_i$, $t = t_1 + \cdots + t_k$ *and define* $c_1, \ldots, c_t$ *by* (1.4) *and* (1.3). *Then the sequence* $\{u_n\}_{n\in\mathbb{Z}}$ *defined by* (1.5) *satisfies the recurrence relation* (1.1). *Moreover if* $t_i = \deg P_i + 1$ *then* $\{u_n\}_{n\in\mathbb{Z}}$ *is of order* t.

Proof. Consider the vector space, V, consisting of all sequences $\{u_n\}_{n\in\mathbb{Z}}$ with $u_n \in \mathbb{C}$ for all $n \in \mathbb{Z}$. Let $\mathcal{P}(z) \in \mathbb{C}[z]$ be the polynomial given by (1.3) and (1.4). Let $\mathcal{P}$ act on V by

$$\mathcal{P}(\{u_n\}_{n\in\mathbb{Z}}) = \{v_n\}_{n\in\mathbb{Z}}$$

where, for each $n \in \mathbb{Z}$,

$$v_n = u_n - c_1 u_{n-1} - \cdots - c_t u_{n-t}.$$

Let W be the kernel of this map. This is the subspace of V consisting of all sequences satisfying (1.1). Clearly $\dim W = t$ and we claim that W is spanned by the sequences

$$\{n^j \alpha_i^n\}_{n\in\mathbb{Z}} \tag{1.6}$$

for $1 \le i \le k$ and $0 \le j \le t_i - 1$. We have t vectors and they are clearly linearly independent, hence it remains to show that each does belong to W, i.e. that

$$n^j \alpha_i^n - c_1 (n-1)^j \alpha_i^{n-1} - \cdots - c_t (n-t)^j \alpha_i^{n-t} = 0 \tag{1.7}$$

for each $1 \le i \le k$, $0 \le j \le t_i - 1$ and all $n \in \mathbb{Z}$. The left hand side of (1.7) is equal to

$$\underbrace{z\frac{\mathrm{d}}{\mathrm{d}z}\left(\cdots\left(z\frac{\mathrm{d}}{\mathrm{d}z}\right.\right.}_{j \text{ times}} z^{n-t}\mathcal{P}(z)\left.\left.\right)\cdots\right)\Big|_{z=\alpha_i}, \tag{1.8}$$

which is to be interpreted as $\alpha_i^{n-t}\mathcal{P}(\alpha_i)$ if $j = 0$. Since, for each $1 \le i \le k$, α_i has multiplicity t_i and $j < t_i$ we see that (1.8) vanishes, establishing (1.7). Since the sequences (1.6) are a basis for W we see that every recurrence sequence satisfying (1.1) is given by (1.5). If $\{u_n\}_{n\in\mathbb{Z}}$ is given by (1.5) such that some P_i has $\deg P_i < t_i - 1$, we say $\deg 0 = -1$, then we see that $\mathcal{P}_0(\{u_n\}_{n\in\mathbb{Z}}) = \{0\}$, where $\mathcal{P}_0(z) = \mathcal{P}(z)(z - \alpha_i)^{-1}$. Hence if our sequence is of order t then we must have $\deg P_i = t_i - 1$ for each $1 \le i \le k$.

The converse is also established, since any sequence satisfying (1.5) will be in the subspace W of V consisting of all sequences that vanish under $\mathcal{P}$. Thus it must satisfy a recurrence relation with companion polynomial (1.3), i.e. the recurrence relation (1.1). □

Note that the proof of Theorem 1.1 establishes another subtle fact, i.e. if a recurrence sequence satisfies (1.1) with companion polynomial $\mathcal{P}$ then the companion polynomial of its minimal recurrence relation divides $\mathcal{P}$.

For a recurrence sequence $\{u_n\}_{n\in\mathbb{Z}} \subseteq \mathbb{C}$ and $\omega \in \mathbb{C}$, the *ω-multiplicity* of the recurrence is the number of $n \in \mathbb{Z}$ such that $u_n = \omega$.

Theorem 1.2. (Skolem-Mahler-Lech) *Let $\{u_n\}_{n\in\mathbb{Z}} \subseteq \mathbb{C}$ be a recurrence sequence and let $\mathcal{Z}$ denote the set of $n \in \mathbb{Z}$ such that $u_n = 0$. Then $\mathcal{Z}$ is the union of finitely many single numbers and arithmetic progressions.*

Where, by *arithmetic progression*, we mean a set

$$\mathcal{A} = \{ax + b : x \in \mathbb{Z}\}$$

for fixed $a, b \in \mathbb{Z}$ with $a > 0$. We call a, sometimes denoted $a(\mathcal{A})$, the *modulus* of $\mathcal{A}$.

Proof. See [13]. □

Corollary 1.3. *Let $\{u_n\}_{n\in\mathbb{Z}}$ be a linear recurrence sequence of order t whose companion polynomial has the distinct roots $\alpha_1, \ldots, \alpha_k$. If there is some $1 \leq i_0 \leq k$ such that α_{i_0}/α_j is not a root of unity for any $j \neq i_0$ then the zero multiplicity of $\{u_n\}_{n\in\mathbb{Z}}$ is finite.*

Proof. By Theorem 1.1 we know that there exists polynomials $P_1, \ldots, P_k \in \mathbb{C}[z]$ with $\deg P_i = t_i - 1$, where t_i is the multiplicity of α_i in the companion polynomial to $\{u_n\}_{n\in\mathbb{Z}}$, such that

$$u_n = P_1(n)\alpha_1^n + \cdots + P_k(n)\alpha_k^n.$$

We group together summands $P_i(n)\alpha_i^n$ and $P_j(n)\alpha_j^n$ with α_i/α_j a root of unity. We now write, uniquely up to ordering,

$$u_n = f_1(n) + \cdots + f_s(n)$$

where, for $1 \leq i \leq s$,

$$f_i(n) = P_{i1}\alpha_{i1}^n + \cdots + P_{ik_i}\alpha_{ik_i}^n,$$

with $k_1 + \cdots + k_s = k$ and, for $1 \leq j \leq k_i$ and $1 \leq l \leq k_{i'}$, $\alpha_{ij}/\alpha_{i'l}$ is a root of unity if and only if $i = i'$.

Say $u_n = 0$ for every n in the arithmetic progression $\mathcal{A} = \{ax + b : x \in \mathbb{Z}\}$ with fixed $a, b \in \mathbb{Z}$, $a > 0$. Take positive integer m so that $(\alpha_{i,j}/\alpha_{i,l})^m = 1$ for every $1 \leq i \leq s$ and $1 \leq j, l \leq k_i$. The progression $\mathcal{A}$ is a finite union of arithmetic progressions of the form

$\mathcal{A}' = \{amx + b' : x \in \mathbb{Z}\}$. Take some such progression $\mathcal{A}'$. When $n = amx + b' \in \mathcal{A}'$, we have $\alpha_{ij}^n = \alpha_{ij}^{b'}\alpha_{i1}^{amx}$, hence

$$f_i(n) = Q_i(x)\alpha_{i1}^{amx},$$

for $1 \leq i \leq s$ with $Q_i(x) = \sum_{j=1}^{k_i} \alpha_{ij}^{b'} P_{ij}(amx + b')$. Thus

$$Q_1(x)\alpha_{11}^{amx} + \cdots + Q_s(x)\alpha_{s1}^{amx} = 0 \tag{1.9}$$

for all $x \in \mathbb{Z}$. Since $\alpha_{i1}/\alpha_{i'1}$ is not a root of unity for $i \neq i'$, clearly $\alpha_{i1}^{amx}/\alpha_{i'1}^{amx}$ is not a root of unity for $i \neq i'$. But then $\{x^l\alpha_{i1}^{amx}\}_{x\in\mathbb{Z}}$, for $1 \leq i \leq s$ and $l \geq 0$, are linearly independent recurrence sequences. Thus (1.9) can vanish for every $x \in \mathbb{Z}$ only if $Q_1 = \cdots = Q_s = 0$. So for every $n \in \mathcal{A}'$ we have

$$f_1(n) = \cdots = f_s(n) = 0. \tag{1.10}$$

This will hold for any one of these progressions $\mathcal{A}'$ above, hence (1.10) holds for every $n \in \mathcal{A}$.

Let $\mathcal{Z} = \{n \in \mathbb{Z} : u_n = 0\}$. If there is some α_{i_0} satisfying the conditions of the corollary then $f_{i_0}(n) = P_{i_0}(n)\alpha_{i_0}^n$ and can have at most t_i zeros. Hence, by (1.10), $\mathcal{Z}$ cannot contain any arithmetic progressions. Theorem 1.2 then implies that $|\mathcal{Z}|$ is finite. □

We call a recurrence sequence with companion polynomial (1.4) *non-degenerate* if $i \neq j$ implies α_i/α_j is not a root of unity. By Corollary 1.3 we see that non-degenerate sequences have finite zero-multiplicity. Moreover Corollary 1.3 also implies that if $\{u_n\}_{n\in\mathbb{Z}}$ is a nondegenerate recurrence and $\omega \in \mathbb{C}$ then the ω-multiplicity is finite. If $k = 1$ the result is clear so we may assume $k \geq 1$. Say $\{u_n\}_{n\in\mathbb{Z}}$ is given by (1.5). The ω-multiplicity of $\{u_n\}_{n\in\mathbb{Z}}$ is the zero multiplicity of the recurrence given by

$$P_1(n)\alpha_1^n + \cdots + P_k(n)\alpha_k^n - \omega 1^n. \tag{1.11}$$

Since $\{u_n\}_{n\in\mathbb{Z}}$ is non-degenerate there exists $1 \leq i_0 \leq k$ such that α_{i_0} is not a root of unity. Then, setting $\alpha_{k+1} = 1$, we have that α_{i_0}/α_j is not a root of unity for any $1 \leq j \leq k+1$ with $i \neq j$. Thus the 0-multiplicity of (1.11) and hence the ω-multiplicity of $\{u_n\}_{n\in\mathbb{Z}}$ is finite.

1.2 Valuations and height functions

Let K be a field and say $|\ |_1$ and $|\ |_2$ are absolute values on K. We say that $|\ |_1$ and $|\ |_2$ are *equivalent* if they generate the same topology on K. It can be shown that two absolute values are equivalent if and only if there exists $\lambda \in \mathbb{R}$ with $\lambda > 0$ such that for all $x \in K$

$$|x|_1^\lambda = |x|_2 . \tag{1.12}$$

Note however that if $|\ |$ is an absolute value and $\lambda \in \mathbb{R}$, $\lambda > 0$, then $|\ |^\lambda$ need not be an absolute value on K as it may violate the triangle inequality. For example if $|\ |$ is the usual absolute value on $\mathbb{C}$ and $\lambda = 2$ then we may not have $|x+y|^2 \leq |x|^2 + |y|^2$. If $|\ |$ is a multiplicative function from K to the non-negative reals such that $|x| = 0$ implies $x = 0$ we call it a *valuation* if it is equivalent to some absolute value on K via the relation (1.12). We denote by M_K the set of equivalence classes of valuations on K, which are called *places*.

Say K is a number field and $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K. Let $\mathfrak{a}$ be an ideal in $\mathcal{O}_K$. Then there are unique prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ and positive integers $e_1, \ldots, e_n$ such that

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}. \tag{1.13}$$

For any $1 \leq i \leq n$ we say that $\mathfrak{p}_i$ *divides* $\mathfrak{a}$ and write $\mathfrak{p}_i | \mathfrak{a}$. In particular if L is a subfield of K with ring of integers $\mathcal{O}_L$ and $\mathfrak{a}$ is a prime ideal of $\mathcal{O}_L$ then $\mathfrak{a}$ has a decomposition (1.13) in terms of primes ideals of $\mathcal{O}_K$. In this case e_i is called the *ramification index* of $\mathfrak{p}_i$ over $\mathfrak{a}$ and we say that $\mathfrak{p}_i$ *ramifies* to order e_i over $\mathfrak{a}$, $1 \leq i \leq n$. If for each $1 \leq i \leq n$ we set

$$f_i = [\mathcal{O}_K/\mathfrak{p}_i : \mathcal{O}_L/\mathfrak{a}],$$

then we have

$$[K : L] = \sum_{i=1}^{n} e_i f_i.$$

The number f_i is called the *residue degree* of $\mathfrak{p}_i$ over $\mathfrak{a}$. Moreover if K/L is Galois with Galois group G then G acts transitively on the set $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ and we have that $e_1 = \cdots = e_n$ and $f_1 = \cdots = f_n$. In particular, letting these common values be denoted by e and f respectively, we have

$$ef | [K : L].$$

For nonzero $x \in \mathcal{O}_K$ and $\mathfrak{p}$ a prime ideal in $\mathcal{O}_K$, we define $\mathrm{ord}_{\mathfrak{p}}(x)$ to be the unique nonnegative integer n such that

$$x \in \mathfrak{p}^n,\ x \notin \mathfrak{p}^{n+1}.$$

We then extend this to all of $K^\times$ by

$$\mathrm{ord}_{\mathfrak{p}}\left(\frac{x}{y}\right) = \mathrm{ord}_{\mathfrak{p}}(x) - \mathrm{ord}_{\mathfrak{p}}(y)$$

for any non-zero $x, y \in \mathcal{O}_K$. For any $0 < c < 1$ we define an absolute value on K by

$$|x|_{\mathfrak{p}} = \begin{cases} c^{\mathrm{ord}_{\mathfrak{p}}(x)} & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases}. \tag{1.14}$$

Note that different choices of $0 < c < 1$ will generate equivalent absolute values by (1.12). However if $\mathfrak{p} \neq \mathfrak{p}'$ then $|\ |_{\mathfrak{p}}$ is not equivalent to $|\ |_{\mathfrak{p}'}$.

Let $|\ |$ denote the usual absolute value on $\mathbb{C}$. If K is a number field and $\sigma : K \hookrightarrow \mathbb{C}$ is an embedding of K into $\mathbb{C}$ then we define an absolute value on K by

$$|x|_{\sigma} = |\sigma(x)| \tag{1.15}$$

for all $x \in K$. Note that conjugate embeddings will yield equivalent absolute values since $|x| = |\overline{x}|$. However if σ_1 and σ_2 are distinct embeddings and are not conjugate then $|\ |_{\sigma_1}$ will not be equivalent to $|\ |_{\sigma_2}$. It can be shown that every valuation on K is equivalent to one of the form (1.14) or (1.15).

For $v \in M_K$ we say that v is *finite* if it is the set of valuations equivalent to (1.14) for some prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ and we say that p *lies above* v, where p is the rational prime such that $\mathfrak{p}|(p)$. Moreover if the ramification index of $\mathfrak{p}$ over (p) is e we say that v has *ramification index* e. If v is not finite then we say that v is *infinite*. If $v \in M_K$ is an infinite place that contains a valuation arising from a real embedding it is called *real* and if it contains a valuation arising from a pair of conjugate complex embeddings it is called *complex*.

Let $v \in M_K$ be a finite place such that $|\ |_{\mathfrak{p}} \in v$ for a prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$ and p the rational prime above v. We define the valuation $|\ |_v$ by (1.14) where the constant c is chosen such that

$$|p|_v = p^{-d_{\mathfrak{p}}/d},$$

where $d = [K : \mathbb{Q}]$ and $d_{\mathfrak{p}} = [K_{\mathfrak{p}} : \mathbb{Q}_{\mathfrak{p}}]$, and where $K_{\mathfrak{p}}$ and $\mathbb{Q}_{\mathfrak{p}}$ are the completions of K and $\mathbb{Q}$, respectively, with respect to the topology generated by $|\ |_{\mathfrak{p}}$. It can be shown that $d_v = ef$, where e and f are the ramification index and the residue degree of $\mathfrak{p}$ over (p), respectively. Note that $K_{\mathfrak{p}}$ and $\mathbb{Q}_{\mathfrak{p}}$ do not depend on the choice of constant $0 < c < 1$ in (1.14) since equivalent absolute values will generate equivalent topologies. If $v \in M_K$ is an infinite place containing the valuation $|\ |_{\sigma}$ as in (1.15), for an embedding σ of K in $\mathbb{C}$, then we define the valuation $|\ |_v$ by

$$|x|_v = \begin{cases} |x|_{\sigma}^{1/d} & \text{if } v \text{ is real} \\ |x|_{\sigma}^{2/d} & \text{if } v \text{ is complex} \end{cases}$$

for $x \in K$, where $d = [K : \mathbb{Q}]$. With these choices for valuations we have the *product formula*

$$\prod_{v \in M_K} |x|_v = 1,$$

for any $x \in K^{\times}$.

It must be noted however that these normalisations may not yield absolute values, they are merely valuations. However if we define $r(v)$ by

$$r(v) = \begin{cases} 1 & \text{if } v \text{ is finite} \\ 2^{1/d} & \text{if } v \text{ is real} \\ 2^{2/d} & \text{if } v \text{ is complex} \end{cases}.$$

Then we have

$$|x+y|_v \leq r(v) \max\{|x|_v, |y|_v\},$$

for all $x, y \in K$. Note also that $\prod_{v \in M_K} r(v) = 2$. Let α be a non-zero algebraic number and K any field that contains α. It can be shown that the number

$$H(\alpha) = \prod_{v \in M_K} \max\{1, |\alpha|_v\} \tag{1.16}$$

is independent of the choice of K containing α. We call $H(\alpha)$ the *absolute height* of α. The absolute height satisfies the following useful identities

$$\begin{aligned} H(\alpha\beta) &\leq H(\alpha)H(\beta), \\ H(\alpha+\beta) &\leq 2H(\alpha)H(\beta), \\ H(1/\alpha) &= H(\alpha), \\ H(\alpha^n) &= H(\alpha)^n \text{ for any integer } n \geq 0, \\ H(\alpha) = 1 &\Leftrightarrow \alpha \text{ is a root of unity.} \end{aligned}$$

The *absolute logarithmic height*, denoted by $h(\alpha)$, is given by

$$h(\alpha) = \log H(\alpha) = \sum_{v \in M_K} \max\{0, \log |\alpha|_v\}.$$

The absolute height and the absolute logarithmic height will be vital in the proofs of many of the theorems in this report. With the exception of §2.2 anytime we refer to height we will mean either the absolute height or the absolute logarithmic height, depending on the context.

1.3 Main results

For a linear recurrence sequence $\{u_n\}_{n \in \mathbb{Z}} \subseteq \mathbb{C}$ and $\omega \in \mathbb{C}$ we let $u(\omega)$ denote the ω-multiplicity of the recurrence. The purpose of this report is to exhibit some important results on such multiplicities of linear recurrence sequences.

In Chapter 2 we will investigate linear recurrences of order two, which are called *binary* recurrence sequences. We first show a result due to Beukers, that for any non-degenerate rational binary recurrence with integral recurrence relation and $\omega \in \mathbb{Q}$ we have $u(\omega) + u(-\omega) \leq 3$ with finitely many exceptions that are explicitly given. In the second part of Chapter 2 we will establish criteria, due to Brindza, Pinter and Schmidt, for recurrences of algebraic integers so that $u(\omega) = 1$ for non-zero ω.

In Chapter 3 we will investigate *ternary* recurrences, i.e. recurrences of order three. The main result of this chapter is due to Beukers, building on work of Beukers and Tidjeman. It shows that a non-degenerate rational ternary recurrence has zero-multiplicity at most six, which is best possible.

Chapter 4 does not directly concern linear recurrence sequences. Chapter 4 contains arguments due to Schmidt on the denominators of rational numbers, which is necessary for the result in Chapter 5.

Chapter 5 will prove the following result due to Schmidt: for any linear recurrence sequence, $\{u_n\}_{n\in\mathbb{Z}}$, of order t, if $\mathcal{Z}$ is the set of subscripts such that $u_n = 0$ for any $n \in \mathcal{Z}$, then $\mathcal{Z}$ is the union of at most $c(t)$ numbers and arithmetic progressions, where $c(t)$ is a function depending on t alone. The importance of this result lies in the dependence of the bound on t alone. No previous result had been able to avoid dependence on the degree of the number field in which the sequence belongs or the height of the numbers involved.

Chapter 2

Binary Recurrence Sequences

2.1 Rational binary recurrence sequences

In this section we will be investigating non-degenerate rational linear recurrences of order two. Let $\{u_n\}_{n\in\mathbb{Z}}$ be a non-degenerate linear recurrence satisfying

$$u_n = c_1 u_{n-1} + c_2 u_{n-2}, \tag{2.1}$$

for all $n \in \mathbb{Z}$, with $c_1, c_2 \in \mathbb{Z}$. For $\omega \in \mathbb{Q}$, let $u(\omega)$ denote the number of $n \in \mathbb{Z}$ such that $u_n = \omega$. By the results of §1.1 we know that for any $\omega \in \mathbb{Q}$, $u(\omega)$ is finite. For $\omega \in \mathbb{Q}$, if $u(\omega) > 0$ then let $n_0 = \min\{n \in \mathbb{Z} : u_n = \pm\omega\}$. The sequence given by $u'_n = u_{n-n_0}$ satisfies

$$u'_n = \omega \;\Rightarrow\; n \geq 0.$$

Hence we may consider sequences indexed by non-negative integers opposed to all of $\mathbb{Z}$. Moreover we may assume that $u_0 = \pm\omega$ so in order to bound $u(\omega) + u(-\omega)$ it suffices to bound the size of the set $\{n \geq 0 : u_n = \pm u_0\}$. If $s \in \mathbb{Z}$ is the least common denominator of u_0 and u_1, then $\{su_n\}_{n\geq 0} \subseteq \mathbb{Z}$ and the ω-multiplicity of $\{u_n\}_{n\geq 0}$ is equal to the $s\omega$-multiplicity of $\{su_n\}_{n\geq 0}$. Thus we may further assume that our recurrence is integral. Also note that $\gcd(u_0, u_1)|u_n$ for all $n \geq 0$ so we may assume $\gcd(u_0, u_1) = 1$ and that $u_0 \geq 0$ by multiplying the entire sequence by -1 if necessary. Lastly we may assume $c_1 \geq 0$ since the sequence given by $u'_n = (-1)^n u_n$, for each $n \geq 0$, satisfies the recurrence $u'_n = (-c_1)u_{n-1} + c_2 u_{n-2}$ for each $n \geq 2$ and $\{n \geq 0 : u_n = \pm u_0\} = \{n \geq 0 : u'_n = \pm u'_0\}$.

In the late 1930s, Ward conjectured that $u(\omega) \leq 5$ for all $\omega \in \mathbb{Q}$. This conjecture was proved by Kubota [10]. Later in [11] he improved the result by showing that in fact $u(\omega) \leq 4$. In [2], Beukers showed that if the companion polynomial is irreducible over $\mathbb{Q}$ then $u(\omega) + u(-\omega) \leq 3$ except in finitely many cases which he gave explicitly. Moreover

this bound is achieved infinitely often. If $c_1 = 1$, c_2 is arbitrary, $u_0 = 1$ and $u_1 = -1$ then $u_3 = -1$. In this section we show that this result holds for all nondegenerate binary recurrence sequences with integral recurrence relation. It can be shown, see for instance [20] pg. 36-37, that this includes all recurrence sequences $\{u_n\}_{n\in\mathbb{Z}}$ with $\{u_n\}_{n\in\mathbb{Z}} \subset \mathbb{Z}$. We essentially reproduce the argument in [2] but add a few extra details in order to deal with the case when the companion polynomial has rational roots. This result is divided into two theorems, Theorem 2.1 treats the case $c_1^2 + 4c_2 < 0$ and Theorem 2.2 the case $c_1^2 + 4c_2 \geq 0$.

We begin with a simple Lemma, akin to Theorem 1.1.

Lemma 2.1. *Let $\{u_n\}_{n\geq 0} \subseteq \mathbb{Z}$ be a nondegenerate linear recurrence sequence satisfying recurrence relation (2.1) with $c_1, c_2 \in \mathbb{Z}$. Say α_1 and α_2 are the roots of $z^2 - c_1 z - c_2$ and set $\lambda_1 = u_1 - u_0\alpha_2$, $\lambda_2 = u_1 - u_0\alpha_1$. Then, for all $n \geq 0$,*

$$u_n = \frac{\lambda_1\alpha_1^n - \lambda_2\alpha_2^n}{\alpha_1 - \alpha_2}.$$

Proof. This is an easy exercise in induction. □

We wish to bound the size of the set $\{n \geq 0 : u_n = \pm u_0\}$, which by Lemma 2.1 is given by

$$\left\{ n \geq 0 : \frac{\lambda_1\alpha_1^n - \lambda_2\alpha_2^n}{\alpha_1 - \alpha_2} = \pm\frac{\lambda_1 - \lambda_2}{\alpha_1 - \alpha_2} \right\}.$$

Thus it suffices to bound the size of the set

$$\{n \geq 0 : \lambda_1\alpha_1^n - \lambda_2\alpha_2^n = \pm(\lambda_1 - \lambda_2)\} \tag{2.2}$$

Also, we may assume that the algebraic integers λ_1 and λ_2 do not have any common rational integer factors in the ring of integers of $\mathbb{Q}(\alpha_1, \alpha_2)$. If $u_0 = 0$ then $\lambda_1 = \lambda_2$ and (2.2) reduces to

$$\alpha_1^n - \alpha_2^n = 0,$$

which has no solutions $n \neq 0$ since α_1/α_2 is not a root of unity. Hence we will assume throughout that $u_0 \neq 0$.

In the following Lemmas we will assume that the companion polynomial to our recurrence has negative discriminant, i.e. that $c_1^2 + 4c_2 < 0$. This implies that α_1 and λ_1 are algebraic integers in an imaginary quadratic field and that $\alpha_2 = \overline{\alpha}_1$ and $\lambda_2 = \overline{\lambda}_1$. In this case we write α and λ instead of α_1 and λ_1.

Lemma 2.2. *Let λ and α be algebraic integers in an imaginary quadratic number field K with ring of integers $\mathcal{O}_K$. Suppose λ and $\overline{\lambda}$ have no common rational integer factor in $\mathcal{O}_K$. If $\lambda\alpha^n - \overline{\lambda}\overline{\alpha}^n = \delta(\lambda - \overline{\lambda})$, for some $\delta \in \{-1, 1\}$ and positive rational integer n, then there is a rational integer a such that $\alpha^n = \delta + a\overline{\lambda}$.*

Proof. Since $\lambda(\alpha^n - \delta) = \overline{\lambda}(\overline{\alpha}^n - \delta)$ we see that $\lambda(\alpha^n - \delta)$, which we will denote by d, is a rational integer. Now $d\overline{\lambda} = \lambda\overline{\lambda}(\alpha^n - \delta)$, so if $\lambda\overline{\lambda} \nmid d$ we must have a prime factor p of $\lambda\overline{\lambda}$ which divides $\overline{\lambda}$ in $\mathcal{O}_K$. But then we must have $p|\lambda$, which is a contradiction as λ and $\overline{\lambda}$ have no rational integer factors in common. Thus $\lambda\overline{\lambda}|d$ and there exists $a \in \mathbb{Z}$ such that $\alpha^n - \delta = a\overline{\lambda}$. □

By replacing (2.2) by its complex conjugate, if necessary, and replacing α with $-\alpha$ and λ with $-\lambda$, we may assume that $0 \leq \arg\alpha \leq \pi/2$ and $0 \leq \arg\lambda \leq \pi$. Since α is the root of an irreducible polynomial and $\alpha/\overline{\alpha}$ is not a root of unity we have $0 < \arg\alpha < \pi/2$. Moreover we can assume $0 < \arg\lambda < \pi$ since $u_0 \neq 0$.

Lemma 2.3. *Let K be an imaginary quadratic field with ring of integers $\mathcal{O}_K$. Let $\gamma, \eta \in \mathcal{O}_K$ and let $t \in \mathbb{Z}$, $t \neq 0$. Consider the equation*

$$\gamma(1 + t\eta)^n - \overline{\gamma}(1 + t\overline{\eta})^n = \gamma - \overline{\gamma} \tag{2.3}$$

in the positive integer n.

1. *Suppose that $\gamma\eta - \overline{\gamma\eta} \neq 0$ and let $\beta \in \mathcal{O}_K$, $\beta \neq 0$, divide $\gamma\eta^l - \overline{\gamma\eta}^l$ for all $l > 0$. There are no solutions $n > 0$ if one of the following conditions is satisfied:*
   (a) $t \equiv 0 \pmod 2$ *and* $\frac{t}{2} \nmid \frac{\gamma\eta - \overline{\gamma\eta}}{\beta}$,
   (b) $t \not\equiv 0 \pmod 2$ *and* $t \nmid \frac{\gamma\eta - \overline{\gamma\eta}}{\beta}$.
2. *Suppose that $\gamma\eta - \overline{\gamma\eta} = 0$ and $\gamma\eta \neq 0$. Let $\beta \in \mathcal{O}_K$, $\beta \neq 0$, divide $\eta - \overline{\eta}$. Then $n = 1$ is the only solution in if any of the following conditions are satisfied:*
   (a) $t \equiv 0 \pmod 3$ *and* $\frac{t}{3} \nmid \frac{\eta - \overline{\eta}}{\beta}$,
   (b) $t \equiv 0 \pmod 3$, $t \nmid \frac{\eta - \overline{\eta}}{\beta}$ *and* $\frac{\eta^2 - \overline{\eta}^2}{\beta} \equiv 0 \pmod 3$,
   (c) $t \not\equiv 0 \pmod 3$ *and* $t \nmid \frac{\eta - \overline{\eta}}{\beta}$.

Proof. Assume that equation (2.3) has a solution $n > 0$. It can be rewritten as

$$\gamma - \overline{\gamma} + \sum_{j=1}^{n} \binom{n}{j} t^j (\gamma\eta^j - \overline{\gamma\eta}^j) = \gamma - \overline{\gamma},$$

which yields

$$\sum_{j=1}^{n} \binom{n}{j} t^j (\gamma\eta^j - \overline{\gamma\eta}^j) = 0. \tag{2.4}$$

In both part 1 and part 2 of the Lemma we have $\beta \neq 0$ hence we can multiply (2.4) by β^{-1}. Similarly, since $n > 0$ and $t \neq 0$ we can multiply (2.4) by n^{-1} and t^{-1}. Then, noting that $\binom{n}{j} = \frac{n}{j}\binom{n-1}{j-1}$, we obtain

$$\sum_{j=1}^{n} \frac{t^{j-1}}{j}\binom{n-1}{j-1}\frac{\gamma\eta^j - \overline{\gamma\eta}^j}{\beta} = 0. \tag{2.5}$$

Assume we are in the situation of part 1 of the Lemma, in particular that $\gamma\eta - \overline{\gamma\eta} \neq 0$. Suppose $t \equiv 0 \pmod 2$ and $t/2 \nmid (\gamma\eta - \overline{\gamma\eta})/\beta$. If $j = 2$ then $t^{j-1}/j \equiv 0 \pmod{t/2}$ and if $j \geq 3$ then $t^{j-1}/j \equiv 0 \pmod t$. Thus $t/2$ must divide the first term of (2.5), i.e. $(t/2)|(\gamma\eta - \overline{\gamma\eta})/\beta$, a contradiction. Suppose $t \not\equiv 0 \pmod 2$ and $t \nmid (\gamma\eta - \overline{\gamma\eta})/\beta$. Then we have $t^{j-1}/j \equiv 0 \pmod t$ for all $j \geq 2$ thus $t|(\gamma\eta - \overline{\gamma\eta})/\beta$, which is a contradiction. So, in either case there is no solution in the positive integers.

Now assume we are in the situation of part 2 and that $n \geq 2$. Then equation (2.5) reduces to

$$\sum_{j=2}^{n} \frac{t^{j-1}}{j}\binom{n-1}{j-1}\gamma\eta\frac{\eta^{j-1} - \overline{\eta}^{j-1}}{\beta} = 0.$$

Then applying $\binom{n-1}{j-1} = \frac{n-1}{j-1}\binom{n-2}{j-2}$ and multiplying by $\frac{2}{t(n-1)}$, since $t \neq 0$ and $n \geq 2$, we have

$$\sum_{j=2}^{n} \frac{2t^{j-2}}{j(j-1)}\binom{n-2}{j-2}\frac{\eta^{j-1} - \overline{\eta}^{j-1}}{\beta} = 0. \tag{2.6}$$

Suppose $t \equiv 0 \pmod 3$. If $j = 3$ we have $2t^{j-2}/j(j-1) \equiv 0 \pmod{t/3}$ and $2t^{j-2}/j(j-1) \equiv 0 \pmod t$ if $j \geq 4$. Thus $t/3$ divides the first term of (2.6), hence there are no solutions $n \geq 2$ if $t/3 \nmid (\eta - \overline{\eta})/\beta$. If $(\eta - \overline{\eta})/\beta \equiv 0 \pmod 3$ then t divides the $j = 3$ term and so it must also divide the first term as well. So if $t \nmid (\eta - \overline{\eta})/\beta$ then there is no solution $n \geq 2$. Now suppose that $t \not\equiv 0 \pmod 3$ and $t \nmid (\eta - \overline{\eta})/\beta$. Then we have $2t^{j-2}/j(j-1) \equiv 0 \pmod t$ for all $t \geq 3$, thus t divides the first term of (2.6), which is a contradiction. □

Lemma 2.4. *Let λ and α be algebraic integers in an imaginary quadratic field K with ring of integers $\mathcal{O}_K$ such that $0 < \arg\lambda < \pi$, $0 < \arg\alpha < \pi/2$ and $\alpha/\overline{\alpha}$ is not a root of unity. Assume there exist positive integers k and l with $k \leq l$ such that $\alpha^k = \delta + a\overline{\lambda}$ and $\alpha^l = \delta' + a'\overline{\lambda}$, for some $a, a' \in \mathbb{Z}$ with $|a| > 1$ and $\delta, \delta' \in \{-1, 1\}$. Write $l = qk + r$ with $0 \leq r < l$. Then $\lambda\alpha^r - \overline{\lambda}\overline{\alpha}^r = \delta'\delta^q(\lambda - \overline{\lambda})$.*

Proof. If $l = k$ then we have $r = 0$, $a = a'$, $\delta = \delta'$ and so the result is trivial. Assume that $l > k$. Observe that

$$\delta'(\lambda - \overline{\lambda}) = \lambda\alpha^l - \overline{\lambda}\overline{\alpha}^l = \lambda\alpha^r(\delta + a\overline{\lambda})^q - \overline{\lambda}\overline{\alpha}^r(\delta + a\lambda)^q.$$

Hence

$$\delta^q\delta'(\lambda-\overline{\lambda}) = \lambda\alpha^r - \overline{\lambda}\overline{\alpha}^r + a\lambda\overline{\lambda}\left(\alpha^r\frac{(1+\delta a\overline{\lambda})^q-1}{a\overline{\lambda}} - \overline{\alpha}^r\frac{(1+\delta a\lambda)^q-1}{a\lambda}\right). \tag{2.7}$$

If $k=1$ then $r=0$ then the term between the brackets in (2.7) is divisible by $a(\lambda-\overline{\lambda})$. Hence $a^2\lambda\overline{\lambda}(\lambda-\overline{\lambda})$ divides $(\lambda-\overline{\lambda})-\delta^q\delta'(\lambda-\overline{\lambda})$. Since $|a|>1$ this is only possible if $\delta^q\delta'=1$ and our Lemma is established in this case.

Now assume $k\geq 2$. Let d be a positive square-free integer such that $K=\mathbb{Q}(\sqrt{-d})$. If $d\equiv -1 \pmod 4$ then the term between the brackets in (2.7) is divisible by $\sqrt{-d}$ in $\mathcal{O}_K$ and we set $C(d)=\sqrt{d}$, otherwise this term is divisible by $2\sqrt{-d}$ and we set $C(d)=2\sqrt{d}$. Then (2.7) implies

$$iC(d)a\lambda\overline{\lambda}|(\lambda\alpha^r - \overline{\lambda}\overline{\alpha}^r - \delta^q\delta'(\lambda-\overline{\lambda})).$$

Suppose that $\lambda\alpha^r-\overline{\lambda}\overline{\alpha}^r \neq \delta^q\delta'(\lambda-\overline{\lambda})$. Then

$$C(d)\left|a\lambda\overline{\lambda}\right| \leq \left|\lambda\alpha^r-\overline{\lambda}\overline{\alpha}^r-\delta^q\delta'(\lambda-\overline{\lambda})\right|.$$

Using $\alpha^k=\delta+a\overline{\lambda}$ and the triangle inequality, we have

$$|\lambda|\,C(d)(|\alpha|^k-1) \leq C(d)\,|\lambda|\left|\alpha^k-\delta\right| < C(d)\left|a\lambda\overline{\lambda}\right| \leq 2\,|\lambda|\,(|\alpha|^r+1),$$

hence

$$1 < \frac{2}{|\alpha|\,C(d)} + \frac{1+2/C(d)}{|\alpha|^k}. \tag{2.8}$$

Since α is an algebraic integer in $\mathbb{Q}(\sqrt{-d})$ and $0<\arg\alpha<\pi/2$ we have $|\alpha|\geq\sqrt{1+d}$. Now if $d\not\equiv -1 \pmod 4$ and $d\geq 2$ then

$$\frac{2}{|\alpha|\,C(d)} + \frac{1+2/C(d)}{|\alpha|^k} \leq \frac{1}{\sqrt{1+d}\sqrt{d}} + \frac{1+1/\sqrt{d}}{1+d} \leq \frac{1}{\sqrt{6}} + \frac{1+1/\sqrt{2}}{3} < 1.$$

If $d\equiv -1 \pmod 4$ and $d\geq 11$, then

$$\frac{2}{|\alpha|\,C(d)} + \frac{1+2/C(d)}{|\alpha|^k} \leq \frac{4}{\sqrt{1+d}\sqrt{d}} + \frac{4+8/\sqrt{d}}{1+d} \leq \frac{2}{\sqrt{33}} + \frac{4+8/\sqrt{11}}{12} < 1.$$

We see that any solution of (2.8) must have $d=1,3,7$. After some calculations it can be shown that these solutions are given by $\alpha=(1+\sqrt{-7})/2, 1+i, 1+\sqrt{-3}, (3+\sqrt{-3})/2, (1+\sqrt{-3})/2$. Every solution except the first has $\alpha/\overline{\alpha}$ a root of unity and can be ignored. Say $\alpha=(1+\sqrt{-7})/2$. Then (2.8) implies that $k\leq 3$. Then the condition $\alpha^k=\delta+a\overline{\lambda}$, with $a\in\mathbb{Z}$ and $|a|>1$, implies that $((1+\sqrt{-7})/2)^k-\delta$ is divisible by a rational integer of absolute value at least 2, which is impossible if $k\leq 3$. Thus $\lambda\alpha^r-\overline{\lambda}\overline{\alpha}^r=\delta'\delta^q(\lambda-\overline{\lambda})$. □

Lemma 2.5. *Let α be an algebraic integer in an imaginary quadratic field with $0 < \arg\alpha < \pi/2$ and $\alpha/\overline{\alpha}$ not a root of unity. Let k, m be positive integers with $k < l$.*

(a) *If $\alpha^l \pm \alpha^k = \pm 2$ for some choice of the $\pm$ signs then $(k, l, \alpha) = (1, 3, (1+\sqrt{-7})/2)$ or $(1, 2, (1+\sqrt{-7})/2)$.*

(b) *If $\alpha^l \pm 2\alpha^k = \pm 3$ for some choice of the $\pm$ signs then $(k, l, \alpha) = (1, 3, (1+\sqrt{-11})/2)$ or $(1, 2, 1+\sqrt{-2})$.*

(c) *If $\alpha^l \pm 3\alpha^k \in \{\pm 2, \pm 4\}$ for some choice of the $\pm$ signs then $(k, l, \alpha) = (2, 4, (1+\sqrt{-7})/2), (1, 4, (1+\sqrt{-7})/2), (1, 2, (3+\sqrt{-7})/2)$ or $(1, 3, (1+\sqrt{-15})/2)$*

Proof. (a) If α satisfies $\alpha^l \pm \alpha^k = \pm 2$ then $\alpha^k | 2$ and $k \leq 2$. Moreover $|\alpha|^l \leq |\alpha|^k + 2 \leq |\alpha|^2 + 2$, hence $l \leq 4$. If $k = 2$ and $l = 4$ then we have a quadratic equation in α^2. Solving, yields $\alpha = \pm i, \pm\sqrt{-2}$ which can be ignored, since these solutions yield $\alpha/\overline{\alpha}$ a root of unity. If $k = 2$ and $l = 3$ we can consider $\alpha^3 \pm \alpha^2 - 2 = 0$ by replacing α with $-\alpha$. If this equation has a solution in quadratic integers then it must also have a solution in $\mathbb{Z}$. This happens in the case $\alpha^3 + \alpha^2 - 2 = 0$ and we get $\alpha = 1, -1 \pm i$, which can all be ignored. We treat the case $k = 1$ and $l = 3$ similarly and obtain $\alpha = (\pm 1 \pm \sqrt{-7})/2$. If $l = 4$ and $k = 1$ then we get $|\alpha|^4 \leq |\alpha| + 2$, contradicting $|\alpha| \geq \sqrt{2}$. If $l = 2$ and $k = 1$ then we get $\alpha = (\pm 1 \pm \sqrt{-7})/2$. In either case the condition $0 < \arg\alpha < \pi$ yields $\alpha = (1+\sqrt{-7})/2$.

(b) If α is such that $\alpha^l \pm 2\alpha^k = \pm 3$, then $\alpha^k | 3$ and $k \leq 2$. Also, $|\alpha|^l \leq 2|\alpha|^k + 3 \leq 2|\alpha|^2 + 3$, and so we must have $l \leq 4$ since $|\alpha|^2 \geq 3$. Solving the equation $\alpha^l \pm 2\alpha^k = \pm 3$ in a similar way as in (a) we obtain the solutions as stated above.

(c) If α satisfies $\alpha^l \pm 3\alpha^k \in \{\pm 2, \pm 4\}$ then $\alpha^k | 4$ and $k \leq 4$. If $\alpha | 4$, $0 < \arg\alpha < \pi/2$ and $\alpha/\overline{\alpha}$ is not a root of unity then $\alpha \in \{(1+\sqrt{-7})/2, (3+\sqrt{-7})/2, 1+\sqrt{-7}, (1+\sqrt{-15})/2\}$. With these choices $\alpha^k | 4$ implies that $k \leq 2$. If $k = 2$ then $\alpha^2 | 4$ and we must have $\alpha = (1+\sqrt{-7})/2$. Then $\alpha^l - 2 \pm 3 \in \{\pm 4/\alpha^2, \pm 2/\alpha^2\}$ and we get $l = 4$. Now assume $k = 1$. We consider $\alpha^l - 1 \pm 3 \in \{\pm 4/\alpha, \pm 2/\alpha\}$ for $\alpha = (1+\sqrt{-7})/2, (3+\sqrt{-7})/2, 1+\sqrt{-7}, (1+\sqrt{-15})/2$ and we get the solutions $(k, l, \alpha) = (1, 4, (1+\sqrt{-7})/2), (1, 2, (3+\sqrt{-7})/2$ or $(1, 3, (1+\sqrt{-15})/2)$. □

Lemma 2.6. *Let α be a complex quadratic integer such that $\alpha/\overline{\alpha}$ is not a root of unit and $0 < \arg\alpha < \pi/2$. Suppose there exists positive rational integers l, k, with $l > k$, and a quadratic integer λ such that $\alpha^k = \delta + a\overline{\lambda}$ and $\alpha^l = \delta' + a'\overline{\lambda}$ for some $\delta, \delta' \in \{-1, 1\}$ and $a, a' \in \mathbb{Z}$. Then $|a| \leq |a'|$.*

Proof. Suppose $|a| > |a'|$. Since $\left|\alpha^k - \delta\right| = \left|a\overline{\lambda}\right|$ and $\left|\alpha^l - \delta'\right| = \left|a'\overline{\lambda}\right|$, we get $(|a'| - |a|)\left|\overline{\lambda}\right| = \left|\alpha^l - \delta\right| - \left|\alpha^k - \delta'\right| \geq |\alpha|^l - |\alpha|^k - 2$. Hence $|\alpha|^l - |\alpha|^k - 2 \leq |a'| - |a| \leq -1$, which yields $|\alpha|^k (|\alpha|^{l-k} - 1) \leq 1$. Since $|\alpha| \geq \sqrt{2}$ we get $l = k + 1$. Moreover we must have $|\alpha| = \sqrt{2}$ and $k = 2$, hence $\alpha = (1+\sqrt{-7})/2$. Now $(1+\sqrt{-7})/2 = \delta + a\overline{\lambda}$ for $\delta \in \{-1, 1\}$ and $a \in \mathbb{Z}$ yields $a = \pm 1$. Then $|a'| < |a|$ gives $a' = 0$ contradicting $((1+\sqrt{-7})/2)^2 = \delta' + a'\overline{\lambda}$. □

Lemma 2.7. *Let α and λ be integers in an imaginary quadratic field K, with $0 < \arg\alpha < \pi/2$, $0 < \arg\lambda < \pi$ and $\alpha/\overline{\alpha}$ not a root of unity. Suppose $\alpha^k = \delta + a\overline{\lambda}$ for some positive integer k, $\delta \in \{-1, 1\}$ and $a \in \mathbb{Z}$ with $|a| > 3$. Then $\lambda\alpha^n - \overline{\lambda}\overline{\alpha}^n = \pm(\lambda - \overline{\lambda})$ has no solutions $n > k$.*

Proof. Suppose

$$\lambda\alpha^n - \overline{\lambda}\overline{\alpha}^n = \delta'(\lambda - \overline{\lambda}) \tag{2.9}$$

for some $\delta' \in \{-1, 1\}$ and $n \geq k$. Say $n = qk + r$ for $q, r \in \mathbb{Z}$ with $q > 0$ and $0 \leq r < k$. By Lemma 2.4 we get $\lambda\alpha^r - \overline{\lambda}\overline{\alpha}^r = \delta'\delta^q(\lambda - \overline{\lambda})$ and then (2.9) can be written as

$$\lambda\alpha^r(\delta + a\overline{\lambda})^q - \overline{\lambda}\overline{\alpha}^r(\delta + a\lambda)^q = \delta^q(\lambda\alpha^r - \overline{\lambda}\overline{\alpha}^r)$$

hence

$$\lambda\alpha^r(1 + \delta a\overline{\lambda})^q - \overline{\lambda}\overline{\alpha}^r(1 + \delta a\lambda)^q = \lambda\alpha^r - \overline{\lambda}\overline{\alpha}^r.$$

If $\alpha^r - \overline{\alpha}^r = 0$ then we must have $r = 0$ since $\alpha/\overline{\alpha}$ is not a root of unity. We can then apply part 2 of Lemma 2.3 with $\gamma = \lambda$, $\eta = \overline{\lambda}$, $\beta = \lambda - \overline{\lambda}$ and $t = \delta a$. Then $(\eta - \overline{\eta})/\beta = -1$. Since $|a| > 3$ the conditions of part 2 in Lemma 2.3 are fulfilled, yielding $q = 1$.

Suppose $\alpha^r - \overline{\alpha}^r \neq 0$. Since $\lambda\alpha^r - \overline{\lambda}\overline{\alpha}^r = \delta'\delta^q(\lambda - \overline{\lambda})$, Lemma 2.2 implies that $\alpha^r = \delta'' + a'\overline{\lambda}$ for some $a' \in \mathbb{Z}$ and $\delta'' \in \{-1, 1\}$. Now we apply part 1 of Lemma 2.3 with $\gamma = \lambda\alpha^r$, $\eta = \overline{\lambda}$, $\beta = \lambda\overline{\lambda}(\lambda\alpha^r - \overline{\lambda}\overline{\alpha}^r)$ and $t = \delta a$. Now

$$\frac{\gamma\eta - \overline{\gamma\eta}}{\beta} = \frac{\lambda\overline{\lambda}(\alpha^r - \overline{\alpha}^r)}{\lambda\overline{\lambda}(\lambda\alpha^r - \overline{\lambda}\overline{\alpha}^r)} = \frac{a'(\overline{\lambda} - \lambda)}{\delta''(\lambda - \overline{\lambda})} = -\delta''a'.$$

This implies that $\beta|(\gamma\eta^l - \overline{\gamma\eta}^l)$ for all $l \geq 1$. Now part 1 of Lemma 2.3 implies that either $q = 0$, which contradicts our assumption that $q > 0$, or that $a|a'$ if $a \equiv 1 \pmod 2$ and $(a/2)|a'$ if $a \equiv 0 \pmod 2$. By Lemma 2.6 we have $|a'| \leq |a|$ thus $|a| = |a'|$ or $|a| = 2\,|a'|$. Suppose $|a| = |a'|$. Then, since $\alpha^k = \delta \pm a'\overline{\lambda}$ and $\alpha^r = \delta'' + a'\overline{\lambda}$, we have $\alpha^k \pm \alpha^r = \pm 2$ or 0. Since $\alpha/\overline{\alpha}$ is not a root of unity we must have $\alpha^k \pm \alpha^r = \pm 2$, thus $\alpha^r|2$ and $|\alpha| \leq \sqrt{2}$. This contradicts $\alpha^r = \delta'' + a'\overline{\lambda}$ because $|a'| = |a| > 3$. If $|a| = 2\,|a'|$, then $\alpha^k = \delta \pm 2a'\overline{\lambda}$ and $\alpha^r = \delta'' + a'\overline{\lambda}$. So $\alpha^k \pm 2\alpha^r = \pm 1, \pm 3$. Since α is not a root of unity we must have $\alpha^k \pm 2\alpha^r = \pm 3$. By Lemma 2.5 we get $(r, k, \alpha) = (1, 3, (1 + \sqrt{-11})/2)$ or $(1, 2, 1 + \sqrt{-2})$. Since $\alpha^r = \delta'' + a'\overline{\lambda}$, with $|a'| \geq 2$ it follows that one of the numbers $\pm 1 + (1 + \sqrt{-11})/2$ as well as one of the numbers $\pm 1 + 1 + \sqrt{-2}$ is divisible in $\mathcal{O}_K$ by a rational integer of absolute value greater than 1, which is a contradiction. Thus there are no solutions n with $n > k$. □

Lemma 2.8. *For each of the given α, λ, we determine all solutions to the equation $\lambda\alpha^n - \overline{\lambda}\overline{\alpha}^n = \pm(\lambda - \overline{\lambda})$ in $n \geq 0$.*

1. $(\alpha, \lambda) = ((1+\sqrt{-7})/2, (1+\sqrt{-7})/2)$ *then* $n = 0, 1, 2, 4, 12$
2. $(\alpha, \lambda) = (1+\sqrt{-2}, \sqrt{-2})$ *then* $n = 0, 1, 2, 5$
3. $(\alpha, \lambda) = ((1+\sqrt{-11})/2, (1+\sqrt{-11})/2)$ *then* $n = 0, 1, 4$
4. $(\alpha, \lambda) = ((1+\sqrt{-11})/2, (-3+\sqrt{-11})/2)$ *then* $n = 0, 1, 3$
5. $(\alpha, \lambda) = ((1+\sqrt{-15})/2, (-3+\sqrt{-15})/2)$ *then* $n = 0, 1, 3$
6. $(\alpha, \lambda) = ((1+\sqrt{-19})/2, (1+\sqrt{-19})/2)$ *then* $n = 0, 1, 6$.

Proof. Part $1, 2, 3$ and 6 can be established by Lemma 2.7 since

$$\begin{aligned}
((1+\sqrt{-7})/2)^{12} &= -1 - 45(1-\sqrt{-7})/2, \\
(1+\sqrt{-2})^5 &= 1 - 11\sqrt{-2}, \\
((1+\sqrt{-11})/2)^4 &= 1 + 5(1-\sqrt{-11})/2, \\
((1+\sqrt{-19}/2)^6 &= 1 - 56(1-\sqrt{-19})/2.
\end{aligned}$$

Thus in these cases all solutions satisfy $n \leq 12$, $n \leq 5$, $n \leq 4$ and $n \leq 6$ respectively. This small set of possibilities in each may be checked by considering the corresponding recurrence sequences, yielding the set of solutions stated above.

In part 4 we notice that $\alpha^4 = 1 + 5\overline{\alpha}$. Write $n = 4q + r$, with $0 \leq r < 4$. We are then looking for solutions to

$$\lambda\alpha^r(1+5\overline{\alpha})^q - \overline{\lambda}\overline{\alpha}^r(1+5\alpha)^q = \pm(\lambda - \overline{\lambda}).$$

If $1 \leq r \leq 3$ then, since $\alpha\overline{\alpha} = 3$, the above yields $\lambda\alpha^r - \overline{\lambda}\overline{\alpha}^r \equiv \pm(\lambda - \overline{\lambda}) \pmod{15}$. Now $\left|\lambda\alpha^r - \overline{\lambda}\overline{\alpha}^r\right| < 15$ since $r \leq 3$, so we have $\lambda\alpha^r - \overline{\lambda}\overline{\alpha}^r = \pm(\lambda - \overline{\lambda})$. Note that this holds trivially if $r = 0$. Thus

$$\lambda\alpha^r(1+5\overline{\alpha})^q - \overline{\lambda}\overline{\alpha}^r(1+5\alpha)^q = \lambda\alpha^r - \overline{\lambda}\overline{\alpha}^r.$$

Now we can apply part 1 of Lemma 2.3 with $\gamma = \lambda\alpha^r$, $\eta = \overline{\alpha}$, $\beta = \sqrt{-11}$ and $t = 5$, which yields $q = 0$. So any solution must satisfy $n \leq 3$ and we can check that the solutions are $n = 0, 1, 3$.

In part 5 we notice that $\alpha^3 = -1 + 3\lambda$. Write $n = 3q + r$ with $0 \leq r \leq 2$ and suppose that $\lambda\alpha^n - \overline{\lambda}\overline{\alpha}^n = \delta(\lambda - \overline{\lambda})$ for some $\delta \in \{-1, 1\}$. If $n \geq 3$ then, by Lemma 2.4, $\lambda\alpha^r - \overline{\lambda}\overline{\alpha}^r = (-1)^q\delta(\lambda - \overline{\lambda})$, yielding

$$\lambda\alpha^r(1-3\overline{\lambda})^q - \overline{\lambda}\overline{\alpha}^r(1-3\lambda)^q = \lambda\alpha^r - \overline{\lambda}\overline{\alpha}^r.$$

If $r = 0$ we can apply part 2(b) of Lemma 2.3 with $\gamma = \lambda\alpha^r = \lambda$, $\eta = \overline{\lambda}$, $\beta = \lambda - \overline{\lambda}$, $t = -3$ and we get $q \leq 1$. If $r \neq 0$ then we apply part 1 of Lemma 2.3 with $\gamma = \lambda\alpha^r$, $\eta = \overline{\lambda}$, $\beta = 6\sqrt{-15}$ and $t = -3$, and we see that there are no solutions with $q \geq 1$. Thus we must have $n \leq 3$ and we can check that the solutions are $n = 0, 1, 3$. □

Theorem 2.1. *Suppose that $\{u_n\}_{n\geq 0}$ is a nondegenerate binary recurrence sequence of rational integers with companion polynomial $z^2 - c_1 z - c_2 \in \mathbb{Z}[x]$ such that $u_0 > 0$, $\gcd(u_0, u_1) = 1$, $c_1 \geq 0$ and $c_1^2 + 4c_2 < 0$. If $u_n = \pm u_0$ has more than three solutions then one of the following holds:*

$$\begin{array}{ll} c_1 = 1,\ c_2 = -2,\ u_0 = u_1 = 1 & \textit{which has solutions } n = 0, 1, 2, 4, 12 \\ c_1 = 1,\ c_2 = -2,\ u_0 = 1,\ u_1 = -1 & \textit{which has solutions } n = 0, 1, 3, 11 \\ c_1 = 3,\ c_2 = -4,\ u_0 = u_1 = 1 & \textit{which has solutions } n = 0, 1, 2, 6 \\ c_1 = 2,\ c_2 = -3,\ u_0 = u_1 = 1 & \textit{which has solutions } n = 0, 1, 2, 5. \end{array}$$

Proof. By Lemma 2.1 the sequence is given by

$$u_n = \frac{\lambda\alpha^n - \overline{\lambda}\overline{\alpha}^n}{\alpha - \overline{\alpha}},$$

for each $n \geq 0$, where α is a root of $z^2 - c_1 z - c_2$ and $\lambda = u_1 - u_0\overline{\alpha}$. We let α be the root with positive imaginary part. Since $\alpha + \overline{\alpha} = c_1 \geq 0$ and $\alpha/\overline{\alpha}$ is not a root of unity we see that $0 < \arg\alpha < \pi/2$. Since $u_0 > 0$, $\lambda \notin \mathbb{R}$ so $0 < \arg\lambda < \pi$. The equation $u_n = \pm u_0$ can be rewritten as

$$\lambda\alpha^n - \overline{\lambda}\overline{\alpha}^n = \pm(\lambda - \overline{\lambda}). \tag{2.10}$$

We may assume that λ and $\overline{\lambda}$ have no common integer factor in $\mathcal{O}_{\mathbb{Q}(\alpha)}$.

Suppose that (2.10) has at least four solution, denoted by $n = 0, k, l, m$ with $0 < k < l < m$. By Lemma 2.2 there are rational integers a, a' such that $\alpha^k = \delta + a\overline{\lambda}$ and $\alpha^l = \delta' + a'\overline{\lambda}$ for $\delta, \delta' \in \{-1, 1\}$. Since there is a larger solution m we have, by Lemma 2.6 and Lemma 2.7, that $|a| \leq |a'| \leq 3$.

Assume $|a| = |a'|$. Then $\alpha^l \pm \alpha^k \in \{-2, 0, 2\}$. Since α is not a root of unit we have $\alpha^l \pm \alpha^k = \pm 2$. By Lemma 2.5 we must have $(k, l, \alpha) = (1, 2, (1 + \sqrt{-7})/2)$ or $(1, 3, (1 + \sqrt{-7})/2)$. Then $\alpha^k = \pm 1 + a\overline{\lambda}$ and $\alpha^l = \pm 1 \pm a\overline{\lambda}$ for λ a quadratic integer in $\mathbb{Q}(\sqrt{-7})$ with $0 < \arg\lambda < \pi$ yields $\lambda = (1 + \sqrt{-7})/2$ if $l = 2$ and $\lambda = (-3 + \sqrt{-7})/2$ if $l = 3$.

Assume $|a'| = 3$ and $|a| = 2$. Then $2\alpha^l \pm 3\alpha^k \in \{-5, -1, 1, 5\}$ and since α is not a root of unity we must have $2\alpha^l \pm 3\alpha^k = \pm 5$. Thus $\alpha^k | 5$, so $|\alpha|^k = \sqrt{5}$ or 5 and $k \leq 2$. Also $|\alpha|^l \leq 3/2\,|\alpha|^k + 5/2 \leq 10$ which gives $l \leq 2$. Solving $2\alpha^2 \pm 3\alpha = \pm 5$ yields no relevant solutions.

Assume $|a'| = 3$ and $|a| = 1$. Then $\alpha^l \pm 3\alpha^k \in \{-4, -2, 2, 4\}$. By Lemma 2.5 we have $(k, l, \alpha) = (1, 4, (1 + \sqrt{-7})/2)$, $(2, 4, (1 + \sqrt{-7})/2)$, $(1, 2, (3 + \sqrt{-7})/2)$ or $(1, 3, (1 + \sqrt{-15})/2)$. The equations $\alpha^k = \pm 1 + a\overline{\lambda}$ and $\alpha^l = \pm 1 + a'\overline{\lambda}$ then yield $\lambda = (1+\sqrt{-7})/2$, $(1+\sqrt{-7})/2$, $(-1+\sqrt{-7})/2$ or $(-3+\sqrt{-15})/2$ respectively.

Assume $|a'| = 2$ and $|a| = 1$. Then $\alpha^l \pm \alpha^k \in \{-3, -1, 1, 3\}$ and since α is not a root of unity we have $\alpha^l \pm \alpha^k = \pm 3$. Lemma 2.5 then gives $(k, l, \alpha) = (1, 2, 1 + \sqrt{-2})$ or $(1, 3, (1 + \sqrt{-11})/2)$. Then $\alpha^k = \pm 1 + a\overline{\lambda}$ and $\alpha^l = \pm 1 + a'\overline{\lambda}$ imply that $\lambda = \sqrt{-2}$ or $(-3 + \sqrt{-11})/2$ respectively.

Thus if equation (2.10) has at least four solutions then (λ, α) is given by one of the following:

$$\begin{gathered}((1 + \sqrt{-7})/2, (1 + \sqrt{-7})/2),\\ ((-1 + \sqrt{-7})/2, (3 + \sqrt{-7})/2),\\ ((-3 + \sqrt{-7})/2, (1 + \sqrt{-7})/2),\\ ((-3 + \sqrt{-11})/2, (1 + \sqrt{-11})/2),\\ ((-3 + \sqrt{-15})/2, (1 + \sqrt{-15})/2),\\ (\sqrt{-2}, 1 + \sqrt{-2}).\end{gathered}$$

In the first case it follows from Lemma 2.8 that (2.10) has the solutions $n = 0, 1, 2, 4, 12$. In the second case, since $(3 - \sqrt{-7})/2 = -((1 + \sqrt{-7})/2)^2$ we have the equation

$$\frac{-1 + \sqrt{-7}}{2}\left(\frac{1 - \sqrt{-7}}{2}\right)^{2n} - \frac{-1 - \sqrt{-7}}{2}\left(\frac{1 + \sqrt{-7}}{2}\right)^{2n} = \pm\sqrt{-7},$$

which has the solutions $n = 0, 1, 2, 6$, corresponding to the even solutions in our first case. In the third case we notice that $(3 - \sqrt{-7})/2 = ((1 + \sqrt{-7})/2)^2$ and so we have the equation

$$-\frac{1 + \sqrt{-7}}{2}\left(\frac{1 + \sqrt{-7}}{2}\right)^{n+1} + \frac{1 - \sqrt{-7}}{2}\left(\frac{1 - \sqrt{-7}}{2}\right)^{n+1} = \pm\sqrt{-7},$$

which has the solutions $n = 0, 1, 3, 11$, corresponding to the last four solutions in the first case. In the fourth, fifth and sixth cases the solutions are given by Lemma 2.8 and only in the last case do we have more than three, namely $n = 0, 1, 2, 5$. For these pairs (λ, α) for which (2.10) has more than three solutions we get the recurrences as stated in the Theorem. □

Theorem 2.2. *Let $\{u_n\}_{n\geq 0}$ be are non-degenerate recurrence sequence of rational integers with companion polynomial $z^2 - c_1 z - c_2 \in \mathbb{Z}[z]$ such that $u_0 > 0$, $\gcd(u_0, u_1) = 1$, $c_1 \geq 0$ and $c_1^2 + 4c_2 \geq 0$. The equation $u_n = \pm u_0$ has at most three solutions in n, unless $c_1 = 1$, $c_2 = 1$, $u_0 = 1$ and $u_1 = -1$, in which case the solutions are $n = 0, 1, 3, 4$.*

Proof. As in the proof of Theorem 2.1 we consider the equation (2.10), where, in this case, λ_1 and α_1 are integers in a real number field K of degree at most two over $\mathbb{Q}$. Let d be the positive squarefree integer such that $K = \mathbb{Q}(\sqrt{d})$, we take $d = 1$ if $c_1^2 + 4c_2 = 0$. Since $c_1 \geq 0$ we may assume $\alpha_1 \geq |\alpha_2|$. Moreover $\alpha_1/\alpha_2 \neq \pm 1$ implies $c_1 = \alpha_1 + \alpha_2 \geq 1$ and since $(\alpha_1 - \alpha_2)/\sqrt{d} \in \mathbb{Z}$, we have $\alpha_1 - \alpha_2 \geq 1$. We conclude $\alpha_1 \geq |\alpha_2| + 1$. First assume that $\alpha_2 = 1$. Then (2.2) becomes

$$\alpha_1^n \in \left\{1, 1 - 2\frac{\lambda_1}{\lambda_2}\right\}, \tag{2.11}$$

which has at most one solution since $\alpha_2 = 1$ implies α_1 is not a root of unity. If $\alpha_2 = -1$ then by considering even and odd solutions separately we get two equations similar to (2.11) each can have at most one solution. Thus we can assume that $\alpha_2 \neq \pm 1$. Note that this also implies $\alpha_1 \neq \pm 1$ since $\alpha_1 \geq |\alpha_2| + 1$.

Suppose we have four solutions $n = 0, k, l, m$. If we eliminate λ_1 and λ_2 from the equations

$$\begin{aligned}\lambda_1\alpha_1^k - \lambda_2\alpha_2^k &= \pm(\lambda_1 - \lambda_2)\\ \lambda_1\alpha_1^l - \lambda_2\alpha_2^l &= \pm(\lambda_1 - \lambda_2)\\ \lambda_1\alpha_1^m - \lambda_2\alpha_2^m &= \pm(\lambda_1 - \lambda_2),\end{aligned}$$

we obtain

$$\frac{\alpha_1^k - \delta}{\alpha_2^k - \delta} = \frac{\alpha_1^l - \delta'}{\alpha_2^l - \delta'} = \frac{\alpha_1^m - \delta''}{\alpha_2^m - \delta''} = \frac{\lambda_1}{\lambda_2}, \tag{2.12}$$

for some $\delta, \delta', \delta'' \in \{-1, 1\}$. We note that two of these deltas must be equal and we treat the cases corresponding to -1 and $+1$ separately. First suppose that $l > k$ and

$$\frac{\alpha_1^k - 1}{\alpha_2^k - 1} = \frac{\alpha_1^l - 1}{\alpha_2^l - 1}. \tag{2.13}$$

If $\alpha_2 > 0$ then note that for any positive integer x

$$\begin{aligned}\left|\frac{\alpha_1^x - 1}{\alpha_2^x - 1}\right| \left|\frac{\alpha_1^{x+1} - 1}{\alpha_2^{x+1} - 1}\right|^{-1} &= \left|\frac{\alpha_1^x - 1}{\alpha_1^{x+1} - 1}\right| \left|\alpha_2 + \frac{\alpha_2 - 1}{\alpha_2^x - 1}\right|\\ &< \frac{1}{\alpha_1}\left|\alpha_2 + \frac{1}{\alpha_2^{x-1} + \cdots + 1}\right|\\ &< \frac{1}{\alpha_1}(|\alpha_2| + 1) \leq 1.\end{aligned}$$

Thus $|(\alpha_1^x - 1)/(\alpha_2^x - 1)|$ is strictly increasing in x and (2.13) cannot hold. So we must have $\alpha_2 < 0$. We distinguish three subcases.

If k and l are both even then we may consider (2.13) with α_1^2 instead of α_1. Since $\alpha_2^2 > 0$ we see, by above, that this cannot occur.

If k is odd then

$$\frac{\alpha_1^k - 1}{|\alpha_2|^k + 1} = \left|\frac{\alpha_1^k - 1}{\alpha_2^k - 1}\right| = \left|\frac{\alpha_1^l - 1}{\alpha_2^l - 1}\right| \geq \frac{\alpha_1^l - 1}{|\alpha_2|^l + 1}.$$

But we see that $(\alpha_1^x - 1)/(|\alpha_2|^x + 1)$ is strictly increasing in $x \geq 1$, since

$$\begin{aligned}\frac{\alpha_1^x - 1}{|\alpha_2|^x + 1}\left(\frac{\alpha_1^{x+1} - 1}{|\alpha_2|^{x+1} + 1}\right)^{-1} &= \frac{\alpha_1^x - 1}{\alpha_1^{x+1} - 1}\frac{|\alpha_2|^{x+1} + 1}{|\alpha_2|^x + 1} \\ &< \frac{1}{\alpha_1}\left(|\alpha_2| + \frac{1 - |\alpha_2|}{|\alpha_2|^x + 1}\right) \\ &< \frac{1}{\alpha_1}(|\alpha_2| + 1) \leq 1.\end{aligned}$$

And so (2.13) cannot hold when $\alpha_2 < 0$ and k is odd.

If k is even and l is odd then by comparing the signs in (2.13) we see that $-1 < \alpha_2 < 0$. Then α_1 and α_2 are conjugate real quadratic integers and since $\alpha_1 > 0$ and $\alpha_2 > -1$ we have $(\alpha_1 + 1)(\alpha_2 + 1) \geq 1$. Hence

$$\begin{aligned}\left|\frac{\alpha_1^k - 1}{\alpha_2^k - 1}\right| &= \frac{1}{\alpha_2 + 1}\frac{\alpha_1^k - 1}{\left|\alpha_2^{k-1} - \alpha_2^{k-2} + \cdots - 1\right|} \\ &\leq \frac{1}{\alpha_2 + 1}\frac{\alpha_1^k - 1}{|\alpha_2| + 1} \\ &\leq (\alpha_1 + 1)\frac{\alpha_1^k - 1}{|\alpha_2| + 1}.\end{aligned}$$

We also have

$$\left|\frac{\alpha_1^l - 1}{\alpha_2^l - 1}\right| > \frac{\alpha_1^l - 1}{2}.$$

These two inequalities combined with (2.13) imply

$$\alpha_1^l - 1 < 2\frac{\alpha_1 + 1}{|\alpha_2| + 1}(\alpha_1^k - 1). \tag{2.14}$$

From (2.14) we have $\alpha_1^l - 2\alpha_1^{k+1} - \alpha_1^k + \alpha_1 + 1 < 0$, so if $l \geq k + 3$ we must have $\alpha_1 < 2$. The only real, positive, non-rational quadratic integer α_1 such that $\alpha_1/\alpha_2 \neq \pm 1$ and $\alpha_1 < 2$

is $(1+\sqrt{5})/2$ which does not satisfy (2.14). Hence we must have $l = k+1$. However there is a third solution m and we have

$$\frac{\alpha_1^m - \delta''}{\alpha_2^m - \delta''} = \frac{\alpha_1^k - 1}{\alpha_2^k - 1}.$$

If $\delta'' = 1$ then we must have that $m > k$ and m is odd since the other possibilities were shown to be impossible. But then we have

$$\frac{\alpha_1^m - 1}{\alpha_2^m - 1} = \frac{\alpha_1^l - 1}{\alpha_2^l - 1},$$

with m and l odd, which was shown to be impossible. But we also cannot take $\delta'' = -1$ since $(\alpha_1^m + 1)/(\alpha_2^m + 1)$ and $(\alpha_1^k - 1)/(\alpha_2^k - 1)$ have opposite signs. We conclude that in (2.12) we can have at most one delta equal $+1$.

We now suppose that $l > k$ and

$$\frac{\alpha_1^k + 1}{\alpha_2^k + 1} = \frac{\alpha_1^l + 1}{\alpha_2^l + 1} \tag{2.15}$$

Note that $(\alpha_1^x + 1)/(\alpha_2^x + 1)$ is a strictly increasing function in $x \geq 1$ if $\alpha_2 > 0$. Hence we must have $\alpha_2 < 0$. We distinguish four subcases.

If k and l are both even the this is equivalent to considering (2.15) with α_1^2 instead of α_1 and this is impossible.

If k is even and l is odd then by consideration of the signs in (2.15) we must have $-1 < \alpha_2 < 0$. Hence

$$\alpha_1^k + 1 > \frac{\alpha_1^k + 1}{\alpha_2^k + 1} = \frac{\alpha_1^l + 1}{\alpha_2^l + 1} > \alpha_1^l + 1,$$

which is impossible since $\alpha_1 > 1$.

If k and l are both odd then (2.15) can be written as

$$\frac{\alpha_1^k + 1}{|\alpha_2|^k - 1} = \frac{\alpha_1^l + 1}{|\alpha_2|^l - 1}.$$

Since

$$\begin{aligned}\frac{\alpha_1^{2x-1}+1}{|\alpha_2|^{2x-1}-1}\left(\frac{\alpha_1^{2x+1}+1}{|\alpha_2|^{2x+1}-1}\right)^{-1} &= \frac{\alpha_1^{2x-1}+1}{\alpha_1^{2x+1}+1}\frac{|\alpha_2|^{2x+1}-1}{|\alpha_2|^{2x-1}-1}\\ &\le \frac{\alpha_1+1}{\alpha_1^3+1}\frac{|\alpha_2|^3-1}{|\alpha_2|-1}\\ &= \frac{|\alpha_2|^2+|\alpha_2|+1}{\alpha_1^2-\alpha_1+1}\\ &\le \frac{|\alpha_2|^2+|\alpha_2|+1}{(|\alpha_2|+1)^2-|\alpha_2|}=1,\end{aligned} \tag{2.16}$$

The sequence $(\alpha_1^{2x-1}+1)/(|\alpha_2|^{2x-1}-1)$ increases with $x \ge 1$. Moreover we have equality in (2.16) if and only if $x = 1$ and $\alpha_1 = 1-\alpha_2$, thus $k = 1$, $l = 3$ and $\alpha_2 = 1-\alpha_1$. Note there is a third solution m and we have

$$\frac{\alpha_1^m-\delta''}{\alpha_2^m-\delta''}=\frac{\alpha_1+1}{\alpha_2+1}.$$

Suppose that $\alpha_1 \ge 2$. Since we have assumed $\alpha_2 = 1-\alpha_1$ and $\alpha_1 \ne -1$ we have $\alpha_2 < -1$, $\alpha_1 > 2$ and m must be odd. Now

$$\frac{\alpha_1^5-1}{(\alpha_1-1)^5+1} \le \frac{\alpha_1^m-\delta''}{(\alpha_1-1)^m+\delta''} = -\frac{\alpha_1^m-\delta''}{\alpha_2^m-\delta''} = -\frac{\alpha_1+1}{\alpha_2+1} = \frac{\alpha_1+1}{\alpha_1-2},$$

which implies $2\alpha_1^5-5\alpha_1^4+5\alpha_1^2-6\alpha_1+2 \le 0$. We can check that this implies $\alpha_1 < (1+\sqrt{13})/2$. However there is no real quadratic integer such that $2 < \alpha_1 < (1+\sqrt{13})/2$, so we must have $\alpha_1 < 2$. This then implies that $\alpha_1 = (1+\sqrt{5})/2$. It then follows that

$$\frac{\alpha_1^m-1}{\alpha_1} \le \left|\frac{\alpha_1^m-\delta''}{\alpha_2^m-\delta''}\right| = \left|\frac{\alpha_1+1}{\alpha_2+1}\right| = \alpha_1^4,$$

hence $m \le 5$. Checking $(\alpha_1^m-\delta'')/(\alpha_2^m-\delta'') = (\alpha_1+1)/(\alpha_2+1)$ for $m \le 5$ then yields $\delta'' = -1$ and $m = 1, 3, 4$.

If k is odd and l is even then comparing the signs in (2.15) implies $-1 < \alpha_2 < 0$ and we

have

$$\begin{aligned}(\alpha_1+1)(\alpha_1^k+1) &\geq \frac{\alpha_1^k+1}{\alpha_2+1}\frac{1}{1+|\alpha_2|+\cdots+|\alpha_2|^{k-1}}\\ &= \frac{\alpha_1^k+1}{\alpha_2^k+1}\\ &= \frac{\alpha_1^l+1}{\alpha_2^l+1}\\ &> \frac{\alpha_1^l+1}{2}.\end{aligned}$$

And that implies $\alpha_1^l+1 < 2(\alpha_1+1)(\alpha_1^k+1)$. If $l \geq k+3$ then $\alpha_1 < 11/5$, hence $\alpha_1 = (1+\sqrt{5})/2$. Since $\alpha_1\alpha_2 = -1$ we get $(\alpha_1^l+1)/(\alpha_2^l+1) = \alpha_1^l$ and (2.15) implies

$$\alpha_1^l = \frac{\alpha_1^k+1}{\alpha_2^k+1} \leq \frac{\alpha_1^k+1}{\alpha_2+1} = \alpha_1^2(\alpha_1^k+1),$$

which yields $k=1$ and $l=4$. Suppose now that $l = k+1$ or that $k=1$ and $l=4$. There is a third solution m and

$$\frac{\alpha_1^m-\delta''}{\alpha_2^m-\delta''} = \frac{\alpha_1^l+1}{\alpha_2^l+1}.$$

If $\delta''=1$ then the terms have opposite sign, so we must have $\delta''=-1$. Note that we cannot have $m > l$ since l is even and we have shown that the smaller of two solutions cannot be even. So $m < l$ and is odd, thus we have $(k,l,m) = (1,4,3)$ or $(3,4,1)$ and $\alpha_1 = (1+\sqrt{5})/2$. By (2.12) we see that

$$\frac{\lambda_1}{\lambda_2} = \frac{\alpha_1^l+1}{\alpha_2^l+1} = \alpha_1^l = \left(\frac{1+\sqrt{5}}{2}\right)^4$$

which gives $\lambda_1 = \pm(3-\sqrt{5})/2$. These values for α_1 and λ_1 yield the recurrence sequence as stated. □

2.2 Algebraic binary recurrence sequences

The purpose of this section is to study certain algebraic binary recurrences. It will be necessary to introduce a different height function than was defined in §1.2. For $\alpha \in \overline{\mathbb{Q}}$ let $a_n z^n + \cdots + a_0$ be the unique irreducible polynomial in $\mathbb{Z}[z]$ for which α is a root such that $\gcd(a_0,\ldots,a_n) = 1$. Then the *usual height* of α, denoted $H_0(\alpha)$ is given by

$$H_0(\alpha) = \max\{|a_0|,\ldots,|a_n|\}.$$

Throughout this section and only in this section whenever we talk of the height of an algebraic number we will mean the usual height. Note that $H_0(\alpha) = H_0(1/\alpha)$. It can be shown, see for example Chapter 1 of Shorey and Tijdeman [20], that if α and β are algebraic numbers of degree at most d then there exists a constant $c(d)$ depending only on d such that

$$\log H_0(\alpha\beta) \leq c(d) \max\{\log H_0(\alpha), \log H_0(\beta)\} \tag{2.17}$$

If K is a number field of degree d and $\sigma_1, \ldots, \sigma_d$ denote the embeddings $K \hookrightarrow \mathbb{C}$ then for $\alpha \in K$ we set

$$\boxed{\alpha} = \max\{|\sigma_1(\alpha)|, \ldots, |\sigma_d(\alpha)|\}.$$

It is not hard to show that if α is an algebraic number of degree d then we have

$$\boxed{\alpha} \leq dH_0(\alpha).$$

Furthermore if α is an algebraic integer then it can be shown that

$$H_0(\alpha) \leq (2\boxed{\alpha})^d. \tag{2.18}$$

Let K be a number field of degree d and $\{u_n\}_{n\geq 0} \subset \mathcal{O}_K$ be a non-degenerate binary recurrence sequence with companion polynomial $f(z) \in \mathbb{Z}[z]$. Note that we are again indexing our recurrence with $n \geq 0$ as opposed to $\mathbb{Z}$. We let α and β be the roots of $f(z)$ and for $\omega \in K$ we let $u(\omega)$ denote the ω-multiplicity of $\{u_n\}_{n\geq 0}$. We know that the $u(\omega)$ is finite for every $\omega \in K$. A natural question to ask is for what sequences $\{u_n\}_{n\geq 0}$ and values $\omega \in K$ do we have $|u(\omega)|$ small? We will prove a theorem, due to Brindza, Pinter and Schmidt, which establish criteria that implies $u(\omega) \leq 1$. We follow the methods in [5].

Theorem 2.3. *Say $\omega \in K^\times$. There exists an effectively computable constant $c(d, f, w)$ such that if $\min\{|\alpha|, |\beta|\} > 1$ and $\max\{H_0(u_0), H_0(u_1)\} > c(d, f, \omega)$ then $u(\omega) \leq 1$.*

Before proceeding with the proof of Theorem 2.3 we will need a few Lemmas.

Lemma 2.9. *Let $\alpha_1, \ldots, \alpha_n$ be non-zero algebraic numbers with splitting field L of degree g. Let $A_1, \ldots, A_n$ denote upper bounds for the respective heights of $\alpha_1, \ldots, \alpha_n$, such that $A_i \geq 2$ for each $1 \leq i \leq n$. Set*

$$\Omega' = \prod_{i=1}^{n-1} \log A_i \qquad \text{and} \qquad \Omega = \Omega' \log A_n.$$

Let $b_1, \ldots, b_n$ be rational integers and set $B = \max\{|b_1|, \ldots, |b_n|, 2\}$. If

$$\Lambda = \left|\alpha_1^{b_1} \cdots \alpha_n^{b_n} - 1\right| \neq 0,$$

then

$$\Lambda > \exp(-c(n,g)\Omega \log \Omega' \log B),$$

where $c(n,g)$ is an effectively computable constant depending only on g and n.

Proof. See [19]. □

As in the previous section it is easily shown that for all $n \geq 0$

$$(\beta - \alpha)u_n = \lambda\alpha^n + \mu\beta^n,$$

where $\lambda = u_0\beta - u_1$ and $\mu = u_1 - u_0\alpha$. Thus it suffices to consider the equation

$$\lambda\alpha^n + \mu\beta^n = \gamma, \tag{2.19}$$

where $\gamma = (\beta - \alpha)\omega$.

Lemma 2.10. *Suppose $\alpha, \beta, \lambda, \mu \in K$, with $|\alpha|, |\beta| > 1$, α/β not a root of unity and $\lambda\mu \neq 0$. There is an effectively computable constant $c_0 = c_0(d, \alpha, \beta)$ such that there is at most one integer $n \geq 0$ with*

$$0 < |\lambda\alpha^n + \mu\beta^n| < \max\{|\lambda|, |\mu|\} (2 + \log H_0(\lambda/\mu))^{-c_0}. \tag{2.20}$$

Proof. $c_1, c_2, \ldots$ will be effectively computable constants depending on α, β and d. We may suppose that $|\lambda| \leq |\mu|$ and we set $h = 2 + \log H_0(\lambda/\mu)$. Now (2.20) may be rewritten as

$$0 < \left|(-\lambda/\mu)^1(\alpha/\beta)^n - 1\right| < |\beta|^{-n} h^{-c_0} < |\beta|^{-n}. \tag{2.21}$$

If $n \geq 2$ then we can apply Lemma 2.9 with $\Omega' = \log H(\alpha/\beta)$, $\Omega = \Omega' \log H(\lambda/\mu)$, and $B = n$ to get

$$\left|(-\lambda/\mu)^1(\alpha/\beta)^n - 1\right| > \exp(-c_1 \log H(\lambda/\mu) \log n) > \exp(-c_1 h \log n).$$

Comparison with (2.21) and taking logarithms yields $-c_1 h \log n < -n \log |\beta|$, thus

$$n < c_2 h \log n < c_2 h \log(c_2 h \log n) < c_3 h \log h. \tag{2.22}$$

If $n < 2$ then (2.22) will still hold by ensuring $c_3 \geq 1$.

Let $0 \leq n_1 < n_2$ be two solutions to (2.20), hence to (2.21). When $c_0 \geq 2$ we have $h^{-c_0} \leq 1/4$ and then, since $|\beta|^{-n_1} \leq 1$, (2.21) yields

$$-1/4 \leq (-\lambda/\mu)(\alpha/\beta)^{n_1} - 1 \leq 1/4$$
$$4/5 \leq (-\mu/\lambda)(\beta/\alpha)^{n_1} \leq 4/3.$$

And so

$$\begin{aligned}\left|\left(\frac{\alpha}{\beta}\right)^{n_2-n_1}-1\right| &= \left|\frac{\mu}{\lambda}\left(\frac{\alpha}{\beta}\right)^{-n_1}\right|\left|\left(\left(-\frac{\lambda}{\mu}\right)\left(\frac{\alpha}{\beta}\right)^{n_2}-1\right)-\left(\left(-\frac{\lambda}{\mu}\right)\left(\frac{\alpha}{\beta}\right)^{n_1}-1\right)\right| \\ &< \frac{4}{3}(|\beta|^{-n_2}+|\beta|^{-n_1})h^{-c_0} \qquad (2.23)\\ &< 4h^{-c_0}.\end{aligned}$$

Since α/β is not a root of unity the left hand side of (2.23) is not zero. Hence we can apply Lemma 2.9 with $B = \max\{n_2 - n_1, 2\}$ and we see that the left hand side of (2.23) is

$$> \exp(-c_4 \log B). \qquad (2.24)$$

If $n_2 - n_1 = 1$ then combining (2.23) and (2.24) yields $h^{c_0} < 2^{c_4+2}$, hence $2^{c_0} < 2^{c_4+2}$, which is impossible if $c_0 \geq c_4 + 2$. If $n_2 - n_1 > 1$ then (2.22) gives

$$c_4 \log(n_2 - n_1) \leq c_4 \log(n_2) < c_4 \log(c_3 h \log h) < c_5 \log h,$$

hence (2.24) is bounded below by h^{-c_5}. Comparison with (2.23) yields $h^{c_0-c_5} < 4$, hence $2^{c_0-c_5} < 4$, which is impossible if $c_0 \geq c_5 + 2$. Then taking $c_0 = \max\{c_4, c_5\} + 2$ establishes the Lemma. □

Lemma 2.11. *Let $\gamma \in K^\times$ and $\lambda, \mu \in \mathcal{O}_K$. Let $\sigma_1, \ldots, \sigma_d$ denote the distinct embeddings of K into $\mathbb{C}$. Suppose*

$$\min_{1\leq i\leq d}\{\min\{|\sigma_i(\alpha)|, |\sigma_i(\beta)|\}\} > 1 \qquad (2.25)$$

and

$$\max\{\lceil\lambda\rceil, \lceil\mu\rceil\} > c_6(d, \alpha, \beta, \gamma), \qquad (2.26)$$

where $c_6(d, \alpha, \beta, \gamma)$ is an effectively computable constant depending only on α, β, γ and d. Then (2.19) has at most one solution $n \geq 0$.

Proof. Set $m = \max\{\lceil\lambda\rceil, \lceil\mu\rceil\}$. We know that there exists a constant $c_7(d)$, depending only on d, such that

$$\begin{aligned}\log H_0(\lambda/\mu) &\leq c_7(d)\max\{\log H_0(\lambda), \log H_0(\mu)\} \\ &\leq dc_7(d)\max\{\log(2\lceil\lambda\rceil), \log(2\lceil\mu\rceil)\} \qquad (2.27)\\ &= c_8(d)\log m.\end{aligned}$$

Take $c_6(d, \alpha, \beta, \gamma)$ to be such that $m > c_6$ implies

$$\frac{m}{(2 + c_8(d) \log m)^{c_0}} > \boxed{\gamma}. \tag{2.28}$$

We may suppose that $\boxed{\lambda} \leq \boxed{\mu}$. Moreover, by applying an appropriate embedding, we may assume that $\boxed{\mu} = |\mu|$, so that $m = \max\{|\lambda|, |\mu|\}$. Then (2.19) combined with (2.27) and (2.28) yield

$$|\lambda\alpha^n + \mu\beta^n| = |\gamma| \leq \boxed{\gamma} < \frac{m}{(2 + c_8(d) \log m)^{c_0}} \leq \frac{\max\{|\lambda|, |\mu|\}}{(2 + \log H_0(\lambda/\mu))^{c_0}}.$$

The result then follows from Lemma 2.10. □

We are now in a position in which we can complete the proof of Theorem 2.3.

Proof. Since α and β are the roots of $f(z) \in \mathbb{Z}[z]$ they are either rational integers or conjugate quadratic integers, hence our assumption $\min\{|\alpha|, |\beta|\} > 1$ establishes (2.25). Now

$$u_0 = \frac{\lambda + \mu}{\alpha - \beta} \quad \text{and} \quad u_1 = \frac{\lambda\alpha + \mu\beta}{\alpha - \beta}.$$

Since $\lambda, \mu \in \mathcal{O}_K$ we get

$$\begin{aligned} H_0(u_0) &\leq \max\{H_0(\alpha - \beta), H_0(\lambda + \mu)\}^{c_9(d)} \\ &\leq c_{10}(d, \alpha, \beta) H_0(\lambda + \mu)^{c_9} \\ &\leq c_{10}(2\boxed{\lambda + \mu})^{dc_9} \\ &\leq c_{11}(d, \alpha, \beta)(\max\{\boxed{\lambda}, \boxed{\mu}\})^{c_{12}(d)}, \end{aligned}$$

where c_9, c_{12} are constants that depend on d only and c_{10}, c_{11} are constants that depend on α, β, d only. Similarly we can show that

$$H_0(u_1) \leq c_{13}(d, \alpha, \beta)(\max\{\boxed{\lambda}, \boxed{\mu}\}^{c_{14}(d)}.$$

And so there exists a constant $c(\alpha, \beta, d, \gamma)$, depending only on α, β, γ and d, such that $\max\{H_0(u_0), H_0(u_1)\} > c(\alpha, \beta, d, \gamma)$ implies (2.26). □

Chapter 3

Ternary Recurrence Sequences

In Chapter 2 we investigated binary recurrence sequences. A natural next step is to look at ternary recurrence sequences. In this chapter we investigate the zero-multiplicity of nondegenerate rational ternary recurrence sequences. In 1957 Ward [22] conjectured that the zero multiplicity is at most five. However Berstel [1] constructed a counterexample given by

$$u_{n+3} = 2u_{n+2} - 4u_{n+1} + 4u_n,$$

with $u_0 = u_1 = 0$ and $u_2 = 1$, which has $u_0 = u_1 = u_4 = u_6 = u_{13} = u_{52} = 0$. It is generally expected that this is the only exception to Ward's conjecture. In this chapter we prove a result of Beukers [3], building on work of Beukers and Tijdeman [4], that every nondegenerate rational ternary recurrence sequence has zero-multiplicity at most six. We follow their methods except that in [3] it is assumed that the companion polynomial has three distinct roots and so we add Lemma 3.13 to include the nonsimple case.

3.1 Hypergeometric Polynomials

We first need to develop some lemmas concerning hypergeometric polynomials. In this section we follow [4].

For $a, b, c \in \mathbb{Z}$ we define the *hypergeometric function*, denoted $F(a, b, c, z)$, by

$$F(a, b, c, z) = 1 + \sum_{j=1}^{\infty} \frac{a \cdots (a + j - 1) b \cdots (b + j - 1)}{c \cdots (c + j - 1) j!} z^j.$$

Lemma 3.1. *Fix a positive integer c. For any positive integers a, b with $a, b < c$ we have*

$$\binom{a+b}{b} F(-a, -b-c, -a-b, z) - \binom{a+b}{b}(1-z)^c F(c-a, -b, -a-b, z)$$
$$= (-1)^a \binom{c+b}{c-a-1} z^{a+b+1} F(b+1, a-c+1, a+b+2, z).$$

Proof. Note that $F(-a, -b-c, -a-b, z)$, $(1-z)^c F(c-a, -b, -a-b, z)$ and $z^{a+b+1}F(b+1, a-c+1, a+b+2, z)$ are polynomials and they each satisfy the differential equation

$$z(z-1)\frac{\mathrm{d}^2}{\mathrm{d}z^2} f + ((1-a-b-c)z + a + b)\frac{\mathrm{d}}{\mathrm{d}z} f + a(b+c)f = 0.$$

Hence there is a linear relationship between them. The coefficients of this linear relationship can be found by considering the constant term and the coefficient of the highest power of z. □

Lemma 3.2. *For a, b, c as in* Lemma 3.1*, define*

$$f_{ab} = \binom{a+b}{b} F(-a, -b-c, -a-b, z) \tag{3.1}$$

$$g_{ab} = \binom{a+b}{b} F(c-a, -b, -a-b, z) \tag{3.2}$$

$$h_{ab} = \binom{c+b}{c-a-1} F(b+1, a-c+1, a+b+2, z). \tag{3.3}$$

Then f_{ab}, g_{ab} and h_{ab} are polynomials in $\mathbb{Z}[z]$ of degree a, b and $c-a-1$ respectively.

Proof. We have

$$\begin{aligned} f_{ab}(z) &= \binom{a+b}{b} F(-a, -b-c, -a-b, z) \\ &= \binom{a+b}{b} + \sum_{j=1}^{\infty} \binom{a+b}{b} \frac{(-a)\cdots(-a+j-1)(-b-c)\cdots(-b-c+j-1)}{(-a-b)\cdots(-a-b+j-1)j!} z^j \\ &= \sum_{j=0}^{a} \frac{(a+b)!}{a!b!} \frac{a!}{j!(a-j)!} \frac{(b+c)!}{(b+c-j)!} \frac{(a+b-j)!}{(a+b)!} (-z)^j \\ &= \sum_{j=0}^{a} \binom{a+b-j}{b} \binom{b+c}{j} (-z)^j, \end{aligned}$$

which establishes the result for f_{ab}. In an analogous way we obtain

$$g_{ab}(z) = \sum_{j=0}^{b} \binom{a+b-j}{a} \binom{c-a+j-1}{j} z^j$$

and

$$h_{ab}(z) = \sum_{j=0}^{c-a-1} \binom{b+j}{j} \binom{c+b}{a+b+j+1} (-z)^j.$$

□

Lemma 3.3. *Let f_{ab}, g_{ab}, h_{ab} be as in* Lemma 3.2. *Then*

$$f_{ab}(z) = \frac{(c+b)!}{(c-a-1)!a!b!} \int_0^1 (1-x)^b x^{c-a-1} (1-x-z)^a \mathrm{d}x, \tag{3.4}$$

$$g_{ab}(z) = \frac{(c+b)!}{(c-a-1)!a!b!} \int_0^1 (1-x)^a x^{c-a-1} (1-x+zx)^b \mathrm{d}x, \tag{3.5}$$

$$h_{ab}(z) = \frac{(c+b)!}{(c-a-1)!a!b!} \int_0^1 (1-x)^a x^b (1-zx)^{c-a-1} \mathrm{d}x. \tag{3.6}$$

Proof. These can be checked by writing down the binomial expansion of $(1-x-z)^a$, $(1-x+zx)^b$ and $(1-zx)^{c-a-1}$ and then performing the integration directly where we use the identity

$$\int_0^1 (1-x)^m x^n \mathrm{d}x = \frac{n!m!}{(n+m+1)!},$$

for any positive integers n, m. □

Lemma 3.4. *For f_{ab}, g_{ab}, h_{ab} as in* Lemma 3.2 *and any $x \neq 0$ we have*

$$f_{ab}(x) g_{a,b-1}(x) - f_{a,b-1}(x) g_{ab}(x) \neq 0.$$

Proof. By Lemma 3.1 and 3.2,

$$f_{ab}(z) - (1-z)^c g_{ab}(z) = (-1)^a z^{a+b+1} h_{ab}(z)$$

and

$$f_{a,b-1}(z) - (1-z)^c g_{a,b-1}(z) = (-1)^a z^{a+b} h_{a,b-1}(z).$$

Upon eliminating $(1-z)^c$ from the above two equations we have that

$$f_{ab}(z) g_{a,b-1}(z) - f_{a,b-1}(z) g_{ab}(z) = z^{a+b} p(z) \tag{3.7}$$

for some polynomial $p(z)$. But the left hand side of (3.7) is a polynomial of degree $a+b$ with a non-zero leading coefficient a_0, so we must have

$$f_{ab}(z)g_{a,b-1}(z) - f_{a,b-1}(z)g_{ab}(z) = a_0 z^{a+b},$$

from which our Lemma follows. □

Lemma 3.5. *For positive integer n,*

$$\frac{(3n)!}{(n-1)!n!n!} < \frac{7}{25}27^n.$$

Proof. This is obvious if $n = 1$. If $n \geq 2$ we have

$$\begin{aligned}
\frac{(3n)!}{(n-1)!n!n!} &= 6\prod_{j=2}^{n} \frac{3j(3j-1)(3j-2)}{(j-1)j^2} \\
&= 6(27)^{n-1}\prod_{j=2}^{n}\left(1 + \frac{2/9}{j(j-1)}\right) \\
&< 6(27)^{n-1}\exp\left(\sum_{j=2}^{n}\frac{2}{9}\frac{1}{j(j-1)}\right) \\
&< 6(27)^{n-1}\exp(2/9) \\
&< (7/25)(27)^n.
\end{aligned}$$

□

For a number field K denote by M_K the set of places of K. For $v \in M_K$ we recall the definition of $|\ |_v$ and $r(v)$ given in §1.2.

Lemma 3.6. *Take a positive integer a and let γ, η be non-zero algebraic numbers in some number field K. There exist polynomials $P(z), Q(z), R(z) \in \mathbb{Z}[z]$ of degree at most a such that*

$$P(z) - (1-z)^{2a}Q(z) = z^{2a}R(z), \tag{3.8}$$

$$P(\gamma) - \eta Q(\gamma) \neq 0 \tag{3.9}$$

and

$$\max\{|P(\xi)|_v, |Q(\xi)|_v, |R(\xi)|_v\} \leq (6\sqrt{3})^{a\frac{\log r(v)}{\log 2}}\max\{1, |\xi|_v^a\} \tag{3.10}$$

for any $\xi \in K$ and $v \in M_K$.

Proof. We define the polynomials f_{aa}, g_{aa}, h_{aa} as in the previous Lemmas with $c = 2a$. If $f_{aa}(\gamma) - \eta g_{aa}(\gamma) \neq 0$ then set $P(z) = f_{aa}(z), Q(z) = g_{aa}(z)$ and $R(z) = (-1)^a z h_{aa}(z)$. Then (3.9) is automatically satisfied and we know that (3.8) is satisfied by Lemma 3.1. If $f_{aa}(\gamma) - \eta g_{aa}(\gamma) = 0$ then by Lemma 3.4 we must have $f_{a,a-1}(\gamma) - \eta g_{a,a-1}(\gamma) \neq 0$. In this case we set $P(z) = f_{a,a-1}(z), Q(z) = g_{a,a-1}(z)$ and $R(z) = (-1)^a h_{a,a-1}(z)$. Again (3.9) is automatically satisfied and (3.8) follows from Lemma 3.1.

It remains to show (3.10). First note that if $v \in M_K$ is finite then

$$|P(\xi)|_v \leq \max\{1, |\xi|_v^a\}$$

for any $\xi \in K$, since $P(z) \in \mathbb{Z}[x]$ and $\deg P(z) \leq a$, and similarly for $Q(z)$ and $R(z)$. Thus (3.10) holds for v finite. Assume v is infinite. If $b = a - 1$ or $b = a$ then, since $g_{ab}(z)$ has positive coefficients and f_{ab}, h_{ab} have alternating coefficients, we have

$$\begin{aligned} |f_{ab}(x)| &\leq f_{ab}(-1) \max\{1, |x|^a\}, \\ |g_{ab}(x)| &\leq g_{ab}(1) \max\{1, |x|^b\}, \\ |h_{ab}(x)| &\leq h_{ab}(-1) \max\{1, |x|^{2a-b-1}\}, \end{aligned}$$

for any $x \in \mathbb{C}$, where $|\ |$ is the usual absolute value on $\mathbb{C}$. Then is suffices to show that

$$f_{ab}(-1), g_{ab}(1), h_{ab}(-1) < (6\sqrt{3})^a.$$

Consider $f_{aa}(-1)$. By Lemma 3.3 we have

$$f_{aa}(-1) = \frac{(3a)!}{(a-1)!a!a!} \int_0^1 (1-x)^a x^{a-1} (2-x)^a \mathrm{d}x.$$

For $0 \leq x \leq 1$ we have $|x(1-x)(2-x)| \leq 2/(3\sqrt{3})$. This together with Lemma 3.5 yields

$$f_{aa}(-1) < \frac{7}{25}(27)^a \left(\frac{2}{3\sqrt{3}}\right)^{a-1} \int_0^1 (1-x)(2-x)\mathrm{d}x < (6\sqrt{3})^a.$$

The verifications for $f_{a,a-1}(-1), g_{aa}(1), g_{a,a-1}(1), h_{aa}(-1)$ and $h_{a,a-1}(-1)$ are similar. □

3.2 The equation $\lambda\alpha^n + \mu\beta^n = 1$

Let K be a number field and let $\alpha, \beta, \lambda, \mu \in K$ be non-zero. We are interested in solutions to the equation

$$\lambda\alpha^x + \mu\beta^x = 1, \tag{3.11}$$

in $x \in \mathbb{Z}$. The hypergeometric polynomials will be used in Lemma 3.7 to bound the larger solutions of (3.11) while Lemmas 3.8 to 3.10 will create gaps between consecutive solutions. We will suppose throughout this section that (3.11) has solutions $x = 0, k, l, m$ with $0 < k < l < m$. We will also assume throughout this section that none of $\alpha, \beta, \alpha/\beta$ is a root of unity. For an algebraic number γ recall the definition of the absolute height of γ, denoted $H(\gamma)$, given in §1.2. In the proof of the following Lemma we follow [4].

Lemma 3.7. *Suppose that $m \geq 10l$. Let $H = \max\{H(\alpha), H(\beta), H(\alpha/\beta)\}$ and suppose $H > 1$. Then*

$$l \leq 27\frac{\log 2}{\log H} + \frac{50}{3}k.$$

Proof. First note that if $H = H(\alpha/\beta)$ then instead of (3.11) we may consider

$$(-\lambda/\mu)(\alpha/\beta)^x + (-1/\mu)(1/\beta)^x = 1.$$

Hence, without loss of generality, we may assume $H = H(\alpha)$.

Take $q \in \mathbb{Z}$, $q > 0$, and $\delta \in \mathbb{R}$ with $0 \leq \delta < 2$ so that $m = 2lq + \delta l$. By Lemma 3.6 we have polynomials $P(z), Q(z), R(z) \in \mathbb{Z}[z]$ of degree at most q with

$$P(\lambda\alpha^l) - (\mu\beta^l)^{2q}Q(\lambda\alpha^l) = (\lambda\alpha^l)^{2q}R(\lambda\alpha^l). \tag{3.12}$$

Now define Δ by

$$\Delta = P(\lambda\alpha^l) - \mu^{2q-1}\beta^{-\delta l}Q(\lambda\alpha^l). \tag{3.13}$$

Then using (3.12) together with the facts that $m = 2lq + \delta l$ and $\mu\beta^m = 1 - \lambda\alpha^m$, we have

$$\Delta = (\lambda\alpha^l)^{2q}\left(R(\lambda\alpha^l) - \left(\frac{\mu}{\lambda}\right)^{2q-1}\left(\frac{\alpha}{\beta}\right)^{\delta l}Q(\lambda\alpha^l)\right). \tag{3.14}$$

Take $v \in M_K$. If $\left|\lambda\alpha^l\right|_v < 1$ then by (3.14) we have

$$\begin{aligned}
|\Delta|_v &\leq \left|\lambda\alpha^l\right|_v^{2q} r(v)(6\sqrt{3})^{q\frac{\log r(v)}{\log 2}} \max\left\{1, \left|\frac{\mu}{\lambda}\right|_v^{2q-1+\delta}\left|\frac{\lambda\alpha^l}{\mu\beta^l}\right|_v^{\delta}\left|\lambda\alpha^l\right|^q\right\} \\
&\leq \left|\lambda\alpha^l\right|_v^{2q} r(v)(6\sqrt{3})^{q\frac{\log r(v)}{\log 2}} \max\left\{1, \left|\frac{1-\lambda}{\lambda}\right|_v^{2q-1+\delta}\right\}\max\left\{1, \frac{1}{|\mu\beta^l|_v^{\delta}}\right\} \qquad (3.15) \\
&\leq \left|\lambda\alpha^l\right|_v^{2q} r(v)^{2q+\delta}(6\sqrt{3})^{q\frac{\log r(v)}{\log 2}} \max\left\{1, \frac{1}{|\lambda|_v^{2q-1+\delta}}\right\}\max\left\{1, \frac{1}{|\mu\beta^l|_v^{\delta}}\right\}.
\end{aligned}$$

If $\left|\lambda\alpha^l\right|_v \geq 1$ then by (3.13) we have

$$\begin{aligned}|\Delta|_v &\leq r(v)(6\sqrt{3})^{q\frac{\log r(v)}{\log 2}} \left|\lambda\alpha^l\right|_v^q \max\{1, |\mu|_v^{2q-1+\delta} \left|\mu\beta^l\right|_v^{-\delta}\} \\ &\leq r(v)^{2q+\delta}(6\sqrt{3})^{q\frac{\log r(v)}{\log 2}} \left|\lambda\alpha^l\right|_v^q \max\{1, |\lambda|_v^{2q-1+\delta}\} \max\left\{1, \frac{1}{|\mu\beta^l|_v^{\delta}}\right\}. \end{aligned} \tag{3.16}$$

Since $\prod_{v\in M_K} |\Delta|_v = 1$ and $\prod_{v\in M_K} r(v) = 2$, (3.15) and (3.16) yield

$$1 \leq \frac{2^{2q+\delta}}{H(\lambda\alpha^l)^q}(6\sqrt{3})^q H(\lambda)^{2(2q-1+\delta)} H(\mu\beta^l)^{\delta}.$$

Now $H(\mu\beta^l) = H(1-\lambda\alpha^l) \leq 2H(1)H(\lambda\alpha^l) = 2H(\lambda\alpha^l)$ and so

$$1 \leq \frac{4^{q+\delta}}{H(\lambda\alpha^l)^q}(6\sqrt{3})^q H(\lambda)^{2(2q-1+\delta)} H(\lambda\alpha^l)^{\delta}.$$

Using $H(\lambda\alpha^l) \geq H(\alpha^l)/H(\lambda)$ we have

$$H(\alpha^l)^{q-\delta} \leq 4^{q+\delta}(6\sqrt{3})^q H(\lambda)^{5q-2+\delta}. \tag{3.17}$$

From $\lambda+\mu = 1$ and $\lambda\alpha^k + \mu\beta^k = 1$ it follows that $\lambda = (\beta^k - 1)/(\beta^k - \alpha^k)$, hence

$$H(\lambda) = H\left(\frac{1-\beta^{-k}}{1-(\alpha/\beta)^k}\right) \leq H(1-\beta^{-k})H(1-(\alpha/\beta)^k) \leq 4H(\alpha)^{2k}.$$

Substituting this into (3.17) yields

$$H(\alpha^l)^{q-\delta} \leq 4^{6q-2+2\delta}(6\sqrt{3})^q H(\alpha)^{2(5q-2+\delta)k}.$$

Then, since $0 \leq \delta < 2$ and $m \geq 10l$ implies $q \geq 5$, we obtain

$$H(\alpha)^l \leq 4^{32/3}(6\sqrt{3})^{5/3} H(\alpha)^{50k/3} \leq 2^{27} H(\alpha)^{50k/3},$$

from which our Lemma follows. □

For the rest of this chapter we will follow [3] with the exception of Lemma 3.13. The next series of Lemmas establish criteria in order to create large gaps between the solutions of (3.11).

Lemma 3.8. *Suppose there exists finite $v \in M_K$ such that $|\alpha|_v < 1$ and $|\beta|_v = 1$. Then there is a positive integer d such that*

1. $d > 1$, $d|(m-l)$ *and* $d|(l-k)$.

2. *If there is a solution* $x = n$ *of* (3.11) *with* $0 < n < k$ *then* $d \geq 4$.

3. *If* $|\alpha|_v^k |\beta - 1|_v < |p|_v^{1/(p-1)}$, *where* p *is the rational prime that lies above* v, *then* $|(m-l)/d|_v \leq |\alpha|_v^{l-k}$ *and* $|(l-k)/d|_v = 1$.

Proof. If $\lambda\alpha^x + \mu\beta^x = 1$ then, since $\lambda + \mu = 1$, we have $\beta^x - 1 = \lambda(\lambda-1)^{-1}(\alpha^x - 1)$, hence $\left|\beta^k - 1\right|_v = \left|\beta^l - 1\right|_v = |\beta^m - 1|_v$. We will denote this value by B. Note that since $|\beta|_v = 1$ we have $B \leq |\beta - 1|_v$. After eliminating λ and μ from (3.11) with $x = 0, k, l$ we have

$$\beta^l - \beta^k = (\beta^l - 1)\alpha^k - (\beta^k - 1)\alpha^l.$$

Hence

$$\left|\beta^l - \beta^k\right|_v = |\alpha|_v^k \left|\beta^l - 1\right|_v = |\alpha|_v^k B,$$

and since $|\beta|_v = 1$, we have

$$\left|\beta^{l-k} - 1\right|_v = |\alpha|_v^k B.$$

In the same way we obtain

$$\left|\beta^{m-l} - 1\right|_v = |\alpha|_v^l B < |\alpha|_v^k B.$$

We take d to be the smallest positive integer such that $\left|\beta^d - 1\right| \leq |\alpha|_v^k B$. We must have $d > 1$ since $d = 1$ implies $|\beta - 1| \leq |\alpha|_v^k B < |\beta - 1|_v$, a contradiction. Also if $|\beta^x - 1|_v \leq |\alpha|_v^k B$ then we must have $d|x$, in particular $d|(l-k)$ and $d|(m-l)$. This establishes part 1. We further note that $\left|\beta^{l-k} - 1\right|_v = |\alpha|_v^k B$ implies $\left|\beta^d - 1\right| = |\alpha|_v^k B$.

Suppose we have another solution $x = n$ to (3.11) with $0 < n < k$. Take e to be the smallest positive integer such that $|\beta^e - 1|_v \leq |\alpha|_v^n B$. We have, as above, that $e > 1$ and $|\beta^e - 1|_v = |\alpha|_v^n B$. Now $\left|\beta^d - 1\right|_v = |\alpha|_v^k B < |\alpha|_v^n B$, hence we have $e|d$ and $e \neq d$, so $d \geq 4$.

Put $\gamma = \beta^d - 1$ and assume $|\alpha|_v^k |\beta - 1|_v < |p|_v^{1/(p-1)}$. Note in particular that $|\gamma|_v < |p|_v^{1/(p-1)}$. Let $t = (m-l)/d$, then

$$\beta^{m-l} - 1 = (1+\gamma)^t - 1 = t\gamma + \binom{t}{2}\gamma^2 + \cdots + \gamma^t = t\gamma + t\gamma\left(\binom{t-1}{1}\frac{\gamma}{2} + \cdots + \binom{t-1}{t-1}\frac{\gamma^{t-1}}{t}\right).$$

Now

$$\left|\sum_{j=2}^{t}\binom{t-1}{j-1}\frac{\gamma^{j-1}}{j}\right|_v \leq \max_{j\geq 2}\left|\frac{\gamma^{j-1}}{j}\right|_v \leq \max_{i\geq 1}\left\{|\gamma|_v, \left|\frac{\gamma^{p^i-1}}{p^i}\right|_v\right\} \leq \max_{i\geq 1}\left\{|\gamma|_v, \left|\frac{\gamma^{p-1}}{p}\right|_v^i\right\} < 1,$$

since $|\gamma|_v < |p|_v^{1/(p-1)}$. Then

$$|t\gamma|_v = \left|\beta^{m-l} - 1\right| = |\alpha|_v^l B,$$

hence

$$|t|_v = |\gamma|_v^{-1} |\alpha|_v^l B = |\alpha|_v^{l-k},$$

as asserted. If we had $|(l-k)/d|_v < 1$ then we would have $\left|\beta^{l-k} - 1\right|_v < \left|\beta^d - 1\right|_v$, which is not the case. Hence $|(l-k)/d|_v = 1$. □

Lemma 3.9. *Let $0 \le x_1 < x_2$ be two solutions to $\lambda\alpha^x + \mu\beta^x = 1$, with $\lambda\mu\alpha\beta \neq 0$. Suppose there exists a positive integer d such that $x_1 + d$ and $x_2 + d$ are also solutions. Then α and β are roots of unity.*

Proof. We have $(\alpha^{x_1+d} - \alpha^{x_1})\lambda + (\beta^{x_1+d} - \beta^{x_1})\mu = 0$ and $(\alpha^{x_2+d} - \alpha^{x_2})\lambda + (\beta^{x_2+d} - \beta^{x_2})\mu = 0$. Thus the determinant of the matrix

$$\begin{bmatrix} \alpha^{x_1+d} - \alpha^{x_1} & \beta^{x_1+d} - \beta^{x_1} \\ \alpha^{x_2+d} - \alpha^{x_2} & \beta^{x_2+d} - \beta^{x_2} \end{bmatrix}$$

must vanish. Hence $\beta^{x_1}\alpha^{x_1}(\alpha^d - 1)(\beta^d - 1)((\beta/\alpha)^{x_2-x_1} - 1) = 0$. First assume α is a dth root of unity. Then we have $\lambda\alpha^{x_1} + \mu\beta^{x_1} = \lambda\alpha^{x_1} + \mu\beta^{x_1+d}$, which yields $\mu\beta^{x_1}(\beta^d - 1) = 0$. Similarly if β is a dth root of unity then so is α. If β/α is a $(x_2 - x_1)$th root of unity the we have $1 = \lambda\alpha^{x_2} + \mu\beta^{x_2} = (\lambda\alpha^{x_1} + \mu\beta^{x_1})\beta^{x_2-x_1} = \beta^{x_2-x_1}$. Hence β is a root of unity and then, by above, so is α. □

Note that this Lemma essentially states that a given difference between two solutions of (3.11) can occur at most once. It is worth noting in particular, that if $x_1 < x_2 < \cdots < x_n$ are solutions, then $x_n - x_1 \ge \binom{n}{2}$.

Lemma 3.10. *Assume again that* (3.11) *has solutions $x = 0 < k < l < m$. Further suppose that $\beta = \overline{\alpha}$ and $\mu = \overline{\lambda}$. Then we have the following:*

1. *If $|\alpha| \ge 4/3$, $k > 50$ and $10^{-4} < \arg(\overline{\alpha}/\alpha) < \pi - 10^{-4}$, then $m - k \ge |\alpha|^k$.*
2. *If $|\alpha| \ge 2.1$ and $k \ge 2$, then $m - k > 2\,|\alpha|^k$.*

Proof. Using the equations $\lambda\alpha^x + \overline{\lambda}\overline{\alpha}^x = 1$ with $x = 0, k, l, m$ we eliminate λ and $\overline{\lambda}$ to obtain

$$\frac{\overline{\alpha}^k - 1}{\alpha^k - 1} = \frac{\overline{\alpha}^l - 1}{\alpha^l - 1} = \frac{\overline{\alpha}^m - 1}{\alpha^m - 1}.$$

These quotients cannot equal one since we have assumed that $\overline{\alpha}/\alpha$ is not a root of unity. Let

$$\eta = \frac{\overline{\alpha}^k - 1}{\alpha^k - 1} - 1.$$

Note that $\eta \neq 0$ and $|\eta| \leq 2$. For $x = k, l, m$ we have

$$\frac{\overline{\alpha}^x - 1}{\alpha^x - 1} = \left(\frac{\overline{\alpha}}{\alpha}\right)^x + \frac{\eta}{\alpha^x}.$$

Hence

$$\begin{aligned} \left(\frac{\overline{\alpha}}{\alpha}\right)^{l-k} - 1 &= \eta \left(\frac{\alpha}{\overline{\alpha}}\right)^k \left(\frac{1}{\alpha^k} - \frac{1}{\alpha^l}\right) \\ \left(\frac{\overline{\alpha}}{\alpha}\right)^{m-l} - 1 &= \eta \left(\frac{\alpha}{\overline{\alpha}}\right)^l \left(\frac{1}{\alpha^l} - \frac{1}{\alpha^m}\right). \end{aligned} \tag{3.18}$$

It can be checked that the assumptions made in either of the cases in the statement of the Lemma will ensure the right hand sides of (3.18) are smaller than one in absolute value. If $w \in \mathbb{C}$ satisfies $|1 + w| = 1$ and $|w| \leq 1$ then $|w| \leq |\arg(1 + w)| \leq (\pi/3)\,|w|$. Applying this to the right hand sides of (3.18) we have

$$\begin{aligned} (l-k)\arg(\overline{\alpha}/\alpha) + 2\pi r &= \arg\left(1 + \eta\left(\frac{\alpha}{\overline{\alpha}}\right)^k \left(\frac{1}{\alpha^k} - \frac{1}{\alpha^l}\right)\right) = \theta \left|\frac{1}{\alpha^k} - \frac{1}{\alpha^l}\right| |\eta|\,, \\ (m-l)\arg(\overline{\alpha}/\alpha) + 2\pi s &= \arg\left(1 + \eta\left(\frac{\alpha}{\overline{\alpha}}\right)^l \left(\frac{1}{\alpha^l} - \frac{1}{\alpha^m}\right)\right) = \phi \left|\frac{1}{\alpha^l} - \frac{1}{\alpha^m}\right| |\eta|\,, \end{aligned} \tag{3.19}$$

for some $r, s \in \mathbb{Z}$ and $\theta, \phi \in \mathbb{R}$ with $1 \leq |\theta|\,, |\phi| < \pi/3$. Define E by

$$E = (m-l)\theta \left|\frac{1}{\alpha^k} - \frac{1}{\alpha^l}\right| |\eta| - (l-k)\phi \left|\frac{1}{\alpha^l} - \frac{1}{\alpha^m}\right| |\eta|\,.$$

By (3.19) we must have either $E = 0$ or $|E| \geq 2\pi$. First assume $E = 0$, then since $\eta \neq 0$ we have

$$(m-l)\theta \left|\alpha^{l-k} - 1\right| = (l-k)\phi \left|1 - \alpha^{l-m}\right|.$$

Thus

$$\frac{\left|\alpha^{l-k} - 1\right|}{l-k} = \frac{\left|1 - \alpha^{l-m}\right|}{m-l} \left|\frac{\phi}{\theta}\right|,$$

which yields

$$\frac{|\alpha|^{l-k} - 1}{l-k} \leq \frac{1 + |\alpha|^{l-m}}{m-l} \frac{\pi}{3}. \tag{3.20}$$

Suppose we are in the situation of case 1. Since $|\alpha| \geq 4/3$ and $k > 50$ we see that the right hand sides of (3.19) are less than 10^{-5}. Since $10^{-4} < \arg \overline{\alpha}/\alpha < \pi - 10^{-4}$ then (3.19) implies $\min\{l-k, m-l\} \geq 3$. Also by Lemma 3.9 we cannot have $m-l = l-k = 3$. If either $l-k \geq 3$ and $m-l \geq 4$ or $l-k \geq 4$ and $m-l \geq 3$ then (3.20) cannot hold. If we are in the situation of case 2 then by Lemma 3.9 we cannot have $l-k = m-l$. With either $l-k \geq 1$ and $m-l \geq 2$ or $l-k \geq 2$ and $m-l \geq 1$, (3.20) cannot hold since $|\alpha| \geq 2.1$. We conclude that $E \neq 0$.

Since $E \neq 0$ we have

$$\begin{aligned} 2\pi &\leq (m-l)\frac{\pi}{3}\left|\frac{1}{\alpha^k} - \frac{1}{\alpha^l}\right||\eta| + (l-k)\frac{\pi}{3}\left|\frac{1}{\alpha^l} - \frac{1}{\alpha^m}\right||\eta| \\ &\leq (m-k)\frac{2\pi}{3}(1+|\alpha|^{-1})\,|\alpha|^{-k}. \end{aligned}$$

Thus $m-k \geq 3(1+|\alpha|^{-1})^{-1}\,|\alpha|^k$, from which our Lemma follows. □

Lemma 3.11. *Let $\alpha \in \overline{\mathbb{Q}}$ be such that $|\alpha| \geq 4$ and $H(\alpha) \geq 2^{1/3}$. Then for $\lambda \in \mathbb{C}$ the equation*

$$\lambda\alpha^x + \overline{\lambda}\overline{\alpha}^x = 1$$

has at most six solutions $x \in \mathbb{Z}$.

Proof. Suppose the equation has seven solutions, which we may assume to be $0 < x_1 < x_2 < x_3 < x_4 < x_5 < x_6$. By Lemma 3.10 we have $x_6 - x_4 > 2\,|\alpha|^{x_4}$. By Lemma 3.9, $x_4 \geq 10$, so $x_6 > 2\,|\alpha|^{x_4} + x_4$ implies $x_6 \geq 10x_4$. Thus we can apply Lemma 3.7 to get

$$x_4 < 27\frac{\log 2}{\log 2^{1/3}} + \frac{50}{3}x_1 = 81 + \frac{50}{3}x_1.$$

Appealing to case 2 of Lemma 3.10 we find $x_4 \geq x_2 + 2\,|\alpha|^{x_2}$, which yields

$$x_2 + 2\,|\alpha|^{x_2} < 81 + \frac{50}{3}x_1.$$

This implies $x_1 + 2 \cdot 4^{x_1+1} < 80 + (50/3)x_1$, hence $x_1 = 1$. But then we have $x_2 \geq 3$, thus $3 + 2 \cdot 4^3 < 81 + 50/3$. This is a contradiction and our result follows. □

Lemma 3.12. *Let λ, μ, α and β be non-zero algebraic numbers in a number field K such that $\max\{H(\alpha), H(\beta), H(\alpha/\beta)\} \geq 2^{1/6}$. Let $v \in M_K$ be a finite place such that $|\alpha|_v < 1$ and $|\beta|_v = 1$. Let p be the rational prime above v and say v has ramification index at most 2. Then* (3.11) *has at most six solutions.*

Proof. Suppose that (3.11) has seven solutions, which we may assume to be $0 < x_1 < x_2 < x_3 < x_4 < x_5 < x_6$. Lemma 3.9 implies $x_2 \geq 3$ and since v has ramification index at most two we have $|\alpha|_v^{x_2} \leq |\alpha|_v^3 < |p|_v \leq |p|_v^{1/(p-1)}$. Then by applying Lemma 3.8 we obtain

$$\left|\frac{x_4 - x_3}{d}\right|_v \leq |\alpha|_v^{x_3 - x_2},$$

for some $d \geq 4$. Since v has ramification index ≤ 2 we then have

$$x_4 - x_3 \geq d \cdot p^{(x_3-x_2)/2} \geq 4 \cdot 2^{(x_3-x_2)/2}. \tag{3.21}$$

Similarly,

$$x_5 - x_4 \geq 4 \cdot 2^{(x_4-x_3)/2} \quad \text{and} \quad x_6 - x_5 \geq 4 \cdot 2^{(x_5-x_4)/2}. \tag{3.22}$$

By Lemma 3.8 we also know that $d|(x_3 - x_2)$, hence $x_3 - x_2 \geq 4$. Again applying Lemma 3.8, but this time with $k = x_2, l = x_5, m = x_6$, we see that

$$x_6 - x_2 = x_6 - x_5 + x_5 - x_2 \geq 4 \cdot 2^{(x_5-x_2)/2} + x_5 - x_2 \geq 10(x_5 - x_2),$$

since $x_5 - x_2 \geq \binom{4}{2} = 10$. Then applying Lemma 3.7 with $H \geq 2^{1/6}$ to the equation $(\lambda\alpha^{-x_2})\alpha^x + (\mu\beta^{-x_2})\beta^x = 1$ yields

$$x_5 - x_2 \leq 27\frac{\log 2}{\log 2^{1/6}} + \frac{50}{3}(x_3 - x_2) = 162 + \frac{50}{3}(x_3 - x_2). \tag{3.23}$$

Combining (3.21) and (3.22) we have

$$x_5 - x_2 > x_5 - x_4 \geq 4 \cdot 2^{(x_4-x_3)/2} \geq 4 \cdot 2^{2\cdot 2\cdot (x_3-x_2)/2} = 4^{1+x_3-x_2}.$$

But, since $x_3 - x_2 \geq 4$, this violates (3.23). □

3.3 Rational ternary recurrence sequences

We now consider the zero-multiplicity of non-degenerate rational recurrence sequences of order three. We know by §1.1 that this will be finite and we will show that it is at most six, which is best possible. The case when our recurrence is not simple is dispensed with easily.

Lemma 3.13. *If $\{u_n\}_{n\in\mathbb{Z}}$ is a non-degenerate rational ternary recurrence sequence with zero-multiplicity greater than four then $\{u_n\}_{n\in\mathbb{Z}}$ is simple.*

Proof. Let $\mathcal{P}(z) = z^3 - c_1 z^2 - c_2 z - c_3$ be the companion polynomial to the recurrence sequence $\{u_n\}_{n\in\mathbb{Z}}$. If $\mathcal{P}(z)$ has only one distinct root, say α, then there is a degree two polynomial $P(z) \in \mathbb{C}[z]$ such that

$$u_n = P(n)\alpha^n.$$

Thus $u_n = 0$ implies $P(n) = 0$ and so $\{u_n\}_{n\in\mathbb{Z}}$ has zero multiplicity at most two. Say $\mathcal{P}(z)$ has two distinct roots, say α_1 and α_2. Then there is a degree one polynomial $P(z) = a_1 z + a_2 \in \mathbb{C}[z]$ and a number $a_3 \in \mathbb{C}^\times$ such that

$$u_n = P(n)\alpha_1^n + a_3\alpha_2^n.$$

Since $\mathcal{P}(z) \in \mathbb{Q}[z]$ has a double root, α_1, we must have $\alpha_1 \in \mathbb{Q}$ and hence $\alpha_2 \in \mathbb{Q}$. It is then clear that $P(z) \in \mathbb{R}[z]$ and $a_3 \in \mathbb{R}$. For any $a, b, c \in \mathbb{R}$, with $a \neq 0$ and $c > 0$ the equation

$$(ax + b)c^x - 1$$

in $x \in \mathbb{R}$ has at most one max/min, at $x = -\frac{1}{\log c} - \frac{b}{a}$. Hence it is zero at most twice. We are interested in the equation

$$\left(-\frac{a_1}{a_3}x - \frac{a_2}{a_3}\right)\left(\frac{\alpha_1}{\alpha_2}\right)^x = 1. \tag{3.24}$$

If α_1/α_2 is positive then (3.24) can have at most two solutions $x \in \mathbb{Z}$. If α_1/α_2 is negative then we split (3.24) into the two equations

$$\left(-2\frac{a_1}{a_3}x - \frac{a_2}{a_3}\right)\left(\frac{\alpha_1^2}{\alpha_2^2}\right)^x = 1$$

and

$$\left(-2\frac{a_1\alpha_1}{a_3\alpha_2}x - \left(\frac{a_1\alpha_1}{a_3\alpha_2} + \frac{a_2\alpha_1}{a_3\alpha_2}\right)\right)\left(\frac{\alpha_1^2}{\alpha_2^2}\right)^x = 1,$$

each of which has at most two solutions $x \in \mathbb{Z}$. Our Lemma follows. □

Henceforth we will assume our recurrence is simple. Let $\{u_n\}_{n\in\mathbb{Z}}$ be a non-degenerate rational ternary recurrence with companion polynomial $\mathcal{P}(z)$. Say $\mathcal{P}(z)$ has distinct roots α_1, α_2 and α_3. Then there exists $a_1, a_2, a_3 \in \mathbb{C}^\times$ such that

$$u_n = a_1\alpha_1^n + a_1\alpha_2^n + a_3\alpha_3^n.$$

Note that u_0, u_1, u_2 are not all zero and, by Lemma 3.9, the matrix

$$\begin{bmatrix} 1 & 1 & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 \end{bmatrix}$$

has non-zero determinant. Hence applying Cramer's Rule to

$$\begin{bmatrix} 1 & 1 & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ a_3 \end{bmatrix} \begin{bmatrix} u_0 \\ u_1 \\ u_2 \end{bmatrix},$$

we see that a_1, a_2 and a_3 are in the splitting field of $\mathcal{P}(z)$. Thus we are interested in the equation

$$a_1\alpha_1^x + a_2\alpha_2^x + a_3\alpha_3^x = 0, \tag{3.25}$$

in $x \in \mathbb{Z}$, where $\alpha_1, \alpha_2, \alpha_3$ are non-zero roots of some cubic polynomial $\mathcal{P}(z) \in \mathbb{Q}[z]$ and $a_1, a_2, a_3 \in \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$.

Lemma 3.14. *Let K be the splitting field of a cubic polynomial, $P(z) \in \mathbb{Z}[z]$, with roots $\alpha_1, \alpha_2, \alpha_3$ and say K is not real. If $v \in M_K$ is finite and has ramification index ≥ 3 then $|\alpha_1|_v = |\alpha_2|_v = |\alpha_3|_v$. Conversely if $v \in M_K$ is finite, $|\alpha_1|_v = |\alpha_2|_v = |\alpha_3|_v \neq 1$ and $\alpha_1, \alpha_2, \alpha_3$ have no common rational integer factor in $\mathcal{O}_K$ then v has ramification index ≥ 3.*

Proof. Let $v \in M_K$ be a finite place with ramification index $e \geq 3$, $\mathfrak{p}$ be the prime ideal in $\mathcal{O}_K$ associated to v and p be the rational prime above v. Let G be the Galois group of K over $\mathbb{Q}$. First assume that $p\mathcal{O}_K = \mathfrak{p}^e$. We know that G acts transitively on the prime ideals in $\mathcal{O}_K$ that divide p, hence for any $\sigma \in G$ we have $\sigma\mathfrak{p} = \mathfrak{p}$. Let $\alpha_1, \alpha_2, \alpha_3$ be the roots of $P(z)$. Say $\sigma \in G$ is such that $\sigma\alpha_1 = \alpha_2$. Then

$$|\alpha_2|_{\mathfrak{p}} = |\sigma\alpha_1|_{\mathfrak{p}} = |\alpha_1|_{\sigma^{-1}\mathfrak{p}} = |\alpha_1|_{\mathfrak{p}},$$

hence $|\alpha_1|_v = |\alpha_2|_v$. Similarly we have $|\alpha_1|_v = |\alpha_3|_v$. Now assume $p\mathcal{O}_K \neq \mathfrak{p}^e$. Then since $e|[K:\mathbb{Q}]$ we must have $e = 3$ and $[K:\mathbb{Q}] = 6$. Since G acts transitively on the prime ideals that divide p we have that $p\mathcal{O}_K = \mathfrak{p}^3\mathfrak{p}'^3$ and moreover if $\sigma \in G$ is such that $\sigma\mathfrak{p} = \mathfrak{p}'$ then σ is of order two, hence $\mathfrak{p}' = \overline{\mathfrak{p}}$. This implies that if $\sigma \in G$ has order three then $\sigma\mathfrak{p} = \mathfrak{p}$. Now since $[K:\mathbb{Q}]$ has degree six we must have one of $\alpha_1, \alpha_2, \alpha_3$ in $\mathbb{R}$, say α_1. Then we can find $\sigma, \sigma' \in G$, each of order three, such that $\sigma\alpha_1 = \alpha_2$ and $\sigma'\alpha_1 = \alpha_3$. Then

$$|\alpha_2|_{\mathfrak{p}} = |\sigma\alpha_1|_{\mathfrak{p}} = |\alpha_1|_{\sigma^{-1}\mathfrak{p}} = |\alpha_1|_{\mathfrak{p}}.$$

hence $|\alpha_1|_v = |\alpha_2|_v$. Similarly we have $|\alpha_1|_v = |\alpha_3|_v$.

Now assume that $v \in M_K$ is a finite place such that $|\alpha_1|_v = |\alpha_2|_v = |\alpha_3|_v \neq 1$. Let p denote the rational prime above v and say

$$p\mathcal{O}_K = \mathfrak{p}_1^e \cdots \mathfrak{p}_k^e,$$

for some positive integers k and e such that $ke|[K:\mathbb{Q}]$. We may assume that $\mathfrak{p}_1$ is the prime ideal associated to v. Again let G denote the Galois group of K over $\mathbb{Q}$. Since G acts transitively on $\{\mathfrak{p}_1,\dots,\mathfrak{p}_k\}$, there is a $\sigma_i \in G$, for each $1 \le i \le k$, such that $\sigma_i\mathfrak{p}_1 = \mathfrak{p}_i$. Then since $|\alpha_1|_{\mathfrak{p}_1} = |\alpha_2|_{\mathfrak{p}_1} = |\alpha_3|_{\mathfrak{p}_3}$ we have

$$|\alpha_j|_{\mathfrak{p}_i} = |\alpha_j|_{\sigma\mathfrak{p}_1} = \left|\sigma^{-1}\alpha_j\right|_{\mathfrak{p}_1} = |\alpha_j|_{\mathfrak{p}_1},$$

for each $1 \le j \le 3$ and $1 \le i \le k$. This then implies that $\mathrm{ord}_{\mathfrak{p}_i}\alpha_j$ is the same for each $1 \le j \le 3$ and $1 \le i \le k$ and we denote this number by a. Since $P(z) \in \mathbb{Z}[z]$ we know that a is a nonnegative integer and since $|\alpha_j|_{\mathfrak{p}_1} \ne 1$, for $1 \le j \le 3$ by assumption, we have $a \ge 1$. If $e = 1$ then we have

$$\alpha_1, \alpha_2, \alpha_3 \in \mathfrak{p}_1 \cdots \mathfrak{p}_k = p\mathcal{O}_K,$$

hence p divides α_1, α_2 and α_3 in $\mathcal{O}_K$, which is a contradiction. If $e = 2$ then since $\alpha_1\alpha_3\alpha_3 \in \mathbb{Z}$ we must have $2|\mathrm{ord}_{\mathfrak{p}_1}(\alpha_1\alpha_2\alpha_3)$. But $\mathrm{ord}_{\mathfrak{p}_1}(\alpha_1\alpha_2\alpha_3) = 3a$, hence $2|a$. This implies that

$$\alpha_1, \alpha_2, \alpha_3 \in \mathfrak{p}_1^2 \cdots \mathfrak{p}_k^2 = p\mathcal{O}_K,$$

which, as in the $e = 1$ case, is a contradiction. Thus we must have $e \ge 3$. □

Lemma 3.15. *Let $\{u_n\}_{n\in\mathbb{Z}}$ be a non-degenerate rational ternary recurrence sequence with companion polynomial $\mathcal{P}(z) = z^3 - c_1z^2 - c_2z - c_3$ that has distinct roots $\alpha_1, \alpha_2, \alpha_3$. Suppose that $u_0 = 0$ and that we can find $a, b \in \mathbb{Q}^\times$, positive integers c and d and a prime p such that*

1. *$\alpha_i^d = a + b\alpha_i^c$ for each $i = 1, 2, 3$,*
2. *$|b|_p \le 1/4$, $|c_3|_p = |a|_p = 1$ and $|u_n|_p \le 1$ for all $n \in \mathbb{Z}$,*
3. *$|u_n|_p < 1$ and $0 \le n \le d + 2c$ implies $u_n = 0$.*

Then $u_n = 0$ implies either $0 \le n < d$ or that $n = d + r$ for some $0 \le r < d$ and $u_r = u_{r+c} = 0$.

Proof. Suppose $u_n = 0$ and put $n = qd + r$ with q and r positive integers and $0 \le r < d$. If $q = 0$ then $n = r < d$ and we are done, so we will assume $q > 0$. By assumption 1 and (3.25) we have

$$\sum_{i=1}^{3} a_i \left(1 + \frac{b}{a}\alpha_i^c\right)^q \alpha_j^r = 0.$$

Using binomial expansions we get

$$u_r + \sum_{j=1}^{q} \binom{q}{j} \left(\frac{b}{a}\right)^j \left(\sum_{i=1}^{3} a_i\alpha_i^{r+jc}\right),$$

hence

$$u_r + \sum_{j=1}^{q} \binom{q}{j} \left(\frac{b}{a}\right)^j u_{r+jc} = 0. \tag{3.26}$$

Since $|u_{r+jc}|_p \leq 1$ and $\left|\frac{b}{a}\right|_p < 1$, (3.26) implies that $|u_r|_p < 1$. So, by condition 3, we have $u_r = 0$, hence

$$\sum_{j=1}^{q} \binom{q}{j} \left(\frac{b}{a}\right)^j u_{r+jc} = 0. \tag{3.27}$$

If $q = 1$ then $(qb/a)u_{r+c} = 0$, hence we have $n = d + r$ with $0 \leq r < d$, $u_r = 0$ and $u_{r+c} = 0$. We now assume $q \geq 2$ and will derive a contradiction. Dividing (3.27) by qb/a we have

$$u_{r+c} + \sum_{j=2}^{q} \binom{q-1}{t-1} \frac{1}{j} \left(\frac{b}{a}\right)^{j-1} u_{r+jc} = 0. \tag{3.28}$$

Since $|b|_p \leq 1/4$ and $|a|_p = 1$, we have $\left|\frac{1}{j}\left(\frac{b}{a}\right)^{j-1}\right|_p < 1$ for all $j \geq 2$, hence $u_{r+c} < 1$. Then by condition 3 we have $u_{r+c} = 0$. If $q = 2$ then (3.28) then gives $u_{r+2c} = 0$. But $u_r = u_{r+c} = u_{r+2c} = 0$ violates Lemma 3.9 since our sequence is non-degenerate. Assume $q \geq 3$. Dividing

$$\sum_{j=2}^{q} \binom{q-1}{t-1} \frac{1}{j} \left(\frac{b}{a}\right)^{j-1} u_{r+jc} = 0$$

by $(q-1)b/a$ yields

$$u_{r+2c} + \sum_{j=3}^{q} \binom{q-1}{j-1} \frac{1}{j(j-1)} \left(\frac{b}{a}\right)^{j-2} u_{r+jc} = 0. \tag{3.29}$$

Similar to above, since $|b|_p \leq 1/4$ and $|a|_p = 1$, we have $\left|\frac{1}{j(j-1)}\left(\frac{b}{a}\right)^{t-2}\right|_p < 1$ for every $j \geq 3$. Then (3.29) implies $|u_{r+2c}| < 1$. Condition 3 then implies $u_{r+2c} = 0$. But $u_r = u_{r+c} = u_{r+2c} = 0$ contradicts Lemma 3.9. Thus we have either $0 \leq n < d$ or $n = d + r$ with $0 \leq r < d$ and $u_r = u_{r+c} = 0$. □

Theorem 3.1. *Let $\{u_n\}_{n\in\mathbb{Z}}$ be a non-degenerate rational ternary recurrence sequence. Then the zero-multiplicity of $\{u_n\}_{n\in\mathbb{Z}}$ is at most six.*

Proof. By Lemma 3.13 we may assume that $\{u_n\}_{n\in\mathbb{Z}}$ is a simple recurrence. Let α_1, α_2 and α_3 be the roots of the companion polynomial to $\{u_n\}_{n\in\mathbb{Z}}$. Then there exists $a_1, a_2, a_3 \in K^\times$, where $K = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$, such that

$$u_n = a_1\alpha_1^n + a_1\alpha_2^n + a_3\alpha_3^n.$$

We consider equation (3.25) in the unknown $x \in \mathbb{Z}$.

First assume $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}$. We rewrite equation (3.25) as

$$a_1 \left(\frac{\alpha_1}{\alpha_3}\right)^x + a_2 \left(\frac{\alpha_2}{\alpha_3}\right)^x + a_3 = 0.$$

If we have at least five solutions then there must be at most three of the same parity. But the equations

$$a_1 \left(\frac{\alpha_1^2}{\alpha_3^2}\right)^x + a_2 \left(\frac{\alpha_2^2}{\alpha_3^2}\right)^x + a_3 = 0$$

and

$$a_1 \frac{\alpha_1}{\alpha_3} \left(\frac{\alpha_1^2}{\alpha_3^2}\right)^x + a_2 \frac{\alpha_1}{\alpha_3} \left(\frac{\alpha_2^2}{\alpha_3^2}\right)^x + a_3 = 0$$

have at most one max/min. This is a contradiction, hence (3.25) has at most four solutions when $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}$.

Henceforth we may assume that we have one real root and two complex conjugate roots. Take a finite $v \in M_K$. For any $\gamma, \eta \in M_K$ we have

$$|\gamma + \eta|_v \leq \max\{|\gamma|_v, |\eta|_v\},$$

moreover if $|\gamma|_v \neq |\eta|_v$ then

$$|\gamma + \eta|_v = \max\{|\gamma|_v, |\eta|_v\}.$$

So if equation (3.25) holds for some $x \in \mathbb{Z}$ then we must have

$$|a_i \alpha_i^x|_v = \left|a_j \alpha_j^x\right|_v, \tag{3.30}$$

for some $i \neq j$. If there is a finite $v \in M_K$ such that $|\alpha_1|_v, |\alpha_2|_v, |\alpha_3|_v$ are all distinct then, by (3.30) we can have at most three solutions to (3.25).

Now assume that there is a finite valuation $v \in M_K$ such that $|\alpha_1|_v = |\alpha_2|_v \neq |\alpha_3|_v$. Then by Lemma 3.14 v has ramification ≤ 2. We can then apply Lemma 3.12 to the equation

$$\left(-\frac{a_1}{a_3}\right)\left(\frac{\alpha_1}{\alpha_3}\right)^x + \left(-\frac{a_2}{a_3}\right)\left(\frac{\alpha_2}{\alpha_3}\right)^x = 1,$$

if $|\alpha_1|_v < |\alpha_3|_v$, or to the equation

$$\left(-\frac{a_3}{a_1}\right)\left(\frac{\alpha_3}{\alpha_1}\right)^x + \left(-\frac{a_2}{a_1}\right)\left(\frac{\alpha_2}{\alpha_1}\right)^x = 1,$$

if $|\alpha_1|_v > |\alpha_3|_v$, which yields at most six solutions.

We are left with the case when $|\alpha_1|_v = |\alpha_2|_v = |\alpha_3|_v$ for all finite $v \in M_K$. Let α_1 be the real root of $\mathcal{P}(z)$. If $\alpha_1 \in \mathbb{Q}$ then K is an imaginary quadratic field. In this case there is only one infinite place $v \in M_K$ and it satisfies $|\alpha_2|_v = |\alpha_3|_v$. But then $|\alpha_2/\alpha_3|_v = 1$ for all $v \in M_K$ which implies that α_2/α_3 is a root of unity. So we must have that $\alpha_1 \notin \mathbb{Q}$ and $[K : \mathbb{Q}] = 6$.

Note that if (3.25) has the solution $x \in \mathbb{Z}$ then if we replace each α_i by α_i^{-1} our new equation has the solution $-x$ and so the corresponding recurrence sequences will have the same zero-multiplicity. By making this substitution, if necessary, we may assume $|\alpha_1| \leq |\alpha_2|$. Further we may multiply $\alpha_1, \alpha_2, \alpha_3$ by the same rational number so that $\alpha_1 > 0$ and $\alpha_1, \alpha_2, \alpha_3$ are algebraic integers with no common rational integer factor in $\mathcal{O}_K$.

Since $K \not\subseteq \mathbb{R}$ if $|\alpha_2/\alpha_1| \geq 4$ there is an infinite complex place $v \in M_K$ such that $|\alpha_2/\alpha_1|_v \geq 4^{2/6} = 4^{1/3}$. In particular this implies $H(\alpha_2/\alpha_1) > 2^{1/3}$. We can then apply Lemma 3.11 with $\lambda = -a_2/a_1$ and $\alpha = \alpha_2/\alpha_1$. We may thus assume that $|\alpha_2/\alpha_1| < 4$. The set of polynomials in $\mathbb{Z}[z]$ with roots satisfying this as well as the conditions of the above two paragraphs is finite and is given in Table 3.1 of the following section. Note that for each of the entries in the table we have $|\alpha_2/\alpha_1| > 4/3$ and $10^{-4} < |\arg(\alpha_2/\alpha_1)| < \pi - 10^{-4}$.

Suppose that (3.25) has seven solutions, $0 < x_1 < x_2 < x_3 < x_4 < x_5 < x_6$. First suppose that $x_2 > 50$. Applying part 1 of Lemma 3.10 with $m = x_6$, $l = x_5$, $k = x_4$ and $\alpha = \alpha_2/\alpha_1$ to obtain $x_6 - x_4 > |\alpha_2/\alpha_1|^{x_4} > (4/3)^{x_4}$. Since $x_4 > 50$ we clearly have $x_6 > 10x_4$ and we can apply Lemma 3.7 which yields

$$x_4 < 196 + \frac{50}{3}x_1, \tag{3.31}$$

since $H(\alpha_2/\alpha_1) \geq (4/3)^{2/6} = (4/3)^{1/3}$. But applying part 1 of Lemma 3.10 we have $x_4 - x_2 > |\alpha_2/\alpha_1|^{x_2} > (4/3)^{x_2}$. This contradicts (3.31) since $x_2 > 50$. Thus we may assume $x_2 \leq 50$. For every entry in Table 3.1 there is a recurrence relation given by the c_1, c_2, c_3. We have determined all the initial values u_0, u_1, u_2 such that $u_0 = 0$ and $u_n = 0$ has at least three solutions in n with $0 \leq n \leq 250$. These recurrences are listed in Table 3.2 of the following section. In particular the recurrences that we have not yet ruled out will be in this list. If $x_4 > 50$ then inequality (3.31) still holds. From Table 3.2 we see that $x_1 \leq 2$ with one exception, and (3.31) then yields $x_4 < 250$. The one exception corresponds to $c_1 = -2$, $c_2 = 0$ and $c_3 = 2$. In this case we have $|\alpha_2/\alpha_1| > 1.6$, hence $H(\alpha_2/\alpha_1) > (1.8)^{1/3}$. From this the 196 in (3.31) can be improved to 100 and again we get $x_4 < 250$ since $x_1 = 4$. So we may assume that $x_4 < 250$. We then are left with the following recurrences

$c_1 = 2$, $c_2 = -4$, $c_4 = 4$, $u_0 = 0$, $u_1 = 0$ and $u_2 = 1$ with solutions $n = 0, 1, 4, 6, 13, 52$
$c_1 = 2$, $c_2 = -4$, $c_3 = 4$, $u_0 = 0$, $u_1 = 1$ and $u_2 = 2$ with solutions $n = 0, 3, 5, 12, 51$
$c_1 = -1$, $c_2 = 0$, $c_3 = 1$, $u_0 = 0$, $u_1 = 1$ and $u_2 = 0$ with solutions $n = 0, 2, 3, 7, 16$
$c_1 = -2$, $c_2 = 0$, $c_3 = 4$, $u_0 = 0$, $u_1 = 1$ and $u_2 = 0$ with solutions $n = 0, 2, 3, 8, 24$.

We don't need to consider the second as it is a subsequence of the first. We apply Lemma 3.15 to each in order to show that there are no solutions $u_n = 0$ with n greater than the ones listed. For the first recurrence we take $a = -206 \cdot 2^{34}$, $b = 159 \cdot 2^{34}$, $c = 1$, $d = 52$ and $p = 53$. For the third sequence we take $a = 4$, $b = -7$, $c = 2$, $d = 16$ and $p = 7$. For the last sequence we take $a = 26 \cdot 2^{14}$, $b = -23 \cdot 2^{14}$, $c = 1$, $d = 22$ and $p = 23$. □

3.4 Tables 3.1 and 3.2

Let $\mathcal{P}(z) \in \mathbb{Z}[z]$ be given by $\mathcal{P}(z) = z^3 - c_1 z^2 - c_2 z - c_3$ with splitting field K. Suppose that $\mathcal{P}(z)$ is irreducible with roots $\alpha_1, \alpha_2, \alpha_3$ such that $\alpha_1 \in \mathbb{R}$ and α_2, α_3 are complex conjugate roots. In Table 3.1 we list all c_1, c_2, c_3 such that $\alpha_1 > 0$, $|\alpha_2/\alpha_1| < 4$, $|\alpha_1|_v = |\alpha_2|_v = |\alpha_3|_v$ for all finite places $v \in M_K$ and $\alpha_1, \alpha_2, \alpha_3$ have no common rational integer factor in $\mathcal{O}_K$.

We compile the table by first noting that Lemma 3.14 implies that for any finite place v we have either $|\alpha_i| = 1$, for $i = 1, 2, 3$, or v ramifies to order $e \geq 3$. Since K is Galois over $\mathbb{Q}$ we see that $e = 3$ or 6. Let $\mathfrak{p}$ be the prime ideal in $\mathcal{O}_K$ associated to v. Since the α_i are of degree three over $\mathbb{Q}$, if $|\alpha_i|_v \neq 1$ we have either v ramifies to order 3 or it ramifies to order 6 and $\alpha_i \in \mathfrak{p}^2$. This implies that we can find conjugate units $\eta_1, \eta_2, \eta_3 \in \mathcal{O}_K$ and a positive integer a such that $\alpha_i^3 = a\eta_i$ for each $i = 1, 2, 3$. Now $|\alpha_2/\alpha_1| < 4$ implies that $|\eta_2/\eta_1| < 64$ and noting that $\eta_1\eta_2\eta_3 = 1$ we have that $|\eta_1| < 1$ and $1 < |\eta_2| = |\eta_3| < 4$. Using these bounds we can compute all the polynomials that have roots η_1, η_2, η_3 satisfying the above conditions. The discriminants of these polynomials give the possible primes in $\mathbb{Q}$ that will ramify to order 3 or 6 in $\mathbb{Q}(\eta_1, \eta_2, \eta_3)$ which then yields the possibilities for a.

The sequences in Table 3.2 are all of those satisfying a recurrence relation from Table 3.1 such that $u_0 = 0$ and $u_n = 0$ has at least three solutions with $0 \leq n < 250$. If $\{u_n\}_{n\geq 0}$ is listed then we do not list its multiples or its shifted versions $\{u_{n+k}\}_{n\geq 0}$ for any $k \in \mathbb{Z}$.

The table is compiled as follows. For each recurrence relation in Table 3.1 and each $0 < m < 250$ we determine u_1 and u_2 so that $u_m = 0$. This is done in the following way. If $m = 1$ then we set $u_2 = 1$. Note that we may take $u_2 = 1$ because u_3 will be a linear combination of u_2 and $u_0 = 0$ and $u_1 = 0$, hence will be divisible by u_2. Then u_4 will be a linear combination of u_3, u_2 and 0, hence will be divisible by u_2. Continuing in this manner we see that all of the terms of the recurrence sequence will be divisible by u_2 and we may take it to be 1. If $m \geq 2$ then using the recurrence relation we have

$$0 = c_1 u_{n-1} + c_2 u_{n-2} + c_3 u_{n-3} = \cdots = cu_1 + du_2, \tag{3.32}$$

for some integers c and d not both zero. If $c = 0$ then we set $u_1 = 1$ and $u_2 = 0$, if $d = 0$ we set $u_1 = 0$ and $u_2 = 1$ and if both c and d are non-zero we take u_1 and u_2 to be the unique pair satisfying (3.32) so that $u_1 > 0$ and $\gcd(u_1, u_2) = 1$. We then check our recurrence for

Table 3.1: Possible recurrences

c_1	c_1	c_3	$\lvert\alpha_2/\alpha_1\rvert$	c_1	c_2	c_3	$\lvert\alpha_2/\alpha_1\rvert$	c_1	c_2	c_3	$\lvert\alpha_2/\alpha_1\rvert$
-6	0	36	1.961	0	-12	-12	3.847	0	-1	1	1.774
-5	0	25	1.905	0	-11	11	3.713	1	-2	1	2.325
-3	0	9	1.762	0	-10	10	3.574	2	-4	2	2.769
-2	-4	4	3.528	0	-9	9	3.428	2	-4	4	1.356
-2	-2	2	3.246	0	-7	7	3.115	2	-3	1	3.545
-2	-1	1	3.148	0	-6	6	2.944	3	-9	9	1.961
-2	0	2	1.839	0	-5	5	2.761	3	-6	3	3.104
-2	0	4	1.664	0	-4	4	2.562	4	-8	4	3.383
-1	-1	1	2.494	0	-3	3	2.342	5	-25	25	3.677
-1	0	1	1.525	0	-2	1	3.276	5	-10	5	3.627
0	-13	13	3.977	0	-2	2	2.089	6	-18	18	1.961

all solutions $u_n = 0$ with $0 < n < 250$ and record only the recurrences with at least two solutions other than u_0.

Table 3.2: Recurrences with at least three small solutions

c_1	c_2	c_3	u_0	u_1	u_2	Solutions n with $0 \leq n < 250$
-3	0	9	0	1	0	0,2,3,9
-2	0	2	0	1	0	0,2,3,26
-2	0	2	0	2	-1	0,4,12
-2	0	4	0	1	0	0,2,3,8,24
-1	-1	1	0	0	1	0,1,4,17
-1	0	1	0	1	0	0,2,3,7,16
0	-6	6	0	1	0	0,1,3,12
0	-3	3	0	0	1	0,1,3,10
0	-1	1	0	0	1	0,1,3,8
2	-4	2	0	0	1	0,1,4,12
2	-4	4	0	0	1	0,1,4,6,12,52
3	-9	9	0	0	1	0,1,4,9

Chapter 4

Denominators of Rational Numbers

The results of this chapter do not directly concern linear recurrence sequences but they are vital to the proof of our main theorem in the next chapter. It will become important to deal with equations of the form

$$b_1\beta_1^x + \cdots + b_n\beta_n^x = 0, \tag{4.1}$$

in $x \in \mathbb{Z}$, where β_i/β_j is a root of unity for each $1 \leq i, j \leq n$. If we fix $1 \leq j \leq n$ and rewrite this equation as

$$\left(-\frac{b_1}{b_j}\right)\left(\frac{\beta_1}{\beta_j}\right)^x + \cdots + \left(-\frac{b_n}{b_j}\right)\left(\frac{\beta_n}{\beta_j}\right)^x = 1,$$

we see that the order of the β_i/β_j, $1 \leq i \leq n$, become important in determining the solutions $x \in \mathbb{Z}$. For distinct i, j, k, the size of the group $G(\beta_i : \beta_j : \beta_k)$ generated by β_i/β_j and β_i/β_k will play a key role. In particular we will need to show that there exist equations of the form (4.1), with $\beta_1, \ldots, \beta_n$ in some given set, such that the size of the groups $G(\beta_i : \beta_j : \beta_k)$ are sufficiently large for our purposes. Since β_i/β_j is a root of unity for each $1 \leq i, j \leq n$ we see that there exist real numbers b and $\rho_1, \ldots, \rho_n$ such that

$$\beta_j = b\mathrm{e}^{2\pi\mathrm{i}\rho_j},$$

for each $1 \leq j \leq n$. Moreover we see that $\rho_i - \rho_j \in \mathbb{Q}$, hence if we let r_{ij} be the denominator of $\rho_i - \rho_j$ then

$$|G(\beta_i : \beta_j : \beta_k)| = \mathrm{lcm}(r_{ij}, r_{ik}),$$

and so our problem becomes one of determining least common multiples of denominators of rational numbers. In particular if we can give an upper bound on the number of times $\mathrm{lcm}(r_{ij}, r_{ik})$ is small then we can find $\beta_1, \ldots, \beta_n$, provided the set from which they belong is large enough, such that that the groups $G(\beta_i : \beta_j : \beta_k)$ are not too small.

The results in this Chapter are due to Schmidt and in particular §4.1 follows [17] and §4.2 follows [18].

4.1 Denominators of rational numbers and ε-bad l-tuples

Let $R = \{\rho_1, \ldots, \rho_n\}$ be a set of real numbers such that $\rho_i - \rho_j \in \mathbb{Q}$ for each $1 \leq i, j \leq n$ and $\rho_i - \rho_j \notin \mathbb{Z}$ if $i \neq j$. For the remainder of this chapter we will call such a set of reals a *denominator system*. In this chapter we will usually refer to a denominator system as simply a *system* for brevity. Let r_{ij} be the smallest positive integer such that $r_{ij}(\rho_i - \rho_j) \in \mathbb{Z}$, we call r_{ij} the *denominator* of $\rho_i - \rho_j$. Let $N(\varepsilon)$ be the number of triples i, j, k with $1 \leq i, j, k \leq n$ such that

$$\operatorname{lcm}(r_{ij}, r_{ik}) \leq \varepsilon n. \tag{4.2}$$

In [17] Schmidt conjectures that there is a function $\delta(\varepsilon)$, independent of n and R, which tends to zero as ε tends to zero, such that

$$N(\varepsilon) \leq \delta(\varepsilon) n^3 \tag{4.3}$$

In light of this conjecture it is natural to ask if there is a function $\delta(\varepsilon)$ as above such that the number of pairs i, j with $1 \leq i, j \leq n$ and $r_{ij} \leq \varepsilon n$ is bounded by $\delta(\varepsilon)n^2$. This is not the case. Consider $R = \{0, 1/n, \ldots, (n-1)/n\}$ and let $N_0(\varepsilon)$ be the number of such pairs. We have $N_0(\varepsilon) = nN_0'(\varepsilon)$ where $N_0'(\varepsilon)$ is the number of integers i, $1 \leq i \leq n$, such that $gcd(i, n) \geq 1/\varepsilon$. We have that $N_0'(\varepsilon) = n - N_0''(\varepsilon)$ where $N_0''(\varepsilon)$ is the number of integers i, $1 \leq i \leq n$, with $\gcd(i, n) < 1/\varepsilon$. We have

$$N_0''(\varepsilon) \leq n \prod_{\substack{p \mid n \\ p \geq 1/\varepsilon}} (1 - p^{-1})$$

If we set n to be the product of all the primes in the interval $[1/\varepsilon, m]$ then since, for $s > 1$,

$$\prod_{\substack{p \mid n \\ p \geq 1/\varepsilon}} (1 - p^{-s})^{-1} \to \zeta(s)$$

as $n \to \infty$ and $\zeta(s) \to \infty$ as $s \to 1$ we can take m large enough to ensure $N_0''(\varepsilon) < n/2$, hence $N_0'(\varepsilon) > n/2$ and $N_0(\varepsilon) > n^2/2$.

For our purposes we will not need to assume Schmidt's conjecture in it's full generality, it will suffice to prove it in special cases. For a system $R = \{\rho_1, \ldots, \rho_n\}$, $1 \leq i \leq n$ and

$x \in \mathbb{Z}$, we let $u_i^R(x)$ denote the number of $1 \le j \le n$ such that

$$r_{ij}|x$$

We will call a system *homogeneous* if $u_i^R(x)$ does not depend on i, in which case we simply write $u^R(x)$. For example $R = \{0, 1/n, \ldots, (n-1)/n\}$ is homogenous. For positive integer q the set of numbers i/q such that $1 \le i \le q$ and $\gcd(i, q) = 1$ is another example. If the system R is understood we will sometimes write $u(x)$.

Theorem 4.1. *If R is a homogeneous system and $0 < \chi < 1$ then*

$$N(\varepsilon) \le \zeta(2-\chi)\varepsilon^{\chi} n^3 \tag{4.4}$$

So in (4.3) we may take $\delta(\varepsilon) = \zeta(2-\chi)\varepsilon^{\chi}$. To prove Theorem 4.1 we will actually prove something slightly stronger. For homogeneous systems R and S we say that R and S are *isomorphic*, denoted $R \cong S$, if for each $x \in \mathbb{Z}$ we have $u^R(x) = u^S(x)$. Note that $R \cong S$ necessarily implies that they are of the same cardinality by taking x so that $u^R(x) = |R|$ and $u^S(x) = |S|$.

Theorem 4.2. *Let $R = \{\rho_1, \ldots, \rho_n\}$, $S = \{\sigma_1, \ldots, \sigma_n\}$ and $T = \{\tau_1, \ldots, \tau_n\}$ be homogeneous and isomorphic to each other. Suppose that for each $1 \le i, j, k \le n$ we have $\rho_i - \sigma_j, \rho_i - \tau_k \in \mathbb{Q}$. Let a_{ij} and b_{ik} be the denominators of $\rho_i - \sigma_j$ and $\rho_i - \tau_k$ respectively. If $N(\varepsilon)$ is the number of triples $1 \le i, j, k \le n$ with*

$$\operatorname{lcm}(a_{ij}, b_{ik}) \le \varepsilon n \tag{4.5}$$

then (4.4) holds for $0 < \chi < 1$.

Theorem 4.2 will be proven via a series of Lemmas. Let $R = \{\rho_1, \ldots, \rho_n\}$ be a homogeneous system. For $x \in \mathbb{Z}$ and $1 \le i, j \le n$ we write $\rho_i \overset{x}{\sim} \rho_j$ if $x(\rho_i - \rho_j) \in \mathbb{Z}$. It is easy to see that $\overset{x}{\sim}$ defines an equivalence relation on R. Since R is homogeneous, each equivalence class will consist of $u(x)$ elements, hence R splits into $n/u(x)$ equivalence classes, which we will denote by $v(x)$.

For $R = \{\rho_1, \ldots, \rho_n\}$, $S = \{\sigma_1, \ldots, \sigma_n\}$ and $x \in \mathbb{Z}$, we write $R \overset{x}{\equiv} S$ if $x(\rho_i - \sigma_j) \in \mathbb{Z}$ for each $1 \le i, j \le n$. The relation $\overset{x}{\equiv}$ for systems is symmetric and transitive but is not necessarily reflexive. However if $R \overset{x}{\equiv} S$ then $R \overset{x}{\equiv} R$ since $R \overset{x}{\equiv} S \overset{x}{\equiv} R$. Note that if $R \overset{x}{\equiv} R$ then $\rho_i = \rho_1 + a_i/x$ with $a_i \in \mathbb{Z}$, but if $i \ne j$ then $\rho_i - \rho_j = (a_i - a_j)/x \notin \mathbb{Z}$, hence $a_i \not\equiv a_j \pmod{x}$ and thus $|R| \le x$.

Lemma 4.1. *Let R be homogeneous, x a positive integer and let $R_1, \dots, R_v$ be the equivalence classes of R with respect to $\overset{x}{\sim}$. Then for each $1 \le r, s \le v$ we have $R_r \overset{x}{\equiv} R_r$ but $R_r \overset{x}{\not\equiv} R_s$ when $r \neq s$. The systems $R_1, \dots, R_v$ are all homogeneous and isomorphic to each other. When $R \overset{m}{\equiv} R$ and $x|m$ then $v \le m/x$. Furthermore, if S is homogeneous and isomorphic to R with equivalence classes $S_1, \dots, S_v$ then $R_1 \cong \cdots \cong R_v \cong S_1 \cong \cdots \cong S_v$. Given $1 \le r \le v$ there is at most one $1 \le s \le v$ with $R_r \overset{x}{\equiv} S_s$.*

Proof. If $\rho_i, \rho_j \in R_r$ then $x(\rho_i - \rho_j) \in \mathbb{Z}$, thus $R_r \overset{x}{\equiv} R_r$. However if $\rho_j \in R_r$ and $\rho_j \in R_s$, for $i \neq j$, then $x(\rho_i - \rho_j) \notin \mathbb{Z}$ so $R_r \overset{x}{\not\equiv} R_s$. Now suppose that $\rho_i, \rho_j \in R_r$. Then $\rho_i \overset{y}{\sim} \rho_j$ when $r_{ij}|y$. Since $r_{ij}|x$ we have $\rho_i \overset{y}{\sim} \rho_j$ precisely when $r_{ij}|d$ where $d = \gcd(x, y)$. Conversely if $\rho_i \in R_r$, $\rho_j \in R$ and $r_{ij}|d$ then $r_{ij}|y$ and $r_{ij}|x$, hence $\rho_j \in R_r$. So we have

$$u_i^{R_r}(y) = u_i^{R_r}(d) = u_i^R(d) = u^R(d)$$

Thus R_r is homogeneous with $u^{R_r}(y) = u^R(y)$. It follows that $R_1 \cong, \dots, \cong R_v$. If $R \overset{m}{\equiv} R$ then for each $1 \le i \le n$ we have $\rho_i = \rho_1 + a_i/m$ for $a_i \in \mathbb{Z}$. Now if $\rho_i \in R_r$ and $\rho_j \in R_s$, with $r \neq s$, then $x(\rho_i - \rho_j) = x(a_i - a_j)/m \notin \mathbb{Z}$, so that $a_i \not\equiv a_j \pmod{m/x}$. Thus we must have $v \le m/x$.

When S is homogeneous with $R \cong S$, each equivalence class $S_1, \dots S_v$ is homogeneous and, for each $1 \le s \le v$, $u^{S_s}(y) = u^S(d) = u^R(d)$. Hence $R_1 \cong \dots \cong R_v \cong S_1 \cong \dots \cong S_v$. Lastly we see that if $R_r \overset{x}{\equiv} S_s$ and $R_r \overset{x}{\equiv} S_t$ then $S_r \overset{x}{\equiv} S_t$, giving $s = t$.

□

For any prime p set $c(\chi, p) = (1 - p^{\chi-2})^{-1}$ and for $m > 1$,

$$c(\chi, m) = \prod_{p|m} c(\chi, p),$$

where, again, $0 < \chi < 1$. We set $c(\chi, 1) = 1$.

Lemma 4.2. *Suppose that systems R, S, T are as in Theorem 4.2 and that there is some $m \in \mathbb{Z}$ such that*

$$R \overset{m}{\equiv} S \overset{m}{\equiv} T. \tag{4.6}$$

Then

$$N(\varepsilon) \le c(\chi, m)\varepsilon^{\chi} n^3.$$

Note that for any systems R, S, T as in Theorem 4.2 there is an $m \in \mathbb{Z}$ satisfying (4.6) and that $c(\chi, m) < \zeta(2 - \chi)$. Thus Lemma 4.2 implies Theorem 4.2.

Proof. If $m = 1$ we have $\rho_i - \rho_j \in \mathbb{Z}$ for $1 \le i, j \le n$ and $\rho_i - \rho_j \notin \mathbb{Z}$ when $i \ne j$, and so $n = 1$. Then (4.5) cannot hold unless $\varepsilon \ge 1$. In this case $N(\varepsilon) = 1 \le \varepsilon^\chi = c(\chi, 1)\varepsilon^\chi 1^3$. Thus it will suffice to prove the lemma for

$$m = p^l m_0$$

where p is a prime with $p \not| m_0$, $l > 0$, assuming the Lemma is true for m_0.

Applying a common translation to R, S, T we may assume that all of their elements are in $m^{-1}\mathbb{Z}$. Set, for $0 \le q \le l$,

$$x_q = m_0 p^{l-q} = m p^{-q}.$$

Let $R_1, \dots, R_{v_1}$ be the equivalence classes of R with respect to $\overset{x_1}{\equiv}$, where $v_1 = v(x_1)$. We see that each R_r, for $1 \le r \le v_1$, has $u(x_1) = n/v_1$ elements. By Lemma 4.1 we have $v_1 \le m/x_1 = p$. Given a class R_r, we split it into subclasses $R_{r,1}, \dots, R_{r,v_2}$ with respect to $\overset{x_2}{\equiv}$. Since $R_r \overset{x_1}{\equiv} R_r$ we have $v_2 \le x_1/x_2 = p$. Moreover, since $R_r \cong R_{r'}$, the number v_2 is independent of the choice of $1 \le r \le v_1$, by Lemma 4.1. Now we have that R splits into the classes R_{r_1,r_2}, $1 \le r_1 \le v_1$ and $1 \le r_2 \le v_2$, with respect to $\overset{x_2}{\equiv}$ and these $v_1 v_2$ systems are isomorphic to each other. We continue in this manner and, for $0 < q \le l$, we construct sets $R_{r_1,\dots,r_q}$ with $1 \le r_i \le v_i$, where v_i is the number of equivalence classes of any $R_{r_1,\dots,r_{i-1}}$ under $\overset{x_i}{\equiv}$. These equivalence classes are all isomorphic to each other and they contain $n/v(x_q) = n/(v_1 \cdots v_q)$ elements. When $q = 0$ the notation $R_{r_1,\dots,r_q}$ denotes R.

Likewise we construct systems $S_{s_1,\dots,s_q}$ and $T_{t_1,\dots,t_q}$, where $1 \le s_i \le v_i$ and $1 \le t_i \le v_i$, for $1 \le i \le q$, with the numbers $v_1, \dots, v_q$ the same as above by Lemma 4.1. Also by Lemma 4.1, since $R \cong S \cong T$, we have

$$R_{r_1,\dots,r_q} \cong S_{s_1,\dots,s_q} \cong T_{t_1,\dots,t_q}$$

for any $r_1, \dots, t_q$ as above.

If we have

$$R_{r_1,\dots,r_q} \overset{x_q}{\equiv} S_{s_1,\dots,s_q} \overset{x_q}{\equiv} T_{t_1,\dots,t_q} \tag{4.7}$$

for some $1 \le q \le l$ and $r_1, \dots, t_q$, then

$$R_{r_1,\dots,r_{q-1}} \overset{x_{q-1}}{\equiv} S_{s_1,\dots,s_{q-1}} \overset{x_{q-1}}{\equiv} T_{t_1,\dots,t_{q-1}} \tag{4.8}$$

When $q = 1$ (4.8) denotes $R \overset{x_0}{\equiv} S \overset{x_0}{\equiv} T$, which is true by (4.6) since $x_0 = m$. On the other hand, when (4.8) holds, then by Lemma 4.1 the number of triples r_q, s_q, t_q with (4.7) is $\le v_q$, since there are at most v_q choices for r_q. Denote by w_1 the number of triples r_1, s_1, t_1 such that (4.7) holds for $q = 1$, in particular $w_1 \le v_1$. Suppose that $w_1, \dots, w_{q-1}$ have been defined such that the number of $3(q-1)$-tuples $r_1, \dots, t_{q-1}$ with (4.8) equals $w_1 \cdots w_{q-1}$. Let w_q be a number such that the number of $3q$-tuples $r_1, \dots, t_q$ with (4.7) equals $w_1 \cdots w_q$. In

particular, when $w_1 \cdots w_{q-1} = 0$, then (4.8) never holds, hence (4.7) never holds, and we set $w_q = 0$. In this way w_q is uniquely defined for each $1 \le q \le l$, and $0 \le w_q \le v_q$.

We will write $\mathbf{r} = (r_1, \dots, r_l),\ \mathbf{s} = (s_1, \dots, s_l),\ \mathbf{t} = (t_1, \dots, t_l)$. There are $(v_1 \cdots v_l)^3$ triples $\mathbf{r}, \mathbf{s}, \mathbf{t}$. For $0 \le q \le l$, let C_q be the set of triples $\mathbf{r}, \mathbf{s}, \mathbf{t}$ such that q is the largest integer in $0 \le q \le l$ for which (4.7) holds. In particular, C_0 consists of the triples where (4.7) does not hold for $q = 1$. The number of $3q$-tuples $r_1, \dots, t_q$ with (4.7) is $w_1 \cdots w_q$. Thus

$$|C_l| = w_1 \cdots w_l. \tag{4.9}$$

When $q < l$, the number of $3(q+1)$-tuples $r_1, \dots, t_{q+1}$ with (4.7) equals $w_1 \cdots w_q v_{q+1}^3$. On the other hand, the number of such $3(q+1)$ tuples where (4.7) holds with $q+1$ in place of q is $w_1 \cdots w_q w_{q+1}$. Thus the number of $3(q+1)$-tuples where (4.7) holds, but not with $q+1$ in place of q, is $w_1 \cdots w_q (v_{q+1}^3 - w_{q+1})$. Given such a $3(q+1)$-tuple, the number of choices for $r_{q+2}, \dots, r_l, \dots, t_{q+2}, \dots, t_l$ is $(v_{q+2} \cdots v_l)^3$, which is to be interpreted as 1 when $q = l-1$. Thus

$$|C_q| = w_1 \cdots w_q (v_{q+1}^3 - w_{q+1})(v_{q+2} \cdots v_l)^3 \tag{4.10}$$

for $0 \le q < l$, where the right hand side is to be interpreted as $(v_1^3 - w_1)(v_1 \cdots v_l)^3$ when $q = 0$ and $w_1 \cdots w_{l-1}(v_l^3 - w_l)$ when $q = l-1$.

Given $\mathbf{r}, \mathbf{s}, \mathbf{t}$, let $N(\mathbf{r}, \mathbf{s}, \mathbf{t}; \varepsilon)$ be the number of triples i, j, k with $\rho_i \in R_{\mathbf{r}},\ \sigma_j \in S_{\mathbf{s}},\ \tau_k \in T_{\mathbf{t}}$ having (4.5). In order to finish the proof of Lemma 4.2 we require a sublemma.

Lemma 4.3. *Suppose that* $\mathbf{r}, \mathbf{s}, \mathbf{t}$ *belong to* C_q. *Then*

$$N(\mathbf{r}, \mathbf{s}, \mathbf{t}; \varepsilon) \le c(\chi, m_0) \varepsilon^\chi n^3 p^{(q-1)\chi} (v_1 \cdots v_l)^{\chi - 3} \tag{4.11}$$

Proof. Numbers $\xi \in m^{-1}\mathbb{Z}$ may be uniquely written as

$$\xi = \frac{y}{m_0} + \frac{z}{p^l} = \xi' + \xi''$$

with $y, z \in \mathbb{Z}$ and $0 \le z < p^l$. For $\rho_i \in R_{\mathbf{r}}$, write $\rho_i = \rho_i' + \rho_i''$ as above. Now $m_0 = x_l$, so $\rho_i \overset{m_0}{\sim} \rho_j$ for each $\rho_i, \rho_j \in R_{\mathbf{r}}$, hence ρ_i'' is the same for every $\rho_i \in R_{\mathbf{r}}$. Using the same argument for $S_{\mathbf{s}}$ and $T_{\mathbf{t}}$ we have

$$\rho_i = \rho_i' + \rho'', \quad \sigma_j = \sigma_j' + \sigma'', \quad \tau_k = \tau_k' + \tau''$$

for $\rho_i \in R_{\mathbf{r}}$, $\sigma_j \in S_{\mathbf{s}}$, and $\tau_k \in T_{\mathbf{t}}$. Since $\mathbf{r}, \mathbf{s}, \mathbf{t} \in C_q$, we have $x_q(\rho_i - \sigma_j) = m_o p^{l-q}(\rho_i - \sigma_j) \in \mathbb{Z}$, hence $p^{l-q}(\rho'' - \sigma'') \in \mathbb{Z}$ and similarly $p^{l-q}(\rho'' - \tau'') \in \mathbb{Z}$. However, when $q < l$, then (4.7) does not hold with $q+1$ in place of q, so that not both $x_{q+1}(\rho_i - \sigma_j),\ x_{q+1}(\rho_i - \tau_k)$ lie in

$\mathbb{Z}$, hence not both of $p^{l-q-1}(\rho''-\sigma'')$, $p^{l-q-1}(\rho''-\tau'')$ are in $\mathbb{Z}$. Thus if a'' and b'' are the denominators of $\rho''-\sigma''$ and $\rho''-\tau''$ respectively, we have

$$\operatorname{lcm}(a'',b'')=p^{l-q} \tag{4.12}$$

Let $R'_{\mathbf{r}}$ be the homogeneous system consisting of the ρ'_i where $\rho_i \in R_{\mathbf{r}}$ and define $S'_{\mathbf{s}}$ and $T'_{\mathbf{t}}$ similarly. Clearly $R'_{\mathbf{r}} \cong R_{\mathbf{r}}$, $S'_{\mathbf{s}} \cong S_{\mathbf{s}}$ and $T'_{\mathbf{t}} \cong T_{\mathbf{t}}$, hence $R'_{\mathbf{r}} \cong S'_{\mathbf{s}} \cong T'_{\mathbf{t}}$. Moreover $R'_{\mathbf{r}} \overset{m_0}{\equiv} S'_{\mathbf{s}} \overset{m_0}{\equiv} T'_{\mathbf{t}}$. For $(\rho'_i,\sigma'_j,\tau'_k) \in R'_{\mathbf{r}} \times S'_{\mathbf{s}} \times T'_{\mathbf{t}}$, let a'_{ij}, b'_{ik} be the denominators of $\rho'_i-\sigma'_j$ and $\rho'_i-\tau'_k$ respectively. Then $a_{ij}=a'_{ij}a''$ and $b_{ik}=b'_{ik}b''$. Since $p \nmid a'_{ij}b'_{ij}$,

$$\operatorname{lcm}(a_{ij},b_{ik})=p^{l-q}\operatorname{lcm}(a'_{ij},b'_{ik})$$

by (4.12). Thus (4.5) becomes

$$\operatorname{lcm}(a'_{ij},b'_{ik}) \le \varepsilon p^{q-l}n = \varepsilon p^{q-l}v_1\cdots v_l\frac{n}{v_1\cdots v_l}. \tag{4.13}$$

We supposed Lemma 4.2 to be true for m_0, thus we can apply it to $R'_{\mathbf{r}}, S'_{\mathbf{s}}, T'_{\mathbf{t}}$ with $\varepsilon p^{q-l}v_1\cdots v_l$ in place of ε. Now each of these three systems has cardinality $n/(v_1\cdots v_l)$. Thus

$$\begin{aligned} N(\mathbf{r},\mathbf{s},\mathbf{t};\varepsilon) &\le c(\chi,m_0)(\varepsilon p^{q-l}v_1\cdots v_l)^{\chi}\left(\frac{n}{v_1\cdots v_l}\right)^3 \\ &= c(\chi,m_0)\varepsilon^{\chi}n^3p^{(q-l)\chi}(v_1\cdots v_l)^{\chi-3}. \end{aligned}$$

□

We can now continue with the proof of Lemma 4.2. Note that

$$N(\varepsilon)=\sum_{\mathbf{r}}\sum_{\mathbf{s}}\sum_{\mathbf{t}}N(\mathbf{r},\mathbf{s},\mathbf{t};\varepsilon)$$

so, by Lemma 4.3,

$$N(\varepsilon) \le c(\chi,m_0)\varepsilon^{\chi}n^3(v_1\cdots v_l)^{\chi-3}\sum_{q=0}^{l}|C_q|p^{(q-l)\chi}. \tag{4.14}$$

We see, by (4.9) and (4.10), that, for $1 \le q \le l$, $|C_{q-1}|,\ldots,|C_l|$ depend on w_q. As w_q increases $|C_{q-1}|$ decreases, unless it is zero, while $|C_q|,\ldots,|C_l|$ will increase, unless they are zero, but the sum $|C_{q-1}|+\cdots+|C_l|$ is constant. Since the coefficient $p^{(q-1-l)\chi}$ of $|C_{q-1}|$

is smaller than the coefficients of $|C_q|, \ldots, |C_l|$, the sum in (4.14) can only increase as w_q increases. Since $0 \le w_q \le v_q$ the sum in (4.14) is bounded by

$$(v_1^3 - v_1)(v_2 \cdots v_l)^3 p^{-l\chi} + v_1(v_2^3 - v_2)(v_3 \cdots v_l)^3 p^{-(l-1)\chi} + \cdots + (v_1 \cdots v_{l-1})(v_l^3 - v_l)p^{-\chi} + v_l \cdots v_l.$$

Then we can conclude

$$N(\varepsilon) \le c(\chi, m_0)\varepsilon^\chi n^3 f(1, v_1, \ldots, v_l) \le c(\chi, m_0)\varepsilon^\chi n^3 f(\gamma, v_1, \ldots, v_l)$$

where $\gamma = c(\chi, p) = (1 - p^{\chi-2})^{-1}$ and

$$f(\lambda, v_1, \ldots, v_l) = (v_1 \cdots v_l)^{\chi-2}\left(\lambda + \frac{v_l^2 - 1}{p^\chi} + \frac{v_{l-1}^2 - 1}{p^{2\chi}}v_l^2 + \cdots + \frac{v_1^2 - 1}{p^{l\chi}}(v_2 \cdots v_l)^2\right).$$

In order to finish the proof of Lemma 4.2, and hence Theorem 4.2, it remains to show that, for $1 \le q \le l$, when $1 \le v_q \le p$ we have

$$f(\gamma, v_1, \ldots, v_l) \le \gamma = c(\chi, p), \tag{4.15}$$

since $c(\chi, p)c(\chi, m_0) = c(\chi, pm_0) \le c(\chi, p^l m_0) = c(\chi, m)$. We will establish (4.15) by induction on l. When $l = 1$ or when $l > 1$ and $v_1, \ldots, v_{l-1}$ are given, $f(\gamma, v_1, \ldots, v_l)$ has the form

$$Av_l^\chi + Bv_l^{\chi-2}$$

with $A, B > 0$. This equation is first decreasing and then increasing in $v_l > 0$, thus its maximum on any closed interval of positive reals occurs at an end point. For $l = 1$ we have

$$f(\gamma, 1) = \gamma,$$
$$f(\gamma, p) = 1 + \gamma p^{\chi-2} - p^{-2} < 1 + \gamma p^{\chi-2} = \gamma$$

establishing (4.15) for $l = 1$. Now assume (4.15) for $l - 1$, where $l > 1$. We have, by induction,

$$\begin{aligned} &f(\gamma, v_1, \ldots, v_{l-1}, 1) \\ &\quad = (v_1 \cdots v_{l-1})^{\chi-2}\left(\gamma + \frac{v_{l-1}^2 - 1}{p^{2\chi}} + \cdots + \frac{v_1^2 - 1}{p^{l\chi}}(v_1 \cdots v_{l-1})^2\right) \\ &\quad \le f(\gamma, v_1, \ldots, v_{l-1}) \le \gamma, \end{aligned}$$

$$\begin{aligned} &f(\gamma, v_1, \ldots, v_{l-1}, p) \\ &\quad = (v_1 \cdots v_{l-1})^{\chi-2}\left(1 + \gamma p^{\chi-2} - p^{-2} + \frac{v_{l-1}^2 - 1}{p^\chi} + \cdots + \frac{v_1^2 - 1}{p^{(l-1)\chi}}(v_1 \cdots v_{l-1})^2\right) \\ &\quad \le f(\gamma, v_1, \ldots, v_{l-1}) \le \gamma, \end{aligned}$$

since $1 + \gamma p^{\chi-2} - p^{-2} < \gamma$, establishing our result. □

We will now state a Corollary to Theorem 4.1 that will be necessary in establishing the main result in this report. For R a system as above, we say that a triple of integers i, j, k is ε-*bad* if (4.2) holds. It is easy to check that this property is independent of the ordering. Let $l \geq 3$ and consider l-tuples of integers $u_1, \ldots, u_l$ in $1 \leq u_1, \ldots, u_l \leq n$. We call such an l-tuple ε-*bad* if some triple u_i, u_j, u_k with distinct i, j, k is ε-bad.

Corollary 4.1. *Suppose that $R = \{\rho_1, \ldots, \rho_n\}$ is homogeneous. Then for any $l \geq 3$, the number of ε-bad l-tuples $u_1, \ldots, u_l$ is*

$$< \varepsilon^{1/2} l^3 n^l.$$

Proof. By taking $\chi = 1/2$ in Theorem 4.1, the number of ε-bad triples is

$$\leq \zeta\left(\frac{3}{2}\right) \varepsilon^{1/2} n^3 < 3\varepsilon^{1/2} n^3.$$

Hence given a triple i, j, k with $1 \leq i < j < k \leq l$, the number of l-tuples $u_1, \ldots, u_l$ for which u_i, u_j, u_k is ε-bad is $< 3\varepsilon^{1/2} n^3 n^{l-3} = 3\varepsilon^{1/2} n^l$. The number of distinct triples i, j, k in $1 \leq i, j, k \leq l$ is $\binom{l}{3}$, so the number of ε-bad l-tuples is

$$\leq 3\binom{l}{3} \varepsilon^{1/2} n^l < \varepsilon^{1/2} l^3 n^l.$$

□

4.2 Denominators of rational numbers and ε-unpleasant l-tuples

Take positive integer q and let R be the system of numbers u/q with $1 \leq u \leq q$ and $\gcd(u, q) = 1$. This system has $n = \phi(q)$ elements, say $R = \{\rho_1, \ldots, \rho_n\}$. As in the last section, for $1 \leq i, j \leq n$, r_{ij} will denote the denominator of $\rho_i - \rho_j$.

In this section we will be concerned with the number of triples $1 \leq i, j, k \leq n$, for this particular system R and $\varepsilon > 0$, such that

$$\operatorname{lcm}(r_{ij}, r_{ik}) \leq \varepsilon q, \tag{4.16}$$

which will be denoted $M(\varepsilon)$.

Theorem 4.3. *For $0 < \kappa < 1$, there is a constant, $c(\kappa)$, depending only on κ such that*

$$M(\varepsilon) \le c(\kappa)\varepsilon^{\kappa} n^3. \tag{4.17}$$

And, in particular, when $\kappa = 1/2$ we may take $c(\kappa) = 11$.

Proof. First note that when $\varepsilon \ge 1/2$, we have $\varepsilon^{\kappa} > 1/2$, so trivially $M(\varepsilon) \le n^3 < 2\varepsilon^{\kappa} n^3$. Hence we may assume $0 < \varepsilon < 1/2$.

For $1 \le u, v, w \le q$ with $\gcd(u, q) = \gcd(v, q) = \gcd(w, q) = 1$, the least common denominator of $u/q - v/q$ and $u/q - w/q$ is q/d, where $d = \gcd(u - v, u - w, q)$. So if S denotes the set of numbers z in $1 \le z \le q$ with $\gcd(z, q) = 1$, then $M(\varepsilon)$ is the number of triples $u, v, w \in S$ with

$$\gcd(u - v, u - w, q) \ge 1/\varepsilon. \tag{4.18}$$

When $\gcd(r, q) = 1$, the left hand side of (4.18) is unchanged if u, v, w are replaced by numbers congruent to $ru, rv, rw \pmod q$. It follows that $M(\varepsilon) = nM_1(\varepsilon)$, where $M_1(\varepsilon)$ is the number of pairs $v, w \in S$ with

$$\gcd(1 - v, 1 - w, q) \ge 1/\varepsilon$$

Given positive integer h, let $M_2(h)$ be the number of pairs $v, w \in S$ such that

$$h | \gcd(1 - v, 1 - w, q). \tag{4.19}$$

Then

$$M_1(\varepsilon) \le \sum_{h \ge 1/\varepsilon} M_2(h) = \sum_{\substack{h | q \\ h \ge 1/\varepsilon}} M_2(h).$$

It is not too difficult to show that, for $0 < \kappa < 1$, the Euler totient function satisfies $\phi(h) \ge c_1(\kappa) h^{(1+\kappa)/2}$, where $c_1(\kappa)$ is a constant depending on κ, see for instance [9] pg. 267-268. In particular if we take $\kappa = 1/2$ we may take $c_1(1/2) = (2/27)^{(1/4)}$. To see this first write $h = p_1^{e_1} \cdots p_s^{e_s}$, where p_i are the distinct prime factors of h and each $e_i \ge 1$, then

$$\begin{aligned}
\phi(h) &= h \prod_{i=1}^{s} (1 - p^{-1}) \\
&= \frac{p_1^{e_1/4}(p_1 - 1)}{p_1} \cdots \frac{p_s^{e_s/4}(p_s - 1)}{p_s} h^{3/4} \\
&\ge \frac{2^{1/4} \cdot 1}{2} \frac{3^{1/4} \cdot 2}{3} h^{3/4} \\
&= \left(\frac{2}{27}\right)^{1/4} h^{3/4}.
\end{aligned}$$

Suppose $h|q$ and let h', q' denote their respective square free parts. Note that $\phi(q)/q = \phi(q')/q'$ and $\phi(h)/h = \phi(h')/h'$. Define t, t' by $q = ht$ and $q' = h't'$, so that $\phi(q') = \phi(h')\phi(t')$. This yields

$$\begin{aligned}(\phi(t')/t')(q/h) &= (\phi(q')/\phi(h'))(t/t') \\ &= (\phi(q)/\phi(h))(q'/q)(h/h')(t/t') \\ &= \phi(q)/\phi(h) \\ &\leq c_1(\kappa)^{-1}\phi(q)h^{-(1+\kappa)/2} \\ &= c_1(\kappa)^{-1}nh^{-(1+\kappa)/2}.\end{aligned} \tag{4.20}$$

Now (4.19) yields $v = 1 + hx$, for some positive integer x. Moreover since $v \in S$ we must have $0 \leq x < q/h$ and $\gcd(1 + hx, q) = 1$. Now $\gcd(1 + hx, q) = 1$ implies $\gcd(1 + hx, t') = 1$ and since $\gcd(h, t') = 1$, we can have at most $\phi(t')$ values for x in an interval of length t', hence $(\phi(t')/t')(q/h)$ values for x in $0 \leq x < q/h$. This is the number of possibilities for v, and similarly for w. Thus

$$M_2(h) = ((\phi(t')/t')(q/h))^2 \leq c_1(\kappa)^{-2}n^2h^{-1-\kappa}$$

by (4.20), which then yields

$$M_1(\varepsilon) \leq c_1(\kappa)^{-2}n^2 \sum_{h \geq 1/\varepsilon} h^{-1-\kappa}. \tag{4.21}$$

Since $0 < \varepsilon < 1/2$ the sum in (4.21) may be estimated by an integral from $1/\varepsilon - 1$ to ∞, and since $1/\varepsilon - 1 \geq 1/(2\varepsilon)$, we have

$$\int_{1/\varepsilon - 1}^{\infty} h^{-1-\kappa}\mathrm{d}h \leq \int_{1/(2\varepsilon)}^{\infty} h^{-1-\kappa}\mathrm{d}h = \kappa^{-1}(2\varepsilon)^{\kappa},$$

which yields

$$M(\varepsilon) = nM_1(\varepsilon) \leq c_1(\kappa)^{-2}\kappa^{-1}2^{\kappa}\varepsilon^{\kappa}n^3.$$

When $\kappa = 1/2$, the value of $c_1(1/2)$ given above yields

$$M_1(\varepsilon) \leq (27/2)^{1/2}2^{1+1/2}\varepsilon^{1/2}n^3 < 11\varepsilon^{1/2}n^3.$$

□

For our particular system R we will call a triple i, j, k in $1 \leq i, j, k \leq n$ *ε-unpleasant* if (4.16) holds. When $l \geq 3$ and $u_1, \ldots, u_l$ is an l-tuple of integers with $1 \leq u_1, \ldots, u_l \leq n$, we call this l-tuple *ε-unpleasant* if some triple u_i, u_j, u_k, with distinct i, j, k, is ε-unpleasant.

Corollary 4.4. *The number of such ε-unpleasant l-tuples is*

$$< 2\varepsilon^{1/2} l^3 n^l.$$

Proof. By the case $\kappa = 1/2$ of Theorem 4.3, the number of ε-unpleasant triples is $< 11\varepsilon^{1/2} n^3$. Thus given i, j, k with $1 \leq i < j < k \leq l$, the number of l-tuples $u_1, \ldots, u_l$ for which u_i, u_j, u_k is ε-unpleasant is $< 11\varepsilon^{1/2} n^3 n^{l-3} = 11\varepsilon^{1/2} n^l$. The number of such triples i, j, k is $\binom{l}{3}$, hence the number of ε-unpleasant l-tuples is

$$< 11\binom{l}{3}\varepsilon^{1/2} n^l < 2\varepsilon^{1/2} l^3 n^l.$$

□

Chapter 5

Recurrences of Order t

In this chapter we investigate linear recurrence sequences or arbitrary order. In §5.1 we give a bound for rational recurrence sequences depending only on the order of the recurrence sequence. The remainder of the chapter will then be devoted to proving that *any* linear recurrence sequence has zero multiplicity bounded by a constant depending only on its order. With the exception of Theorem 5.1 and Lemma 5.7 we follow Schmidt's papers [17] and [18].

5.1 Rational recurrences

Our main problem in dealing with arbitrary linear recurrences of order t is that, in the algebraic case, the logarithmic heights of the numbers involved can be arbitrarily small. If we assume that our recurrence sequence is rational then we do not have this problem and we have the following.

Theorem 5.1. *Let $\{u_n\}_{n\in\mathbb{Z}}$ be a rational linear recurrence sequence of order t and let $\mathcal{Z} = \{n \in \mathbb{Z} : u_n = 0\}$. Then the set $\mathcal{Z}$ can be written as the union of fewer than*

$$t^{25t^3}$$

single numbers and arithmetic progressions.

Proof. We know, by Theorem 1.1, that if the companion polynomial to our recurrence factors as

$$\prod_{i=1}^{k}(z-\alpha_i)^{t_i},$$

then there are polynomials $P_i(z) \in \mathbb{C}[z]$, with $\deg P_i = t_i - 1$, such that

$$u_n = P_1(n)\alpha_1^n + \cdots + P_k(n)\alpha_k^n,$$

for all $n \in \mathbb{Z}$. Hence we will be interested in the equation

$$P_1(x)\alpha_1^x + \cdots + P_k(x)\alpha_k^x = 0 \tag{5.1}$$

in $x \in \mathbb{Z}$. Now all numbers involved lie in the splitting field, K, of a polynomial of degree t with rational coefficients. Hence $d = [K : \mathbb{Q}] \leq t! < t^t$. We define $t = t(P_1, \ldots, P_k)$ by

$$t(P_1, \ldots, P_n) = \sum_{i=1}^{k} (\deg P_i + 1).$$

First assume $\{u_n\}_{n\in\mathbb{Z}}$ is nondegenerate. Note that this implies $|\mathcal{Z}|$ is finite. If $t \leq 2$ then there will be at most one solution so we may assume $t \geq 3$. In this case we can apply a result of Schlickewei and Schmidt [16] and, in particular, by Theorem 2.1 of [16] we have

$$|\mathcal{Z}| < (2t)^{35t^2} d^{6t^2} < (2t)^{35t^2} t^{6t^3} < t^{25t^3}.$$

Now assume that there is some $i \neq j$ such that α_i/α_j is a root of unity. If $t = 2$ again the result is trivial as $\mathcal{Z}$ will consist of a single arithmetic progression of modulus $\mathrm{ord}(\alpha_1/\alpha_2)$. Here and throughout this chapter we denote by $\mathrm{ord}(\zeta)$ the smallest positive integer q such that $\zeta^q = 1$, for root of unity ζ. We will proceed by induction on $t \geq 3$. Without loss of generality we may assume α_k/α_{k-1} is a root of unity. Let $q = \mathrm{ord}(\alpha_k/\alpha_{k-1})$, since $[\mathbb{Q}(\alpha_i, \alpha_j) : \mathbb{Q}] \leq t(t-1)$ we see that $q < t^2$. We divide $\mathbb{Z}$ into the arithmetic progressions $\mathcal{A}(q, b)$, with $0 \leq b < q$. Hence a solution x of (5.5) has the form $x = qy + b$ for some $y \in \mathbb{Z}$ and $0 \leq b < q$. We then set $\hat{\alpha}_i = \alpha_i^q$, for $1 \leq i \leq k-1$, $\hat{P}_i(y) = \alpha_i^b P_i(qy + b)$, for $1 \leq i \leq k-2$, and $\hat{P}_{k-1}(y) = \alpha_{k-1}^b P_{k-1}(qy + b) + \alpha_k^b P_k(qy + b)$. We have the equation

$$\hat{P}_1(y)\hat{\alpha}_1^y + \cdots + \hat{P}_{k-1}(y)\hat{\alpha}_{k-1}^y = 0. \tag{5.2}$$

Now $t(\hat{P}_1, \ldots, \hat{P}_{k-1}) < t(P_1, \ldots, P_k)$ so by induction the solutions of (5.2) are the union of at most

$$(t-1)^{25(t-1)^3}$$

single numbers and arithmetic progressions. Summing over $0 \leq b < q$ we see that $\mathcal{Z}$ can be written as the union of fewer than

$$t^2(t-1)^{25(t-1)^3} < t^{25t^3}$$

single numbers and arithmetic progressions. □

5.2 Main results

In this chapter we deal with linear recurrences of order t, where t is an arbitrary positive integer. A long standing problem, arguably the most important one in the theory of linear recurrence sequences was whether or not the zero-multiplicity of an arbitrary linear recurrence sequence of complex numbers could be bounded by a function depending on t alone. In [15] Schlickewei showed that if $\{u_n\}_{n\in\mathbb{Z}}$ is a non-degenerate algebraic linear recurrence sequence of order t contained in a number field K of degree d then its zero-multiplicity is bounded by a function depending only on t and d. In [8] Evertse, Schlickewei and Schmidt show that the zero multiplicity of any simple non-degenerate linear recurrence sequence is bounded by a function depending only on its order. In [17] Schmidt was able to remove the condition that the recurrence has to be simple. Schmidt [18] then generalised this, in a suitable manner, to all linear recurrence sequences. The remainder of this chapter will be devoted to establishing this result. It is important to note that the main result in [8] is vital in what follows and it in turn relies heavily on a quantitative version of Schmidt's subspace theorem due to Evertse and Schlickewei in [7]. Our main result is the following.

Theorem 5.2. *Let $\{u_n\}_{n\in\mathbb{Z}} \subset \mathbb{C}$ be a linear recurrence sequence of order t and let $\mathcal{Z} = \{n \in \mathbb{Z} : u_n = 0\}$. The set $\mathcal{Z}$ can be taken to be the union of not more than*

$$\exp\exp\exp(3\sqrt{t}\log t) \tag{5.3}$$

single numbers and arithmetic progressions. Also if the companion polynomial to $\{u_n\}_{n\in\mathbb{Z}}$ has k distinct roots, each with multiplicity not exceeding s then (5.3) *can be replaced by*

$$\exp\exp(10sk^s\log k). \tag{5.4}$$

In particular if $\alpha_1, \ldots, \alpha_k$ are the distinct roots of the companion polynomial and there is some $1 \le i_0 \le k$ with α_{i_0}/α_j not a root of unity for every $1 \le j \le k$ with $j \ne i_0$ then we know by Corollary 1.3 that $|\mathcal{Z}|$ is finite and thus is bounded above by (5.3) and (5.4).

Here we have improved Schmidt's result in [18] by lowering the constant from 30 to 10 in (5.4) and by replacing $20t$ with $3\sqrt{t}\log t$ in (5.3). The key change in our argument is an improvement of Lemma 5.7 in which we show that for a certain collection of vectors the number of tuples of linearly independent vectors is bounded by $t^{\sqrt{2t}}$, where in [18] Schmidt provided a bound of e^{12t}.

It will be useful to introduce the notation $\alpha \sim \beta$, for $\alpha, \beta \in \mathbb{C}^\times$, if α/β is a root of unity. This is obviously an equivalence relation on $\mathbb{C}^\times$. Throughout this chapter we will use $h(\beta)$ to denote the absolute logarithmic height of an algebraic number β, as defined in §1.2.

Let $\mathcal{P}(z) \in \mathbb{C}[z]$ be the companion polynomial to the recurrence sequence $\{u_n\}_{n\in\mathbb{Z}} \subset \mathbb{C}$ of order t. Say

$$\mathcal{P}(z) = \prod_{i=1}^{k} (z - \alpha_i)^{t_i},$$

for $\alpha_1, \ldots, \alpha_k$ distinct. Then, by Theorem 1.1, there exists polynomials $P_i(z) \in \mathbb{C}[z]$, with $\deg P_i = t_i - 1$, such that

$$u_n = P_1(n)\alpha_1^n + \cdots + P_k(n)\alpha_k^n,$$

for all $n \in \mathbb{Z}$. Throughout this chapter we investigate the solutions of

$$P_1(x)\alpha_1^x + \cdots + P_k(x)\alpha_k^x = 0 \tag{5.5}$$

in $x \in \mathbb{Z}$.

If $\mathcal{Z} \subset \mathbb{Z}$ can be written as a finite union of single numbers and arithmetic progression then we set

$$\nu(\mathcal{Z}) = \min\{u + v : \mathcal{Z} \text{ can be written as the union of } u \text{ numbers and } v \text{ progressions}\},$$

otherwise we set $\nu(\mathcal{Z}) = \infty$. Thus the goal of this chapter is to show that if $\mathcal{Z}$ is the set of integers satisfying (5.5) then $\nu(\mathcal{Z})$ is bounded by (5.3) and (5.4).

In order to work with (5.5) we first prove a specialisation argument that allows us to assume the α_i and the coefficients of the P_i are all algebraic. The first main step in our proof is Lemma 5.6, which gives us an avenue for induction provided that there is a real number $h^* > 0$ and $1 \le i, j \le k$ with $h(\alpha_i/\alpha_j) > h^*$. This Lemma however introduces a constant that depends not only on t but on h^*. Clearly it is impossible to find one such h^* to apply to all linear recurrence sequences $\{u_n\}_{n\in\mathbb{Z}} \subset \overline{\mathbb{Q}}$.

To get around this we first write

$$P_i(x) = a_{i1} + \cdots + a_{is}x^{s-1}.$$

We then define the linear forms $N_1(\mathbf{X}), \ldots, N_s(\mathbf{X})$, in $\mathbf{X} = (X_1, \ldots, X_k)$, by

$$N_j(\mathbf{X}) = a_{1j}X_1 + \cdots + a_{kj}X_k.$$

Then (5.5) may be rewritten as

$$\sum_{j=1}^{s} N_j(\alpha_1^x, \ldots, \alpha_k^x)x^{j-1} = 0. \tag{5.6}$$

If the α_i and a_{ij} are in a number field K of degree D then we consider the D embeddings $K \hookrightarrow \mathbb{C}$. We let $\beta^{(\sigma)}$ denote the image of $\beta \in K$ under the embedding $\sigma : K \hookrightarrow \mathbb{C}$ and

$$N_j^{(\sigma)}(\mathbf{X}) = a_{1j}^{(\sigma)} X_1 + \cdots + a_{kj}^{(\sigma)} X_k.$$

Then applying σ to (5.6) we see that

$$\sum_{j=1}^{s} N_j^{(\sigma)}(\alpha_1^{(\sigma)x}, \ldots, \alpha_k^{(\sigma)x}) x^{j-1} = 0.$$

Then for any embeddings $\sigma_1, \ldots, \sigma_s$ the determinant of the $s \times s$ matrix with entries $N_j^{(\sigma_i)}(\alpha_1^{(\sigma_i)x}, \ldots, \alpha_k^{(\sigma_i)x})$ must vanish, i.e.

$$|[N_j^{(\sigma_i)}(\alpha_1^{(\sigma_i)x}, \ldots, \alpha_k^{(\sigma_i)x})]_{1 \le i,j \le s}| = 0. \tag{5.7}$$

We prove a proposition stating that all solutions $x \in \mathbb{Z}$ of (5.7) can be divided up into a finite number of classes, depending only on $T = \min\{k^s, t^{\sqrt{2t}}\}$, and in each of these classes there is a positive integer m such that any two solutions in the class are congruent modulo m and there are $i \neq j$ with either $h(\alpha_i^m/\alpha_j^m) > h^*$ or $\alpha_i \sim \alpha_j$ and $\mathrm{ord}(\alpha_i^m/\alpha_j^m) \le (h^*)^{-1}$, where h^* depends only on T. By looking at the solutions in a given class we can replace the α_i in (5.5) with α_i^m and apply an induction argument, the case of $\alpha_i \sim \alpha_j$ being straightforward while the case $\alpha_i \not\sim \alpha_j$ requiring the aforementioned Lemma. Since all of the constants involved depend only on T or on $t < T$ we can get a bound depending only on T, which will yield (5.3) and (5.4).

The hard part, as it turns out, is in proving this proposition mentioned above and most of this chapter is devoted to doing just that. Moreover it is for this result that we need Corollaries 4.1 and 4.4 of Chapter 4.

5.3 Specialisation

For $a, b \in \mathbb{Z}$ with $a > 0$ we denote the arithmetic progression $\{ax + b : x \in \mathbb{Z}\}$ by $\mathcal{A}(a, b)$. It is important to note that $\mathcal{Z} \subseteq \mathcal{Z}'$ does not in general imply $\nu(\mathcal{Z}) \le \nu(\mathcal{Z}')$. It is for this reason that we require the following lemma.

Lemma 5.1. *Suppose $\nu(\mathcal{Z})$ is finite. Then there exists a finite, possibly empty, set $\mathcal{T} \subset \mathbb{Z}$ with $\mathcal{Z} \cap \mathcal{T} = \emptyset$ such that every set $\mathcal{Z}' \supseteq \mathcal{Z}$ with $\mathcal{Z}' \cap \mathcal{T} = \emptyset$ has $\nu(\mathcal{Z}') \ge \nu(\mathcal{Z})$.*

Proof. Suppose that $\nu(\mathcal{Z}) = u + v$ and $\mathcal{Z} = \mathcal{Z}_1 \cup \mathcal{Z}_2$ with $|\mathcal{Z}_1| = u$ and $\mathcal{Z}_2$ the union of v arithmetic progressions. Since $u + v$ is minimum for $\mathcal{Z}$ we have that $\mathcal{Z}_1 \cap \mathcal{Z}_2 = \emptyset$ and $\nu(\mathcal{Z}_2) = v$.

Say $\mathcal{Z}_1 = \{n_1, \dots, n_u\}$. When $u = 0$ or $u = 1$ we set $\mathcal{T}_1 = \emptyset$. When $u > 1$ and $n_i < n_j$ we note that $\mathcal{A}(n_j - n_i, n_i) \not\subseteq \mathcal{Z}$, since if it was then we would have $\mathcal{A}(n_j - n_i, n_i) \subseteq \mathcal{Z}_2$. In particular this would imply $n_i, n_j \in \mathcal{Z}_2$ and we could remove n_i, n_j from $\mathcal{Z}_1$ contradicting the minimality of $\nu(\mathcal{Z})$. Hence, for each $n_i < n_j$, with $1 \le i, j \le u$, we can take some $t_{ij} \in \mathcal{A}(n_j - n_i, n_i)$ such that $t_{ij} \notin \mathcal{Z}$. Set $\mathcal{T}_1 = \cup\{t_{ij}\}$. We now remark that any arithmetic progression $\mathcal{A}$ with $\mathcal{A} \cap \mathcal{T}_1 = \emptyset$ contains at most one element of $\mathcal{Z}_1$. Thus when $v = 0$ the lemma holds with $\mathcal{T} = \mathcal{T}_1$.

Now assume $v > 0$ and let $\mathcal{Z}_2$ be the union of arithmetic progressions $\mathcal{A}(a_i, b_i)$, $1 \le i \le v$. Set $q = \operatorname{lcm}(a_1, \dots, a_v)$. Note that whenever $n \in \mathcal{Z}_2$ then $\mathcal{A}(q, n) \subseteq \mathcal{Z}_2$, we call q the *period* of $\mathcal{A}$. Let $l = qv$ and, if necessary, translate $\mathcal{Z}$ so that $[1, ql] \cap \mathcal{Z}_1 = \emptyset$. Define $\mathcal{T}_2$ by

$$\mathcal{T}_2 = \{n \in [1, ql] : n \notin \mathcal{Z}\}.$$

Suppose $\mathcal{A}$ is an arithmetic progression of modulus $a \le l$. Consider the elements $b, b + a, \dots, b + (q-1)a \in \mathcal{A}$ with $1 \le b \le a$. If each of these is in $\mathcal{Z}_2$ then, since $\mathcal{Z}$ has period q, we have $\mathcal{A} \subseteq \mathcal{Z}_2$. If we have $\mathcal{A} \not\subseteq \mathcal{Z}_2$ then at least one of $b, b + a, \dots, b + (q-1)a$ is in $\mathcal{T}_2$. Hence every arithmetic progression $\mathcal{A}$ with modulus $a \le l$ such that $\mathcal{A} \cap \mathcal{T}_2 = \emptyset$ is contained in $\mathcal{Z}_2$.

Set $\mathcal{T} = \mathcal{T}_1 \cup \mathcal{T}_2$. Suppose that $\mathcal{Z}' \supseteq \mathcal{Z}$ with $\mathcal{Z}' \cap \mathcal{T}$ is the union of u' numbers and v' arithmetic progressions. Say $\mathcal{Z}' = \mathcal{Z}'_1 \cup \mathcal{Z}'_2$ with $|\mathcal{Z}'_1| = u'$ and $\mathcal{Z}'_2$ is the union of the arithmetic progressions $\mathcal{A}'_i = \mathcal{A}'_i(a'_i, b'_i)$, for $1 \le i \le v'$. Note that $\mathcal{Z} \subseteq \mathcal{Z}'$ implies $\mathcal{Z}_2 \subseteq \mathcal{A}'_1 \cup \cdots \cup \mathcal{A}'_{v'}$. Our goal is to show

$$u + v \le u' + v'. \tag{5.8}$$

If $v' \ge u + v$ then we are done, and so we will assume henceforth that $v' < u + v$. If some $\mathcal{A}'_i$ is disjoint from $\mathcal{Z}_2$ then its intersection with $\mathcal{Z}$ is empty or contains a single element of $\mathcal{Z}_1$. In the first case we remove $\mathcal{A}'_i$ from $\mathcal{Z}'$ and in the second we replace it by this single element. We then have a set $\mathcal{Z}'' \supseteq \mathcal{Z}$ with $\mathcal{Z}'' \cup \mathcal{T} = \emptyset$ and $\nu(\mathcal{Z}'') \le (u' + 1) + (v' - 1) = \mathcal{Z}'$. Hence in order to establish (5.8) we may replace $\mathcal{Z}'$ with $\mathcal{Z}''$. Continuing in this manner we may assume that each $\mathcal{A}'_i$ intersects $\mathcal{Z}_2$.

Say $\mathcal{A}'_1, \dots, \mathcal{A}'_w$ have modulus $\le l$ and $\mathcal{A}'_{w+1}, \dots, \mathcal{A}'_{v'}$ have modulus $> l$, where $1 \le w \le v'$. For each $1 \le i \le w$, since $\mathcal{A}'_i = \mathcal{A}'_i(a'_i, b'_i)$ has $a'_i \le l$ and $\mathcal{A}'_i \cap \mathcal{T} = \emptyset$ we have that $\mathcal{A}'_i \subseteq \mathcal{Z}_2$. Since $a'_i x + b'_i \in \mathcal{Z}_2$ for every $x \in \mathbb{Z}$ and $\mathcal{Z}_2$ has period q, we have $a'_i x + b'_i + qy \in \mathcal{Z}_2$ for every $x, y \in \mathbb{Z}$. So if we set $a''_i = \gcd(a'_i, q)$, the progression $\mathcal{A}(a''_i, b'_i) \subseteq \mathcal{Z}_2$. Since $\mathcal{Z}_2 \subseteq \mathcal{A}'_1 \cup \cdots \cup \mathcal{A}'_{v'}$ this union will be unchanged if we replace $\mathcal{A}'_i$ with $\mathcal{A}''_i$ for each $1 \le i \le w$. Hence we may suppose that $a'_i | q$ for each $1 \le i \le w$.

We claim that $\mathcal{A}'_1 \cup \cdots \cup \mathcal{A}'_w = \mathcal{Z}_2$. If a set $\mathcal{X}$ is the union of finitely many numbers and arithmetic progressions we define the *density* of $\mathcal{X}$, denoted by $d(\mathcal{X})$, by

$$d(\mathcal{X}) = \lim_{n\to\infty} \frac{\mathcal{X} \cap [0, n]}{n}.$$

Note that the density of an arithmetic progression is simply the reciprocal of its modulus. Say $\mathcal{Z}_2$ has r elements per period of length q and $\mathcal{A}'_1 \cup \cdots \cup \mathcal{A}'_w$ has s elements per period of length q. Hence $\mathcal{Z}_2$ and $\mathcal{A}'_1 \cup \cdots \cup \mathcal{A}'_w$ have density r/q and s/q respectively. Note that since $\mathcal{A}'_1 \cup \cdots \cup \mathcal{A}'_w \subseteq \mathcal{Z}_2$ we must have $s \leq r$. The sequences $\mathcal{A}'_{w+1}, \ldots, \mathcal{A}'_{v'}$ each have density $< 1/l$. Thus

$$d(\mathcal{A}'_1 \cup \cdots \cup \mathcal{A}'_{v'}) < (s/q) + (v'/l).$$

Since $v' < \nu(\mathcal{Z})$

$$d(\mathcal{Z}') = d(\mathcal{Z}'_2) < \frac{s}{q} + \frac{\nu(\mathcal{Z})}{q\nu(\mathcal{Z})} = \frac{s+1}{q}.$$

Now $\mathcal{Z} \subseteq \mathcal{Z}'$ implies $d(\mathcal{Z}) \leq d(\mathcal{Z}')$, i.e $r/q \leq s/q$. But then $s \leq r < s+1$, hence $s = r$ and our claim is established.

This implies that $w \geq v$. Also, we must have $\mathcal{Z}_1 \subseteq \mathcal{Z}'_1 \cup \mathcal{A}'_{w+1} \cup \cdots \cup \mathcal{A}'_{v'}$. Since each $\mathcal{A}'_i$ contains at most one element of $\mathcal{Z}_1$ we have $(v' - w) + |\mathcal{Z}'_1| \geq |\mathcal{Z}_1|$, i.e. $v' - w + u' \geq u$. We then have $u + v \leq u + w \leq u' + v'$. □

Consider equation (5.5) and say, for $1 \leq i \leq k$,

$$P_i(z) = c_{i0} + \cdots + c_{id_i} z^{d_i}.$$

By Theorem 1.2 the set $\mathcal{Z}$ of $x \in \mathbb{Z}$ satisfying (5.5) has finite $\nu(\mathcal{Z})$. Construct the set $\mathcal{T}$ as in Lemma 5.1.

For any fixed $x \in \mathbb{Z}$, equation (5.5) defines an algebraic set, i.e. a set closed in the Zariski topology, $V(x)$ in the points $(\boldsymbol{\alpha}, \mathbf{c})$, where $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_k)$ and $\mathbf{c} = (c_{10}, \ldots, c_{kd_k})$. Now our particular $(\boldsymbol{\alpha}, \mathbf{c})$ lies in the algebraic set

$$V(\mathcal{Z}) = \bigcap_{n\in\mathcal{Z}} V(n).$$

Let W_0 be the hypersurface given by $\alpha_1 \cdots \alpha_k c_{1d_1} \cdots c_{kd_k} = 0$ and set

$$W(\mathcal{T}) = \left(\bigcup_{n\in\mathcal{T}} V(n) \right) \bigcup W_0.$$

Since $\mathcal{Z} \cap \mathcal{T} = \emptyset$ we have $(\boldsymbol{\alpha}, \mathbf{c}) \in V(\mathcal{Z}) \setminus W(\mathcal{T})$.

It is well known that since $V(\mathcal{Z}) \setminus W(\mathcal{T}) \neq \emptyset$ there exists a point $(\hat{\boldsymbol{\alpha}}, \hat{\mathbf{c}}) \in V(\mathcal{Z}) \setminus W(\mathcal{T})$ with coordinates in $\overline{\mathbb{Q}}$. To see this first note that since $V(\mathcal{Z})$ and $W(\mathcal{T})$ are defined by polynomials with coefficients in $\overline{\mathbb{Q}}$ then the ideals I and J in $\mathbb{C}[x_1, \dots, x_k, y_{10}, \dots, y_{kd_k}]$ of polynomials that vanish at all the points of $V(\mathcal{Z})$ and $W(\mathcal{T})$, respectively, are generated by a finite number of polynomials with coefficients in $\overline{\mathbb{Q}}$. Say I is generated by $f_1, \dots, f_r$ and J is generated by $g_1, \dots, g_s$. Let I' and J' be the ideals generated by $f_1, \dots, f_r$ and $g_1, \dots, g_s$ in $\overline{\mathbb{Q}}[x_1, \dots, x_k, y_{10}, \dots, y_{kd_k}]$, respectively. Now $V(\mathcal{Z}) \not\subseteq W(\mathcal{T})$ implies $J \not\subseteq I$. Since $I = \mathbb{C} \otimes I'$ and $J = \mathbb{C} \otimes J'$ we then have $J' \not\subseteq I'$. Let V' and W' be the algebraic sets in $\overline{\mathbb{Q}}$ space associated to the ideals I' and J'. Then $J' \not\subseteq I'$ implies $V' \not\subseteq W'$. Since V' is defined by the polynomials $f_1, \dots, f_r$ and W' is defined by the polynomials $g_1, \dots, g_s$ this implies that there is a point $(\hat{\boldsymbol{\alpha}}, \hat{\mathbf{c}})$, with coordinates in $\overline{\mathbb{Q}}$, such that $f_1(\hat{\boldsymbol{\alpha}}, \hat{\mathbf{c}}) = \cdots = f_r(\hat{\boldsymbol{\alpha}}, \hat{\mathbf{c}}) = 0$ but there is some g_i, $1 \leq i \leq s$, with $g_i(\hat{\boldsymbol{\alpha}}, \hat{\mathbf{c}}) \neq 0$. Hence $(\hat{\boldsymbol{\alpha}}, \hat{\mathbf{c}}) \in V(\mathcal{Z}) \setminus W(\mathcal{T})$. This point gives rise to an equation

$$\hat{P}_1(x)\hat{\alpha}_1^x + \cdots + \hat{P}_k(x)\hat{\alpha}_k^x = 0, \tag{5.9}$$

with, for each $1 \leq i \leq k$, $\alpha_i \neq 0$ and $\deg \hat{P}_i = \deg P_i$. Let $\mathcal{Z}'$ be the set of solutions in $x \in \mathbb{Z}$ to (5.9). Since $(\hat{\boldsymbol{\alpha}}, \hat{\mathbf{c}}) \in V(\mathcal{Z})$ we see that $\mathcal{Z}' \supseteq \mathcal{Z}$, but $(\hat{\boldsymbol{\alpha}}, \hat{\mathbf{c}}) \notin W(\mathcal{T})$, so no $n \in \mathcal{T}$ is a solution to (5.9). This implies that $\mathcal{Z}' \cap \mathcal{T} = \emptyset$ and Lemma 5.1 implies $\nu(\mathcal{Z}') \geq \nu(\mathcal{Z})$.

Hence it suffices to prove Theorem 5.2 under the assumption that the α_i and the coefficients of the P_i are all algebraic. We will henceforth assume that all these quantities lie in some number field K.

5.4 Some known results

In this section we give an overview of some known results necessary for the proof of our theorem.

Lemma 5.2. *Let $\alpha_1, \dots, \alpha_q, a_1, \dots, a_q \in \mathbb{C}^\times$ and suppose $\alpha_1 \sim \cdots \sim \alpha_q$. There are*

$$B(q) = q^{3q^2}$$

vectors $\mathbf{c}_l = (c_{l1}, \dots, c_{lq})$, $1 \leq l \leq B(q)$, such that if $x \in \mathbb{Z}$ satisfies

$$a_1\alpha_1^x + \cdots + a_q\alpha_q^x = 0, \tag{5.10}$$

but no proper subsum of (5.10) vanishes, then the vector $(\alpha_1^x, \dots, \alpha_q^x)$ is proportional to some $\mathbf{c}_l$.

Proof. Clearly we may suppose $q > 1$. Set $n = q - 1$, $\zeta_i = \alpha_i^x/\alpha_q^x$ and $b_i = -a_i/a_q$ for each $1 \leq i \leq n$. Then (5.10) becomes

$$b_1\zeta_1 + \cdots + b_n\zeta_n = 1, \tag{5.11}$$

where $\zeta_1, \ldots, \zeta_n$ are roots of unity. By a result of Evertse [6], (5.11) has at most $B(n+1) = B(q)$ solutions in roots of unity such that no subsum vanishes. If $\zeta_1, \ldots, \zeta_n$ is one such solution we see that $(\alpha_1, \ldots, \alpha_q)$ is proportional to $(\zeta_1, \ldots, \zeta_n, 1)$. □

Lemma 5.3. *Let Γ be a finitely generated subgroup of $(\mathbb{C}^\times)^q$ of rank r and let $a_1, \ldots, a_q \in \mathbb{C}^\times$. Up to a factor of proportionality the equation*

$$a_1x_1 + \cdots + a_qx_q = 0 \tag{5.12}$$

has at most

$$C(q, r) = \exp((r+1)(6q)^{3q})$$

solutions $\mathbf{x} = (x_1, \ldots, x_q) \in \Gamma$, such that no subsum of (5.12) vanishes.

Proof. Set $n = q - 1$, $b_i = -a_i/a_q$ and $y_i = x_i/x_q$ for $1 \leq i \leq n$. Then (5.12) becomes

$$b_1y_1 + \cdots + b_ny_n = 1, \tag{5.13}$$

where $(y_1, \ldots, y_n)$ is in a group Γ' of rank $\leq r$. Evertse, Schlickewei and Schmidt [8] have shown that (5.13), and hence equation (5.12), has at most

$$\exp((r+1)(6n)^{3n}) < \exp((r+1)(6q)^{3q})$$

solutions such that no proper subsum vanishes. It is worth noting that their result relies heavily on the quantitative version of the subspace theorem due to Evertse and Schlickewei [7]. □

We extend our definition of absolute logarithmic height to include vectors in both affine and projective space. For $\mathbf{x} = (x_1 : \cdots : x_{n+1}) \in \mathbb{P}^n$, where we are over the field $\overline{\mathbb{Q}}$, we define the *absolute logarithmic height* of $\mathbf{x}$, denoted $h_{\mathbb{P}^n}(\mathbf{x})$, by

$$h_{\mathbb{P}^n}(\mathbf{x}) = \sum_{v \in M_K} \log(\max\{|x_1|_v, \ldots, |x_q|_v\}),$$

where K is any field containing $x_1, \ldots, x_q$ and M_K is the set of places of K. Note that this is well defined on $\mathbb{P}^n$ due to the product formula. For a vector $\mathbf{x} = (x_1, \ldots, x_n) \in \overline{\mathbb{Q}}^n$ we define the *absolute logarithmic height* of $\mathbf{x}$, denoted $h_n(\mathbf{x})$, by

$$h_n(\mathbf{x}) = h_{\mathbb{P}^n}(x_1 : \cdots : x_n : 1).$$

Note that for $\alpha \in \overline{\mathbb{Q}}$ we have $h(\alpha) = h_{\mathbb{P}^n}(\alpha : 1) = h_n(\alpha)$.

Lemma 5.4. *Let $q > 1$ and Γ be a finitely generated group of $(\overline{\mathbb{Q}}^\times)^q$ of rank r. The solutions of*

$$z_1 + \cdots + z_q = 0, \tag{5.14}$$

with $z_i = x_i y_i$, where $\mathbf{x} = (x_1, \ldots, x_q) \in \Gamma$ and $\mathbf{y} = (y_1, \ldots, y_q) \in (\mathbb{Q}^\times)^q$ and

$$h_{\mathbb{P}^{q-1}}(\mathbf{y}) \leq \frac{1}{4q^2} h_{\mathbb{P}^{q-1}}(\mathbf{x}), \tag{5.15}$$

are contained in the union of not more than $C(q, r)$ proper subspaces of the $(q-1)$-dimensional space defined by (5.14).

Proof. Set $n = q - 1$ and consider solutions of the equation

$$z_1 + \cdots + z_n = 1, \tag{5.16}$$

where $z_i = u_i v_i$, with $\mathbf{u} = (u_1, \ldots, u_n) \in \Gamma'$, Γ' a subgroup of $(\overline{\mathbb{Q}}^\times)^n$ of rank $\leq r$, and $\mathbf{v} = (v_1, \ldots, v_n) \in (\mathbb{Q}^\times)^n$ with

$$h_n(\mathbf{v}) \leq \frac{1}{4n^2} h_n(\mathbf{u}). \tag{5.17}$$

If we can show that all such solutions of (5.16) are contained in the union of not more than $C(n, r)$ proper subspaces of $\overline{\mathbb{Q}}^n$ then our Lemma follows by setting $u_i = x_i/x_q$ and $v_i = -y_i/y_q$, for $1 \leq i \leq n$.

This inhomogenous version is a variation of Proposition A in [16]. First assume that $h_n(\mathbf{u}) > 2n \log n$. It was shown by Schlickewei and Schmidt [16] that these solutions lie in the union of fewer than

$$2^{30n^2}(21n^2)^r \tag{5.18}$$

proper subspaces.

Now assume $h_n(\mathbf{u}) \leq 2n \log n$. Then, by (5.17) we have $h_n(\mathbf{v}) \leq (2n \log n)/(4n^2) < \log 2$. This implies that for each $1 \leq i \leq n$ we have $h(v_i) < \log 2$, and since $y_i \in \mathbb{Q}^\times$ we have $v_i = \pm 1$. Equation (5.16) now becomes

$$\pm u_1 \pm \cdots \pm u_n = 1. \tag{5.19}$$

The group Ω generated by Γ' and the points $(\pm 1, \ldots, \pm 1)$ is finitely generated with rank equal to that of Γ'. By Theorem 2.1 of [8], due to Evertse, Schilickewei and Schmidt, the solutions of (5.19) with $(\pm u_1, \ldots, \pm u_n) \in \Omega$ are contained in the union of not more than

$$\exp((r+1)(5n)^{3n}) \tag{5.20}$$

proper subspaces of $\overline{\mathbb{Q}}^n$.

Combining the estimates (5.18) and (5.20) we have fewer than

$$2^{30n^2}(21n^2)^r + \exp((r+1)(5n)^{3n}) < C(n,r)$$

proper subspaces of $\overline{\mathbb{Q}}^n$. □

Lemma 5.5. *For $\alpha, \beta \in \overline{\mathbb{Q}}^\times$ there is a $y \in \mathbb{Z}$ such that*

$$h(\alpha\beta^{x-y}) \geq \frac{1}{4}\,|x|\,h(\beta),$$

for every $x \in \mathbb{Z}$.

This follows directly from a result of Schlickewei and Schmidt, in particular it is the $r = n = 1$ case of Lemma 15.1 of [16]. We include the proof of this special case for the convenience of the reader.

Proof. We may suppose that $h(\beta) > 0$. Let $K = \mathbb{Q}(\alpha, \beta)$ and let M_K denote the set of places of K. By the product formula we see that for any $\gamma \in K^\times$

$$h(\gamma) = \sum_{v \in M_K} \max\{0, \log|\gamma|_v\} = \frac{1}{2}\sum_{v \in M_K} |\log|\gamma|_v|\,.$$

Hence, for $x \in \mathbb{Z}$,

$$h(\alpha\beta^x) = \frac{1}{2}\sum_{v \in M_K} |\log|\alpha|_v + x\log|\beta|_v|\,.$$

For $(\zeta, \xi) \in \mathbb{R}^2$, we define the function

$$\psi(\zeta,\xi) = \frac{1}{2}\sum_{v \in M_K} |\zeta\log|\alpha|_v + \xi\log|\beta|_v|\,.$$

Note that we have the equalities

$$\psi(1,x) = h(\alpha\beta^x) \quad \text{and} \quad \psi(0,\xi) = |\xi|\,h(\beta). \tag{5.21}$$

The function ψ is continuous and satisfies $\psi(\zeta+\zeta', \xi+\xi') \leq \psi(\zeta,\xi)+\psi(\zeta',\xi')$ and $\psi(\lambda\zeta, \lambda\xi) = |\lambda|\,\psi(\zeta,\xi)$ for $\lambda \in \mathbb{R}$. Thus, the set $\Psi \subseteq \mathbb{R}^2$ containing points (ζ,ξ) such that $\psi(\zeta,\xi) \leq 1$ is closed, convex, symmetric about the origin and contains the origin in its interior. However, Ψ may not be bounded.

First assume Ψ is unbounded. Consider the function $f(\theta) = \psi(\sin\theta, \cos\theta)$ on $\theta \in [0, 2\pi]$. Since $[0, 2\pi]$ is compact f has a minimum, say η. By the definition of f we know that $\eta \geq 0$. Conversely, since Ψ is unbounded and, for $(\zeta, \xi) \neq (0, 0)$,

$$\psi(\zeta, \xi) = \sqrt{\zeta^2 + \xi^2} f(\theta)$$

for some $\theta \in [0, 2\pi]$, we cannot have $\eta > 0$. In particular we can find some $(\zeta_0, \xi_0) \neq (0, 0)$ such that $\psi(\zeta_0, \xi_0) = 0$. Since $\psi(0, 1) = h(\beta) > 0$, we have that $\zeta_0 \neq 0$. Then, by homogeneity, there is some ξ_1 such that $\psi(1, \xi_1) = 0$. If Ψ is bounded it is compact and we may take (ζ_0, ξ_0) with maximum ζ_0. Writing ξ_0 as $\xi_0 = \zeta_0 \xi_1$ we have $\zeta_0 \psi(1, \xi_1) \leq 1$.

Take arbitrary $(\zeta, \xi) \in \mathbb{R}^2$. When Ψ is unbounded, $\psi(\zeta, \zeta\xi_1) = |\zeta|\, \psi(1, \xi_1) = 0 \leq \psi(\zeta, \xi)$. When Ψ is bounded, $\psi(\zeta, \zeta\xi_1) = |\zeta|\, \psi(1, \xi_1) \leq |\zeta| / \zeta_0 \leq \psi(\zeta, \xi)$, where the last inequality follows from homogeneity and the fact that the maximality of ζ_0 implies $\psi(\zeta_0, \xi \frac{\zeta_0}{\zeta}) \geq 1$. We now have, by (5.21),

$$|\xi - \zeta\xi_1|\, h(\beta) = \psi(0, \xi - \zeta\xi_1) \leq \psi(\zeta, \xi) + \psi(-\zeta, -\zeta\xi_1) \leq 2\psi(\zeta, \xi).$$

Setting $\zeta = 1$ and replacing ξ by $x \in \mathbb{Z}$, we obtain, by (5.21),

$$h(\alpha\beta^x) = \psi(1, x) \geq \frac{1}{2} |x - \xi_1|\, h(\beta).$$

We take $y \in \mathbb{Z}$ such that $\xi_1 = -y + \mu$ with $|\mu| \leq 1/2$. Then

$$h(\alpha\beta^{x-y}) \geq \frac{1}{2} |x - \mu|\, h(\beta) \geq \frac{1}{4} |x|\, h(\beta).$$

□

5.5 An important Lemma

We define the degree of the zero polynomial to be -1. For a k-tuple $\mathbf{P} = (P_1, \ldots, P_k)$ of polynomials we set

$$t(\mathbf{P}) = ((\deg P_1 + 1) + \cdots + (\deg P_k + 1))$$

and

$$s(\mathbf{P}) = 1 + \max\{\deg P_1, \ldots, \deg P_k\}.$$

The key point of the following lemma lies in the inequalities (5.24) as they give a potential avenue for solving our main problem by performing induction on $t(\mathbf{P})$. The difficulty, however, lies in satisfying (5.23).

Lemma 5.6. *Consider the equation*

$$P_1(x)\alpha_1^x + \cdots + P_k(x)\alpha_k^x = 0, \tag{5.22}$$

where $\alpha_1, \ldots, \alpha_k \in \overline{\mathbb{Q}}^\times$ *and each* P_i *is a non-zero polynomial with coefficients in* $\overline{\mathbb{Q}}$. *Set* $\mathbf{P} = (P_1, \ldots, P_k)$, $t = t(\mathbf{P})$ *and* $s = s(\mathbf{P})$. *Suppose that* $t \geq 3$ *and that*

$$\max_{1 \leq i,j \leq k} h\left(\frac{\alpha_i}{\alpha_j}\right) \geq h^*, \tag{5.23}$$

for some $0 < h^* \leq 1$. *Set*

$$E = 16t^2 s/h^* \quad \textit{and} \quad F = \exp(3(6t)^{3t}) + 5E\log E.$$

Then there are k*-tuples of polynomials*

$$\mathbf{P}^{(w)} = (P_1^{(w)}, \ldots, P_k^{(w)}),$$

$1 \leq w < F$, *at least one* $P_i^{(w)}$ *not identically zero, with*

$$\deg P_i^{(w)} \leq \deg P_i \textit{ for each } 1 \leq i < k \textit{ and } \deg P_k^{(w)} < \deg P_k \tag{5.24}$$

such that every solution $x \in \mathbb{Z}$ *of* (5.22) *satisfies*

$$P_1^{(w)}(x)\alpha_1^x + \cdots + P_k^{(w)}(x)\alpha_k^x = 0 \tag{5.25}$$

for some $1 \leq w < F$.

Proof. For $u \in \mathbb{Z}$ let $y = x + u$. Then (5.22) may be rewritten as

$$P_1(y-u)\alpha_1^{-u}\alpha_1^y + \cdots + P_k(y-u)\alpha_k^{-u}\alpha_k^y = 0.$$

Setting $Q_i(y) = P_i(y-u)\alpha_i^{-u}$, for each $1 \leq i \leq k$, (5.22) becomes

$$Q_1(y)\alpha_1^y + \cdots + Q_k(y)\alpha_k^y = 0. \tag{5.26}$$

If our assertion is true for (5.26), with polynomial k-tuples $\mathbf{Q}^{(w)} = (Q_1^{(w)}, \ldots, Q_k^{(w)})$, $1 \leq w \leq F$ then every solution $y \in \mathbb{Z}$ of (5.26) will satisfy

$$Q_1^{(w)}(y)\alpha_1^y + \cdots + Q_k^{(w)}(y)\alpha_k^y = 0$$

for some $1 \leq w < F$ and the corresponding solutions $x = y - u$ of (5.22) will satisfy (5.25) with $P_i^{(w)}(x) = Q_i^{(w)}(x+u)\alpha_i^u$, for $1 \leq i \leq k$. Thus we may consider (5.26) instead of (5.22).

We pick $u \in \mathbb{Z}$ as follows. Write

$$P_i(x) = a_{i0} + \cdots + a_{id_i}x^{d_i},$$

where $d_i = \deg P_i$. We may suppose that $h(\alpha_1/\alpha_2) \geq h^*$. By Lemma 5.5 we can take u so that

$$h\left(\frac{a_{1d_1}}{a_{2d_2}}\left(\frac{\alpha_1}{\alpha_2}\right)^{y-u}\right) \geq \frac{1}{4}\,|y|\,h\left(\frac{\alpha_1}{\alpha_2}\right) \geq \frac{1}{4}\,|y|\,h^*,$$

for every $y \in \mathbb{Z}$. Then, writing

$$Q_i(y) = b_{i0} + \cdots + b_{id_i}y^{d_i},$$

for $1 \leq i \leq k$, we have $b_{1d_1} = a_{1d_1}\alpha_1^{-u}$ and $b_{2t_2} = a_{2d_2}\alpha_2^{-u}$ and so

$$h\left(\frac{b_{1d_1}\alpha_1^y}{b_{2d_2}\alpha_2^y}\right) \geq \frac{1}{4}\,|y|\,h^*, \tag{5.27}$$

for every $y \in \mathbb{Z}$.

The equation (5.26) is of the form

$$(b_{10} + \cdots + b_{1d_1}y^{d_1})\alpha_1^y + \cdots + (b_{k0} + \cdots + b_{kd_k}y^{d_k})\alpha_k^y = 0.$$

Omitting any zero coefficients we rewrite this as

$$(b'_{10}y^{v_{10}} + \cdots + b_{1d_1}y^{d_1})\alpha_1^y + \cdots + (b'_{k0}y^{v_{k0}} + \cdots + b_{kd_k}y^{d_k})\alpha_k^y = 0. \tag{5.28}$$

Let q be the total number of coefficients in (5.28) and consider the vectors

$$\begin{aligned}\mathbf{X} &= (b'_{10}\alpha_1^y, \ldots, b_{1d_1}\alpha_1^y, \ldots, b'_{k0}\alpha_k^y, \ldots, b_{kd_k}\alpha_k^y),\\ \mathbf{Y} &= (y^{v_{10}}, \ldots, y^{d_1}, \ldots, y^{v_{k0}}, \ldots, y^{d_k})\end{aligned}$$

in q-dimensional space. Equation (5.26) then becomes

$$Z_1 + \cdots + Z_q = 0, \tag{5.29}$$

where $Z_i = X_iY_i$, X_i and Y_i the ith components of $\mathbf{X}$ and $\mathbf{Y}$ respectively. Now $\mathbf{X}$ lies the group Γ of rank ≤ 2 generated by $(b'_{10}, \ldots, b_{1d_1}, \ldots, b'_{k0}, \ldots, b_{kd_k})$ and $(\alpha_1, \ldots, \alpha_1, \ldots, \alpha_k, \ldots, \alpha_k)$. Moreover

$$h_{\mathbb{P}^{q-1}}(\mathbf{X}) \geq h\left(\frac{b_{1d_1}\alpha_1^y}{b_{2d_2}\alpha_2^y}\right) \geq \frac{1}{4}\,|y|\,h^*, \tag{5.30}$$

by (5.27). Also we have $\mathbf{Y} \in \mathbb{Q}^q$ and $\mathbf{Y} \in (\mathbb{Q}^\times)^q$ when $y \neq 0$. Since $y \in \mathbb{Z}$ we have $\log |y|_p \leq 0$ for all finite p and since $d_i < s$ for each $1 \leq i \leq k$, we have

$$h_{\mathbb{P}^{q-1}}(\mathbf{Y}) \leq s \log |y| \,. \tag{5.31}$$

Assume that

$$|y| \geq 2E \log E. \tag{5.32}$$

Since $E \geq 16$ we see that $\log(2E \log E) < 2 \log E$. This combined with the fact that $|y| - E \log |y|$ is increasing for $|y| \geq E$ yields

$$|y| > E \log |y| \geq \frac{16q^2 s}{h^*} \log |y| \,,$$

since $q \leq t$. Combining this with (5.30) and (5.31) we have

$$h_{\mathbb{P}^{q-1}}(\mathbf{Y}) \leq s \log |y| < \frac{h^*}{16q^2} |y| = \frac{1}{4q^2} \frac{1}{4} |y| \, h^* < \frac{1}{4q^2} h_{\mathbb{P}^{q-1}}(\mathbf{X}).$$

By Lemma 5.4, every such y is contained in the union of at most

$$C(q, 2) = \exp(3(6q)^{3q}) \leq \exp(3(6t)^{3t}) \tag{5.33}$$

proper subspaces of the space defined by (5.29). Consider such a subspace, given by $c_1 Z_1 + \cdots + c_q Z_q = 0$. Taking a linear combination of this and (5.29) we obtain a nontrivial relation $c_1' Z_1 + \cdots + c_{q-1}' Z_{q-1} = 0$. This implies that y satisfies a nontrivial equation

$$\tilde{Q}_1(y) \alpha_1^y + \cdots + \tilde{Q}_k(y) \alpha_k^y = 0, \tag{5.34}$$

with

$$\deg \tilde{Q}_i \leq d_i \text{ for } 1 \leq i < k \text{ and } \deg \tilde{Q}_k < d_k. \tag{5.35}$$

Clearly there are fewer than $5E \log E$ values of y that do not satisfy (5.32). For fixed y, since $t \geq 3$, we can construct polynomials $\tilde{Q}_1, \ldots, \tilde{Q}_k$, not all zero, satisfying (5.34) and (5.35). The total number of such polynomials is thus less than

$$\exp(3(6t)^{3t}) + 5E \log E = F.$$

□

5.6 A proposition that implies the Theorem

We now state a proposition from which Theorem 5.2 will be deduced.

Proposition. *Let $M_j(\mathbf{X}) = a_{1j}X_1 + \cdots + a_{kj}X_k$, $1 \le j \le n$, be linear forms which are linearly independent over $\mathbb{Q}$ and have coefficients in $\overline{\mathbb{Q}}$. Write $\mathbf{a}_i = (a_{i1}, \ldots, a_{in})$ and assume that each $\mathbf{a}_i$ is nontrivial. For each $1 \le i \le n$ define t_i to be the integer such that $\mathbf{a}_i = (a_{i1}, \ldots, a_{it_i}, 0, \ldots, 0)$ with $a_{it_i} \neq 0$. Set $t = t_1 + \cdots + t_k$,*

$$T = \min\{k^n, t^{\sqrt{2t}}\},$$
$$h^* = e^{-3T^4}.$$

For nonzero algebraic numbers $\alpha_1, \ldots, \alpha_k$, the $x \in \mathbb{Z}$ for which

$$M_1(\alpha_1^x, \ldots, \alpha_k^x), \ldots, M_n(\alpha_1^x, \ldots, \alpha_k^x)$$

are $\mathbb{Q}$-linearly dependent fall into at most

$$H(T) = \exp(4(6T)^{3T}) \tag{5.36}$$

classes with the following property. For each class C there is a positive integer m such that

(a) *solutions x and x' in C satisfy $x \equiv x' \pmod m$,*

(b) *there are $i \neq j$ such that either $\alpha_i \not\sim \alpha_j$ and $h(\alpha_i^m/\alpha_j^m) \ge h^*$, or $\alpha_i \sim \alpha_j$ and $\operatorname{ord}(\alpha_i^m/\alpha_j^m) \le (h^*)^{-1}$.*

Proof of Theorem 5.2. For a k-tuple of polynomials $\mathbf{P} = (P_1, \ldots, P_k)$, set $t_i = t_i(\mathbf{P}) = 1 + \deg P_i$, for $1 \le i \le k$, $t = t(\mathbf{P}) = t_1 + \cdots + t_k$ and $s = s(\mathbf{P}) = \max_{1 \le i \le k} t_i$. Suppose that $P_1, \ldots, P_k$ have algebraic coefficients and take $\alpha_1, \ldots, \alpha_k \in \overline{\mathbb{Q}}^\times$. We will prove by induction on t that the set of solutions $\mathcal{Z}$ of

$$P_1(x)\alpha_1^x + \cdots + P_k(x)\alpha_k^x = 0 \tag{5.37}$$

satisfies $\nu(\mathcal{Z}) \le Z(t, T)$ where we define $Z(t, T)$ to be

$$\exp((2^t - 1)(8T)^{3T}), \tag{5.38}$$

and $T = \min\{k^s, t^{\sqrt{2t}}\}$.

We may assume that $k \ge 2$, $t \ge 3$ and that $P_1, \ldots, P_k$ are non-zero. Write, for $1 \le i \le k$, $P_i(x) = \sum_{j=1}^{s} a_{ij}x^{j-1}$. For $1 \le j \le s$ we define the linear forms

$$N_j(\mathbf{X}) = N_j(X_1, \ldots, X_k) = a_{1j}X_1 + \cdots + a_{kj}X_k.$$

Then, letting $\mathbf{a}_i = (a_{i1}, \ldots, a_{is})$ for $1 \leq i \leq k$, we have that each $\mathbf{a}_i$ is nontrivial and $\mathbf{a}_i = (a_{i1}, \ldots, a_{it_i}, 0, \ldots, 0)$ with $a_{it_i} \neq 0$. The linear forms $N_1, \ldots, N_s$ are not necessarily $\mathbb{Q}$-linearly independent. Let $M_1, \ldots, M_n$ be a maximal $\mathbb{Q}$-linearly independent subset. Note that replacing $N_1, \ldots, N_s$ with $M_1, \ldots, M_n$ will not cause the numbers $t_1, \ldots, t_k$ or t to increase.

Equation (5.37) can be rewritten as

$$\sum_{j=1}^{s} N_j(\alpha_1^x, \ldots, \alpha_k^x) x^{j-1} = 0. \tag{5.39}$$

For each $1 \leq j \leq s$, there are $c_{j1}, \ldots, c_{jn} \in \mathbb{Q}$ such that $N_j(\mathbf{X}) = c_{j1}M_1(\mathbf{X}) + \cdots + c_{jn}M_n(\mathbf{X})$. We can then rewrite (5.39) as

$$\sum_{r=1}^{n} \left(\sum_{j=1}^{s} c_{jr} x^{j-1} \right) M_r(\alpha_1^x, \ldots, \alpha_k^x) = 0. \tag{5.40}$$

There are fewer than s numbers $x \in \mathbb{Z}$ such that each polynomial $c_{1r} + \cdots + c_{sr}x^{s-1}$, $1 \leq r \leq n$, vanishes. For any other solution of (5.40), the numbers $M_1(\alpha_1^x, \ldots, \alpha_k^x), \ldots, M_n(\alpha_1^x, \ldots, \alpha_k^x)$ are $\mathbb{Q}$-linearly dependent and, by the proposition, lie in at most $H(T)$ classes, since $n \leq s$.

Fix a class C and let $\mathcal{Z}_C$ denote the set of solutions of (5.37) in C. The solutions in $\mathcal{Z}_C$ are of the form $x = x_0 + my$, with $y \in \mathbb{Z}$. Setting $\hat{\alpha}_i = \alpha_i^m$ and $\hat{P}_i(y) = \alpha_i^{x_0} P_i(x_0 + my)$, for $1 \leq i \leq k$, equation (5.37) becomes

$$\hat{P}_1(y)\hat{\alpha}_1^y + \cdots + \hat{P}_k(y)\hat{\alpha}_k^y = 0. \tag{5.41}$$

Assume first that there is some $i \neq j$ with $\alpha_i \sim \alpha_j$ and $\mathrm{ord}(\hat{\alpha}_i/\hat{\alpha}_j) = \mathrm{ord}(\alpha_i^m/\alpha_j^m) \leq (h^*)^{-1}$. We may suppose that $i = k$ and $j = k-1$. Set $q = \mathrm{ord}(\hat{\alpha}_k/\hat{\alpha}_{k-1})$. Divide $\mathbb{Z}$ up into the q arithmetic progressions $\mathcal{A}(q, b)$, $0 \leq b < q$. For a solution y of (5.41) in one such arithmetic progression $\mathcal{A}(q, b)$ we have that $y = qz + b$ for some $z \in \mathbb{Z}$. We then set $\alpha_i^* = \hat{\alpha}_i^q$, for $1 \leq i \leq k-1$, $P_i^*(z) = \hat{\alpha}_i^b \hat{P}_i(qz + b)$, for $1 \leq i \leq k-2$, and $P_{k-1}^*(z) = \hat{\alpha}_{k-1}^b \hat{P}_{k-1}(qz + b) + \hat{\alpha}_k^b \hat{P}_k(qz + b)$. Then (5.41) becomes

$$P_1^*(z)\alpha_1^{*z} + \cdots + P_{k-1}^*(z)\alpha_{k-1}^{*z} = 0. \tag{5.42}$$

Now $t(P_1^*, \ldots, P_{k-1}^*) < t(\mathbf{P})$ so, by induction, the zeros of (5.42) lie in the union of at most $Z(t-1, T)$ single numbers and arithmetic progressions. Summing over $0 \leq b < q \leq (h^*)^{-1}$ we see that $\mathcal{Z}_C$ satisfies

$$\nu(\mathcal{Z}_C) < \exp(3T^4) Z(t-1, T). \tag{5.43}$$

Now assume that there is $i \neq j$ with $\alpha_i \not\sim \alpha_j$ and $h(\alpha_i^m/\alpha_j^m) \geq h^*$. Then considering equation (5.41), we have $h(\hat{\alpha}_i/\hat{\alpha}_j) \geq h^*$ and we can apply Lemma 5.6. So we have, for $1 \leq w < F$, polynomial k-tuples $\mathbf{P}^{(w)} = (P_1^{(w)}, \ldots, P_K^{(w)}) \neq (0, \ldots, 0)$ with $s(\mathbf{P}^{(w)}) \leq s$ and $t(\mathbf{P}^{(w)}) < t$ such that every solution of (5.41) satisfies

$$P_1^{(w)}(y)\hat{\alpha}_1^y + \cdots + P_k^{(w)}(y)\hat{\alpha}_k^y = 0, \tag{5.44}$$

for some w. Now

$$F = \exp(3(6t)^{3t}) + 5E\log E \text{ with } E = 16t^2 s/h^*.$$

Since $t \leq T$ and $s \leq T$ we get $E \leq 16T^3\exp(6T^4) < \exp(7T^4)$, hence $E\log E < \exp(8T^4)$ and

$$F < \exp(3(6T)^{3T}) + 5\exp(8T^4) < \exp(4(6T)^{3T}). \tag{5.45}$$

By induction on t, the solutions of (5.44), for each $1 \leq w < F$, lie in the union of at most $Z(t-1,T)$ single numbers and arithmetic progressions. We must be careful here as the solutions of (5.41) may be *properly* contained in these progressions since we do not in general have that every solution of (5.44) will be a solution of (5.41).

Consider one such progression $\mathcal{A}(a,b)$. Writing $y = az + b$, (5.44) becomes

$$\hat{P}_1^{(w)}(z)\hat{\alpha}_1^z + \cdots + \hat{P}_k^{(w)}(z)\hat{\alpha}_k^x = 0, \tag{5.46}$$

with $\tilde{\alpha_i} = \hat{\alpha}_i^a$ and $\tilde{P}_i^{(w)}(z) = \hat{\alpha}_i^b P_i^{(w)}(az+b)$, for $1 \leq i \leq k$. If $\tilde{\alpha}_1, \ldots, \tilde{\alpha}_k$ were all distinct then, since (5.46) holds for every $z \in \mathbb{Z}$, we must have each $\tilde{P}_i^{(w)} = 0$, hence each $P_i^{(w)} = 0$, which is not the case. Thus $\tilde{\alpha}_1, \ldots, \tilde{\alpha}_k$ are not all distinct. Say $\tilde{\alpha}_{k-1} = \tilde{\alpha}_k$. Then (5.41) becomes

$$\tilde{P}_1(z)\tilde{\alpha}_1^z + \cdots + \tilde{P}_{k-1}(z)\tilde{\alpha}_{k-1}^z = 0, \tag{5.47}$$

with $\tilde{P}_i(z) = \hat{\alpha}_i^b \hat{P}_i(az+b)$, for $1 \leq i \leq k-2$, and $\tilde{P}_{k-1}(z) = \hat{\alpha}_{k-1}^b \hat{P}_{k-1}(az+b) + \hat{\alpha}_k^b \hat{P}_k(az+b)$. Since $t(\tilde{P}_1, \ldots, \tilde{P}_{k-1}) < t$, the solutions to (5.47) are the union of at most $Z(t-1,T)$ single numbers and arithmetic progressions. So, for our class C, we have

$$\nu(\mathcal{Z}_C) \leq FZ(t-1,T)^2 < \exp(4(6T)^{3T})Z(t-1,T)^2, \tag{5.48}$$

by (5.45).

Considering the possible fewer than s solutions mentioned at the beginning, comparing (5.43) and (5.48) and summing over the classes C, we obtain

$$\begin{aligned}\nu(\mathcal{Z}) &< s + H(T)\exp(4(6T)^{3T})Z(t-1,T)^2 \\ &\leq T + \exp(8(6T)^{3T})\exp((2^t-2)(8T)^{3T}) \\ &< \exp((2^t-1)(8T)^{3T}) = Z(t,T),\end{aligned}$$

establishing (5.38).

Since $t \le T$, we have

$$\nu(\mathcal{Z}) < \exp(2^T (8T)^{3T}).$$

Let $T_1 = t^{\sqrt{2t}}$. Since $T \le T_1$ and $t \ge 3$, we have

$$\begin{aligned}\nu(\mathcal{Z}) &< \exp(2^{T_1}(8T_1)^{3T_1}) \\ &< \exp((8T_1)^{4T_1}) \\ &= \exp\exp(4t^{\sqrt{2t}}(\log 8 + \sqrt{2t}\log t)) \\ &< \exp\exp(t^{3\sqrt{t}}).\end{aligned}$$

Let $T_2 = k^s$. Since $T \le T_2$ and $T_2 \ge ks \ge t \ge 3$, we have

$$\begin{aligned}\nu(\mathcal{Z}) &< \exp(2^{T_2}(8T_2)^{3T_2}) \\ &< \exp(T_2^{10T_2}) \\ &= \exp\exp(10sk^s \log k).\end{aligned}$$

□

The remainder of this chapter will be devoted to proving the Proposition.

5.7 A lemma on linear independence

The following lemma improves on Lemma 2 of [18] by replacing the bound e^{12t} with $t^{\sqrt{2t}}$. This is the key ingredient in our improvement of Schmidt's main result in [18]. If K is a number field and σ is an embedding $K \hookrightarrow \mathbb{C}$ we denote by $\eta^{(\sigma)}$ the image of $\eta \in K$ under σ. If $\mathbf{v} = (v_1, \ldots, v_n) \in K^n$ we set

$$\mathbf{v}^{(\sigma)} = (v_1^{(\sigma)}, \ldots, v_n^{(\sigma)}).$$

Lemma 5.7. *Let K be a field and $\mathbf{a}_1, \ldots, \mathbf{a}_k$ vectors in K^n. Fix n not necessarily distinct embeddings $\sigma_1, \ldots, \sigma_n$ of K into $\mathbb{C}$. For $1 \le i \le k$ write*

$$\mathbf{a}_i = (a_{i1}, \ldots, a_{it_i}, 0, \ldots, 0)\,,$$

where either $t_i = 0$, hence $\mathbf{a}_i = \mathbf{0}$, or $t_i > 0$ and $a_{t_i} \ne 0$. Set $t = t_1 + \ldots + t_k$. Then there are at most $t^{\sqrt{2t}}$ ordered n-tuples $(i_1, \ldots, i_n)$, with $1 \le i_1, \ldots, i_n \le k$, such that $\mathbf{a}_{i_1}^{(\sigma_1)}, \ldots, \mathbf{a}_{i_n}^{(\sigma_n)}$ are linearly independent.

Proof. Note first that the result is trivial if $k < n$ so we may assume $k \geq n$. Also note that the embedding σ_j, for any $1 \leq j \leq n$, will not have any affect on the numbers $t_1, \ldots, t_k$. If $\mathbf{a}_i = \mathbf{0}$ then $\mathbf{a}_i$ doesn't contribute at all to the number of n-tuples that we are counting and t_i doesn't contribute to t. Hence we may assume $\mathbf{a}_i \neq \mathbf{0}$ for each $1 \leq i \leq k$. In particular we may assume $t \geq k$. Suppose $\mathbf{a}_{i_1}^{(\sigma_1)}, \ldots, \mathbf{a}_{i_n}^{(\sigma_n)}$ are linearly independent. Then at most one t_i equals 1. If there exists $\mathbf{a}_i$ such that $t_i = 1$ then there is at most one $\mathbf{a}_i$ such that $t_i = 2$ and so on. Hence if there exist any n-tuples $(i_1, \ldots, i_n)$ such that $\mathbf{a}_{i_1}^{(\sigma_1)}, \ldots, \mathbf{a}_{i_n}^{(\sigma_n)}$ are linearly independent then we must have

$$t \geq \sum_{j=1}^{n} j = \frac{n(n+1)}{2},$$

hence $n < \sqrt{2t}$. Clearly there are at most k^n such n-tuples and we have

$$k^n < t^{\sqrt{2t}}.$$

□

With the exception of the constant $\sqrt{2}$ the above result is best possible. Say $k = n$, $\sigma_1 = \cdots = \sigma_n$ and we have n linearly independent vectors $\mathbf{a}_1, \ldots, \mathbf{a}_n$. Then the number of such n-tuples is $n!$. Stirling's Approximation yields

$$n! > \sqrt{2\pi} n^{n+1/2} e^{-n+1/(12n+1)} > \sqrt{2\pi} e^{n(\log n - 1)}$$

Hence for any constant c and any $\delta > 0$ we have, since $t \leq kn = n^2$,

$$e^{c\sqrt{t}(\log t)^{1-\delta}} = o(n!)\,.$$

5.8 Splitting of the exponential equation

For $a_1, \ldots, a_q, \alpha_1, \ldots, \alpha_q \in \overline{\mathbb{Q}}^\times$ we consider the function

$$f(x) = a_1\alpha_1^x + \cdots + a_q\alpha_q^x. \tag{5.49}$$

Group together summands with $\alpha_i \sim \alpha_j$. After relabelling we may write, uniquely up to ordering,

$$f(x) = f_1(x) + \cdots + f_g(x), \tag{5.50}$$

where, for each $1 \leq i \leq g$,

$$f_i(x) = a_{i1}\alpha_{i1}^x + \cdots + a_{iq_i}\alpha_{iq_i}^x$$

with $q_1 + \cdots + q_g = q$ and

$$\begin{array}{lll} \alpha_{ij} \sim \alpha_{ik} & \text{when} & 1 \le i \le g,\ 1 \le i, k \le q_i \\ \alpha_{ij} \not\sim \alpha_{i'k} & \text{when} & 1 \le i \ne i' \le g,\ 1 \le j \le q_i\ 1 \le k \le q_{i'}. \end{array}$$

If a solution $x \in \mathbb{Z}$ of $f(x) = 0$ satisfies

$$f_1(x) = \cdots = f_g(x) = 0 \tag{5.51}$$

we say that $f(x) = 0$ *splits* into the g equations (5.51).

Lemma 5.8. *All but at most*

$$G(q) = \exp(3(6q)^{3q})$$

solutions of $f(x) = 0$ *split into the* g *equations* (5.51).

Proof. This lemma is trivial if $g = 1$, hence we may assume that $g \ge 2$, hence $q \ge 2$. We will proceed by induction on q. If $q = 2$ and $g = 2$ then we have $f(x) = a_{11}\alpha_{11}^x + a_{21}\alpha_{21}^x$ with $a_{11}a_{21} \ne 0$ and $\alpha_{11} \not\sim \alpha_{21}$. There can then be at most one $x \in \mathbb{Z}$ with $f(x) = 0$.

We now assume $q \ge 3$. Note that $(\alpha_1^x, \dots, \alpha_q^x)$ lies in a group Γ of rank ≤ 1 generated by $(\alpha_1, \dots, \alpha_q)$. Thus by Lemma 5.3 there are at most $C(q, 1) = \exp(2(6q)^{3q})$ vectors $\mathbf{c}^{(r)} = (c_1^{(r)}, \dots, c_q^{(r)})$, $1 \le r \le C(q, 1)$, such that for every nondegenerate solution $x \in \mathbb{Z}$ of $f(x) = 0$ we have $(\alpha_1^x, \dots, \alpha_q^x) = \lambda \mathbf{c}^{(r)}$, for some non-zero constant λ and $1 \le r \le C(q, 1)$. This implies that the quotients $(\alpha_i/\alpha_j)^x$ depend only on r. Since $g \ge 2$, there is some α_i/α_j that is not a root of unity, thus there can be at most one solution $x \in \mathbb{Z}$ for any given $1 \le r \le C(q, 1)$.

When $x \in \mathbb{Z}$ is a degenerate solution of $f(x) = 0$, there is a nontrivial partition of $\{1, \dots, q\}$ into subsets $\{i_1, \dots, i_n\}$ and $\{j_1, \dots, j_m\}$, with $n + m = q$, such that

$$a_{i_1}\alpha_{i_1}^x + \cdots + a_{i_n}\alpha_{i_n}^x = 0 \quad \text{and} \quad a_{j_1}\alpha_{j_1}^x + \cdots + a_{j_m}\alpha_{j_m}^x = 0.$$

There are $< 2^{q-1}$ such partitions. Each partition yields nonzero f^* and f^{**} with $f = f^* + f^{**}$, each f^* and f^{**} having fewer summands than does f and

$$f^*(x) = f^{**}(x) = 0. \tag{5.52}$$

Write

$$\begin{aligned} f^*(x) &= f_1^*(x) + \cdots + f_g^*(x), \\ f^{**}(x) &= f_1^{**}(x) + \cdots + f_g^{**}(x), \end{aligned}$$

where f_i^* and f_i^{**} are linear combinations of $\alpha_{i1}^x, \dots, \alpha_{iq_i}^x$. By induction, all but at most $2G(q-1)$ solutions of (5.52) have

$$f_1^*(x) = \cdots = f_g^*(x) = f_1^{**}(x) = \cdots = f_g^{**}(x) = 0,$$

which then implies (5.51). The number of exceptions to (5.51) is then

$$\begin{aligned} &< \exp(2(6q)^{3q}) + 2^q G(q-1) \\ &< \exp(2(6q)^{3q}) + \exp(3(6q)^{3q-3}) \\ &< \exp(3(6q)^{3q}) = G(q). \end{aligned}$$

□

We call a summand $a_i\alpha_i^x$ of (5.49) a *singleton* if $\alpha_i \not\sim \alpha_j$ for any $j \neq i$, $1 \leq j \leq q$.

Corollary 5.9. *Let f be given by* (5.49). *If f contains a singleton then $f(x) = 0$ has at most $G(q)$ zeros $x \in \mathbb{Z}$.*

Proof. If f contains a singleton then $f_i(x) = a_i\alpha_i^x$. for some $1 \leq i \leq g$ and has no zero, hence our equation cannot split. □

Given a solution x of $f_i(x) = 0$ we may have a subsum of $f_i(x)$ that vanishes. We will refer to such a situation as *subsplitting*. The results of Chapter 4 are vital in dealing with this extra complication. A solution x of $f_i(x)$ is called *nondegenerate* if no subsplitting occurs.

5.9 Algebraic numbers, ε-bad and ε-unpleasant l-tuples

Lemma 5.10. *Let β be algebraic of degree d over $\mathbb{Q}$ and let $S = \{\beta^{[1]}, \dots, \beta^{[d]}\}$ be its set of conjugates. Let $S_1, \dots, S_m$ denote the equivalence classes of S under $\sim$. Then $d = mn$ for some $n \in \mathbb{Z}$ and*

$$|S_1| = \cdots = |S_m| = n.$$

Proof. Let G denote the Galois group of $K = \mathbb{Q}(\beta^{[1]}, \dots, \beta^{[d]})$. For $\eta, \gamma \in \overline{\mathbb{Q}}^\times$ with $\eta \sim \gamma$ and σ an embedding of $\mathbb{Q}(\eta, \gamma)$ into $\mathbb{C}$ we clearly have $\sigma(\eta) \sim \sigma(\gamma)$ since $\sigma(\eta)/\sigma(\gamma) = \sigma(\eta/\gamma)$. Hence we see that G permutes the sets $S_1, \dots, S_m$. Moreover, since G acts transitively on S, G acts transitively on $\{S_1, \dots, S_m\}$. Thus $|S_1| = \cdots = |S_m| = n$ for some $n \in \mathbb{Z}$. If follows that $d = mn$. □

For a positive integer a let $\log^+ a = \max\{1, \log a\}$. By a result of Voutier [21] we know that for an algebraic number $\beta \not\sim 1$ of degree d over $\mathbb{Q}$ we have

$$h(\beta) \geq \frac{1}{4d} \left(\frac{\log^+ \log^+ d}{\log^+ d} \right)^3 .$$

It will suffice for our purposes to use the slightly weaker version

$$h(\beta) \geq \frac{1}{4d(\log^+ d)^3}. \tag{5.53}$$

Lemma 5.11. *Let β be as in Lemma* 5.10*, and suppose β is not a root of unity. Then*

$$h(\beta) \geq \frac{1}{4d(\log^+ m)^3}. \tag{5.54}$$

Proof. We keep the same notation as in Lemma 5.10 and suppose that $\beta \in S_1$. For each $1 \leq i \leq m$, let

$$\gamma_i = \prod_{\beta^{[j]} \in S_i} \beta^{[j]}.$$

Then G permutes $\gamma_1, \ldots, \gamma_m$. Hence every conjugate of γ_1 is in the set $\{\gamma_1, \ldots, \gamma_m\}$ and this implies that the degree of γ_1 is $\leq m$. Moreover γ_1 cannot be a root of unity, since

$$\beta^n \sim \prod_{\beta^{[j]} \in S_1} \beta^{[j]} = \gamma_1,$$

and β is not a root of unity. Hence

$$h(\gamma_1) \geq \frac{1}{4m(\log^+ m)^3}.$$

But

$$h(\gamma_1) \leq \sum_{\beta^{[j]} \in S_1} h(\beta^{[j]}) = nh(\beta),$$

which implies

$$h(\beta) \geq \frac{h(\gamma_1)}{n} \geq \frac{1}{4d(\log^+ m)^3}.$$

□

Henceforth we will use the notation $n(\beta)$ to denote the number n for β as in Lemma 5.10. Suppose K is a number field of degree D with $\beta \in K$. Let $\eta^{(\sigma)}$, $1 \le \sigma \le D$, denote the images of $\eta \in K$ under the D embeddings $K \hookrightarrow \mathbb{C}$. We let $n_K(\beta)$ denote the number of elements in the set $\{\beta^{(1)}, \dots, \beta^{(D)}\}$ that are $\sim$ to β. Since each $\beta^{[j]}$, $1 \le j \le d$, occurs D/d times in $\{\beta^{(1)}, \dots, \beta^{(D)}\}$ we have that

$$n_K(\beta) = \frac{D}{d} n(\beta).$$

This implies that $D = mn_K(\beta)$. Hence we have the following corollary to Lemma 5.11.

Corollary 5.12. *For β as in Lemma* 5.10

$$h(\beta) \ge \frac{1}{4d(\log^+(D/n_K(\beta)))^3}.$$

Suppose that $S_1 = \{\beta^{[1]}, \dots, \beta^{[n]}\}$. Then, since $\beta^{[i]}/\beta^{[j]}$ is a root of unity for every $1 \le i, j \le n$, the elements $\beta^{[1]}, \dots, \beta^{[n]}$ all must have a common absolute value, say λ. We then write, for each $1 \le j \le n$,

$$\beta^{[j]} = \lambda \mathrm{e}^{2\pi \mathrm{i} \rho_j}, \tag{5.55}$$

with $0 \le \rho_j < 1$. Note that $\rho_i - \rho_j \in \mathbb{Q}$ for each $1 \le i, j \le n$ since $\beta^{[i]}/\beta^{[j]} \sim 1$, but that $\rho_i - \rho_j \notin \mathbb{Z}$ since $\beta^{[i]} \ne \beta^{[j]}$ for $i \ne j$. Thus $R = \{\rho_1, \dots, \rho_n\}$ is a denominator system as defined in §4.1. We let r_{ij} denote the smallest positive integer such that $r_{ij}(\rho_i - \rho_j) \in \mathbb{Z}$. For x a positive integer we let $u_i(x)$ denote the number of $1 \le j \le n$ such that $r_{ij} | x$. Recall that in §4.1 we said that R is *homogeneous* if $u_1(x) = \cdots = u_n(x)$ for every x.

Lemma 5.13. *Let $\{\beta^{[1]}, \dots, \beta^{[n]}\}$ be as above and define $\rho_1, \dots, \rho_n$ by* (5.55)*. Then $R = \{\rho_1, \dots, \rho_n\}$ is homogeneous.*

Proof. For x a positive integer we will denote by $v_i(x)$, $1 \le i \le n$, the number of $1 \le j \le n$ such that $v_i(x) = r_{ij}$. Since $u_i(x) = \sum_{y|x} v_i(y)$ it suffices to check that $v_1(x) = \cdots = v_n(x)$ for every x. For each $1 \le i, j \le n$ there is a positive integer s_{ij} with $\gcd(r_{ij}, s_{ij}) = 1$ such that $\beta^{[i]}/\beta^{[j]} = \mathrm{e}^{2\pi \mathrm{i} s_{ij}/r_{ij}}$. This implies that $r_{ij} = x$ precisely when $\beta^{[i]}/\beta^{[j]}$ is a primitive xth root of unity.

Fix $1 \le i \le n$ and set $v = v_i(x)$. Then there are distinct numbers $1 \le h_1, \dots, h_v \le n$ such that $\beta^{[i]}/\beta^{[h_k]}$ is a primitive xth root of unity for each $1 \le k \le v$.

Let G' be the subgroup of the Galois group G of $\mathbb{Q}(\beta^{[1]}, \dots, \beta^{[d]})$ that permutes $\beta^{[1]}, \dots, \beta^{[n]}$. Since G acts transitively on S and permutes $S_1, \dots, S_m$ we see that G' acts transitively on S_1.

Fix $1 \le j \le n$ and take $\sigma \in G'$ such that $\sigma(\beta^{[i]}) = \beta^{[j]}$. There are distinct $1 \le h'_1, \dots, h'_v \le n$ such that $\sigma(\beta^{[h_k]}) = \beta^{[h'_k]}$, for $1 \le k \le v$. Then

$$\frac{\beta^{[j]}}{\beta^{[h'_k]}} = \sigma\left(\frac{\beta^{[i]}}{\beta^{[h_k]}}\right)$$

is a primitive xth root of unity for each $1 \le k \le v$. Thus $v_j(x) \ge v = v_i(x)$. By symmetry we have $v_i(x) \ge v_j(x)$ and the result follows. □

For $\alpha, \beta, \gamma \in \overline{\mathbb{Q}}^\times$ denote by $G(\alpha : \beta : \gamma)$ the subgroup of $\overline{\mathbb{Q}}^\times$ generated by α/β and α/γ. Clearly $G(\alpha : \beta : \gamma)$ is finite if and only if $\alpha \sim \beta \sim \gamma$.

Let K be a number field of degree D with $\beta \in K$ and let $\beta^{(1)}, \dots, \beta^{(D)}$ be the images of β under the D embeddings $K \hookrightarrow \mathbb{C}$. Let $\mathcal{M} \subseteq \{1, \dots, D\}$ be such that $\{\beta^{(\sigma)} : \sigma \in \mathcal{M}\}$ is an equivalence class under $\sim$. For $l \ge 3$ and $\varepsilon > 0$ we call an l-tuple $\sigma_1, \dots, \sigma_l \in \mathcal{M}$ *ε-bad* if there are distinct i, j, k in $1 \le i, j, k \le l$ such that

$$|G(\beta^{(\sigma_i)} : \beta^{(\sigma_j)} : \beta^{(\sigma_k)})| \le \varepsilon n(\beta).$$

Lemma 5.14. *The number of ε-bad l-tuples is less than*

$$\varepsilon^{1/2} l^3 n_K(\beta)^l.$$

Proof. We may assume that for every $\sigma \in \mathcal{M}$ we have $\beta^{(\sigma)} \in \{\beta^{[1]}, \dots, \beta^{[n]}\}$, where $n = n(\beta)$. Write $\beta^{[i]}$ as in (5.55) and let $R = \{\rho_1, \dots, \rho_n\}$. We see that

$$|G(\beta^{[i]} : \beta^{[j]} : \beta^{[k]})| \le \varepsilon n$$

happens precisely when

$$\operatorname{lcm}(r_{ij}, r_{ik}) \le \varepsilon n,$$

where r_{ij} is as above. By Corollary 4.1 we know that the number of l-tuples $u_1, \dots, u_l$ in $1 \le u \le n$ with distinct i, j, k satisfying $\operatorname{lcm}(r_{u_i u_j}, r_{u_i u_k}) \le \varepsilon n$ is less than

$$\varepsilon^{1/2} l^3 n^l.$$

For each $1 \le u \le n$ there are D/d numbers $\sigma \in \mathcal{M}$ with $\beta^{(\sigma)} = \beta^{[u]}$, where d is the degree of β. Hence the number of ε-bad l-tuples is less than

$$\varepsilon^{1/2} l^3 n^l (D/d)^l = \varepsilon^{1/2} l^2 n_K(\beta)^l.$$

□

Now suppose that β is a primitive q-th root of unity, so that $\phi(q) = d$. Note that in this case $n(\beta) = d$. For $l \geq 3$ and $\varepsilon > 0$ we call an l-tuple of integers $\sigma_1, \ldots, \sigma_l$ in $1 \leq \sigma \leq D$ *ε-unpleasant* if there are distinct i, j, k in $1 \leq i, j, k \leq l$ with

$$|G(\beta^{(\sigma_i)} : \beta^{(\sigma_j)} : \beta^{(\sigma_k)})| \leq \varepsilon q.$$

Lemma 5.15. *The number of ε-unpleasant l-tuples is less than*

$$2\varepsilon^{1/2} l^3 D^l.$$

Proof. Again, write $\beta^{[1]}, \ldots, \beta^{[d]}$ as in (5.55). We have that

$$|G(\beta^{[i]} : \beta^{[j]} : \beta^{[k]})| \leq \varepsilon q$$

precisely when

$$\operatorname{lcm}(r_{ij}, r_{ik}) \leq \varepsilon q.$$

By Corollary 4.4 we know that the number of l-tuples $u_1, \ldots, u_l$ in $1 \leq u \leq d$ with distinct i, j, k satisfying $\operatorname{lcm}(r_{u_i u_j}, r_{u_i u_k}) \leq \varepsilon q$ is less than

$$2\varepsilon^{1/2} l^3 d^l.$$

For each u in $1 \leq u \leq d$ there are D/d numbers in $\{1, \ldots, D\}$ with $\beta^{(\sigma)} = \beta^{[u]}$, hence the number of ε-unpleasant l-tuples is bounded by

$$2\varepsilon^{1/2} l^3 d^l (D/d)^l = 2\varepsilon^{1/2} l^3 D^l.$$

□

5.10 Two easy Lemmas

Let K be a number field of degree D and denote by $\eta^{(\sigma)}$, $1 \leq \sigma \leq D$, the image of $\eta \in K$ under the D embeddings $K \hookrightarrow \mathbb{C}$. For $\mathbf{a} = (a_1, \ldots, a_n) \in K^n$ we set $\mathbf{a}^{(\sigma)} = (a_1^{(\sigma)}, \ldots, a_n^{(\sigma)})$.

Lemma 5.16. *Let $\mathbf{a} \in K^n$. Then $\mathbf{a}^{(1)}, \ldots, \mathbf{a}^{(D)}$ span a rational subspace of K^n.*

Proof. If $\mathbf{a} = (0, \ldots, 0)$ then the result is trivial so we may assume otherwise. Write $\mathbf{a} = (a_1, \ldots, a_n)$ and let, for each $1 \leq i \leq n$, $b_i = a_i^{(1)} + \cdots + a_i^{(D)}$. Note that $b_1, \ldots, b_n \in \mathbb{Q}$ and since $\mathbf{a}$ is nontrivial we must have at least one $b_i \neq 0$. Partition $\{1, \ldots, n\}$ into $i_1, \ldots, i_l$

and $j_1, \dots, j_m$, $l+m=n$, such that $b_{i_1} = \cdots = b_{i_l} = 0$ and $b_{j_1}, \dots, b_{j_m}$ are nonzero. Let V consist of all vectors $(X_1, \dots, X_n) \in K^n$ satisfying

$$\begin{aligned} X_{i_r} &= 0 \qquad \text{for} \quad 1 \le r \le l, \\ b_{j_r} X_{j_s} &= b_{j_s} X_{j_r} \quad \text{for} \quad 1 \le r, s \le m. \end{aligned}$$

Clearly V is a rational subspace of K^n. Also, we see that any $(X_1, \dots, X_n) \in V$ is a multiple of the vector $(b_1, \dots, b_n)$, hence is a linear combination of $\mathbf{a}^{(1)}, \dots, \mathbf{a}^{(D)}$. □

Lemma 5.17. *If $\mathbf{a} \in K^n$ but $\mathbf{a} \notin V$, for V some proper subspace of $\mathbb{C}^n$, then there are at least D/n integers σ in $1 \le \sigma \le D$ such that $\mathbf{a}^{(\sigma)} \notin V$.*

Proof. This Lemma is trivial if $D < 2n$ and so we will suppose that $D \ge 2n$. First suppose that $a_1, \dots, a_n$ are $\mathbb{Q}$-linearly independent. If the Lemma were false for $\mathbf{a}$ then there would be a set of more than $D - D/n$ vectors $\mathbf{a}^{(\sigma)}$ in V. Since V is a proper subspace of $\mathbb{C}^n$ it will suffice to show that any set of more than $D - D/n$ vectors $\mathbf{a}^{(\sigma)}$ spans $\mathbb{C}^n$.

Take $\mathcal{X} \subset \{1, \dots, D\}$ such that $|\mathcal{X}| > (1 - 1/n)D$. Let $\mathcal{Y} = \{1, \dots, D\} \backslash \mathcal{X}$, so that $|\mathcal{Y}| < D/n$. Since $a_1, \dots, a_n$ are $\mathbb{Q}$-linearly independent the matrix with columns $\mathbf{a}^{(\sigma)}$, $1 \le \sigma \le D$, will have rank n. Thus $\mathbf{a}^{(1)}, \dots, \mathbf{a}^{(D)}$ span $\mathbb{C}^n$. Without loss of generality we may suppose that $\mathbf{a}^{(1)}, \dots, \mathbf{a}^{(n)}$ are linearly independent. Suppose that $K = \mathbb{Q}(\eta)$ for some algebraic number η and let G be the Galois group of its normal closure $\mathbb{Q}(\eta^{(1)}, \dots, \eta^{(D)})$. For $g \in G$ we have $g(\eta^{(\sigma)}) = \eta^{(\sigma_g)}$, where $1_g, \dots, D_g$ is a permutation of $1, \dots, D$. Given $1 \le \sigma, \tau \le D$ there are $|G|/D$ elements $g \in G$ such that $\sigma_g = \tau$. So for any given σ the number of $g \in G$ with $\sigma_g \in \mathcal{Y}$ is $|G|\,|\mathcal{Y}|/D$. The number of $g \in G$ such that at least one of $1_g, \dots, n_g$ is in $\mathcal{Y}$ is $\le (|G|\,|\mathcal{Y}|/D)n < |G|$. Hence there is a $g \in G$ such that $1_g, \dots, n_g \in \mathcal{X}$. Since $\mathbf{a}^{(1)}, \dots, \mathbf{a}^{(n)}$ are linearly independent and, for each $1 \le i \le n$, $g(\mathbf{a}^{(i)}) = \mathbf{a}^{(i_g)}$ with $1_g, \dots, n_g \in \mathcal{X}$ we have that $\{\mathbf{a}^{(\sigma)} : \sigma \in \mathcal{X}\}$ does indeed span $\mathbb{C}^n$.

Now assume that $a_1, \dots, a_n$ are $\mathbb{Q}$-linearly dependent. Let $a_1, \dots, a_r$ be a maximal $\mathbb{Q}$-linearly independent subset. Then for $r < j \le n$ there are rational $c_{1j}, \dots, c_{rj}$ such that

$$a_j = \sum_{i=1}^{r} c_{ij} a_i.$$

Since $\mathbf{a} \notin V$, there are $\gamma_1, \dots, \gamma_n \in \mathbb{C}$ such that $\gamma_1 x_1 + \cdots + \gamma_n x_n = 0$ for all $(x_1, \dots, x_n) \in V$ but $\gamma_1 a_1 + \cdots + \gamma_n a_n \ne 0$. Setting $\gamma_i' = \gamma_i + \sum_{j=r+1}^{n} c_{ij}\gamma_j$, for $1 \le i \le r$, we have

$$\gamma_1' a_1 + \cdots + \gamma_r' a_r \ne 0.$$

Let $V' \subset \mathbb{C}^r$ be the subspace defined by $\gamma_1' x_1 + \cdots + \gamma_r' x_r = 0$. Now $\hat{\mathbf{a}} = (a_1, \dots, a_r) \notin V'$ and, by the case of the Lemma already shown, there are at least $D/r \ge D/n$ integers σ with $\hat{\mathbf{a}}^{(\sigma)} \notin V'$, so that $\gamma_1 a_1^{(\sigma)} + \cdots + \gamma_n a_n^{(\sigma)} \ne 0$, and hence $\mathbf{a}^{(\sigma)} \notin V$. □

5.11 The cases $k = 1$ and $n = 1$ of the Proposition

If $k = 1$ then $M_j(X) = b_j X$ for $1 \le j \le n$ with $b_1, \dots, b_n$ $\mathbb{Q}$-linearly independent. Then $b_1\alpha_1^x, \dots, b_n\alpha_n^x$ are $\mathbb{Q}$-linearly independent for every $x \in \mathbb{Z}$.

If $n = 1$ then we have $M_1(\mathbf{X}) = a_1X_1 + \cdots + a_kX_k$ with nonzero coefficients. The number $M(\alpha_1^x, \dots, \alpha_k^x)$ is linearly dependent over $\mathbb{Q}$ precisely when it is zero and so we are looking for solutions to the equation

$$a_1\alpha_1^x + \cdots + a_k\alpha_k^x = 0.$$

If $x \in \mathbb{Z}$ is a solution to this equation then there is a subset $\mathcal{S}(x) \subseteq \{1, \dots, k\}$ such that $1 \in \mathcal{S}(x)$ and

$$\sum_{i \in \mathcal{S}(x)} a_i\alpha_i^x = 0, \tag{5.56}$$

but no subsum of (5.56) vanishes. By Lemma 5.8, for all but at most

$$G(k) = \exp(3(6k)^{3k})$$

solutions x the set $\mathcal{S}(x)$ has the property that $\alpha_i \sim \alpha_j$ for any $i, j \in \mathcal{S}(x)$. Each exceptional solution is put in a class by itself where we take m to be any positive integer large enough to satisfy condition (b) of the proposition.

Now let $\mathcal{S} \subseteq \{1, \dots, k\}$ be a nonempty set such that $\alpha_i \sim \alpha_j$ for $i, j \in \mathcal{S}$. We consider solutions x of (5.56) having $\mathcal{S}(x) = \mathcal{S}$. We may suppose that $\mathcal{S} = \{1, \dots, h\}$, so (5.56) becomes

$$a_1\alpha_1^x + \cdots + a_h\alpha_h^x = 0. \tag{5.57}$$

Clearly we must have $h \ge 0$. Since no subsum of (5.57) vanishes Lemma 5.2 yields

$$B(h) = h^{3h^2} \le k^{3k^2}$$

vectors $\mathbf{c}^{(w)} = (c_1^{(w)}, \dots, c_h^{(w)})$, $1 \le w \le B(h)$, such that $(\alpha_1^x, \dots, \alpha_h^x)$ is proportional to some $\mathbf{c}^{(w)}$. Consider solutions with fixed w. For two such solutions x and x' we see that $(\alpha_1/\alpha_2)^x = (\alpha_1/\alpha_2)^{x'} = c_1^{(w)}/c_2^{(w)}$, so that

$$(\alpha_1/\alpha_2)^{x-x'} = 1.$$

When m is the order of α_1/α_2 we have $x \equiv x' \pmod m$, and $\operatorname{ord}(\alpha_1^m/\alpha_2^m) = 1$.

The number of sets $\mathcal{S}$ is less than 2^k and so we obtain $2^k k^{3k^2}$ classes. The total number of classes is then

$$< \exp(3(6k)^{3k}) + 2^k k^{3k^2} < \exp(4(6k)^{3k}) = \exp(4(6T)^{3T}) = H(T),$$

since $n = 1$ yields $T = k$.

We may assume henceforth that $k \ge 2$ and $n \ge 2$.

5.12 Nonvanishing of determinants

For $1 \le j \le n$ write $M_j(\mathbf{X}) = a_{1j}X_1 + \cdots + a_{kj}X_k$. Let K be a field of degree D containing $\alpha_1, \ldots, \alpha_k$ and the a_{ij}, $1 \le i \le k$ and $1 \le j \le n$. As before we denote by $\eta^{(\sigma)}$, $1 \le \sigma \le D$, the images of $\eta \in K$ under the D embeddings $K \hookrightarrow \mathbb{C}$. We will write $\mathbf{a}_i = (a_{i1}, \ldots, a_{in})$ for $1 \le i \le k$. For $1 \le \sigma \le D$ Set $M_j^{(\sigma)}(\mathbf{X}) = a_{1j}^{(\sigma)}X_1 + \cdots + a_{kj}^{(\sigma)}X_k$ for each $1 \le j \le n$ and $\mathbf{a}_i^{(\sigma)} = (a_{i1}^{(\sigma)}, \ldots, a_{in}^{(\sigma)})$ for each $1 \le i \le k$. For $x \in \mathbb{Z}$ say there are $c_1, \ldots, c_n \in \mathbb{Q}$, not all zero, such that

$$c_1 M_1(\alpha_1^x, \ldots, \alpha_k^x) + \cdots + c_n M_n(\alpha_1^x, \ldots, \alpha_k^x) = 0.$$

Then for any $1 \le \sigma \le D$ we have

$$c_1 M_1^{(\sigma)}(\alpha_1^{(\sigma)x}, \ldots, \alpha_k^{(\sigma)x}) + \cdots + c_n M_n^{(\sigma)}(\alpha_1^{(\sigma)x}, \ldots, \alpha_n^{(\sigma)x}) = 0.$$

Then the matrix with rows

$$\left(M_1^{(\sigma)}(\alpha_1^{(\sigma)x}, \ldots, \alpha_k^{(\sigma)x}), \ldots, M_n^{(\sigma)}(\alpha_1^{(\sigma)x}, \ldots, \alpha_k^{(\sigma)x})\right),$$

$1 \le \sigma \le D$, has rank $< n$. Let $\mathcal{D}(\sigma_1, \ldots, \sigma_n; x)$ be the determinant formed from the rows $\sigma_1, \ldots, \sigma_n$ of this matrix. Then

$$\mathcal{D}(\sigma_1, \ldots, \sigma_n; x) = 0. \tag{5.58}$$

We now introduce some notation. For $1 \le \sigma_1, \ldots, \sigma_n \le D$ and $1 \le i_1, \ldots, i_n \le k$ we denote by

$$\Delta\binom{\sigma_1, \ldots \sigma_n}{i_1, \ldots, i_n}$$

the determinant of the matrix with columns $\mathbf{a}_{i_1}^{(\sigma_1)}, \ldots, \mathbf{a}_{i_n}^{(\sigma_n)}$ and we set

$$\mathcal{A}\binom{\sigma_1, \ldots, \sigma_n}{i_1, \ldots, i_n} = \alpha_{i_1}^{(\sigma_1)} \cdots \alpha_{i_n}^{(\sigma_n)}.$$

Lemma 5.18. *For $1 \le \sigma_1, \ldots, \sigma_n \le D$ and $x \in \mathbb{Z}$*

$$\mathcal{D}(\sigma_1, \ldots, \sigma_n; x) = \sum_{i_1=1}^{k} \cdots \sum_{i_n=1}^{k} \Delta\binom{\sigma_1, \ldots, \sigma_n}{i_1, \ldots, i_n} \mathcal{A}\binom{\sigma_1, \ldots, \sigma_n}{i_1, \ldots, i_n}^x. \tag{5.59}$$

Proof. Since $M_j^{(\sigma)}(\alpha_1^{(\sigma)x},\dots,\alpha_k^{(\sigma)x}) = a_{1j}^{(\sigma)}\alpha_1^{(\sigma)x}+\cdots+a_{kj}^{(\sigma)}\alpha_k^{(\sigma)x}$, we have

$$\begin{aligned}\mathcal{D}(\sigma_1,\dots,\sigma_n;x) &= \begin{vmatrix} a_{11}^{(\sigma_1)}\alpha_1^{(\sigma_1)x}+\cdots+a_{k1}^{(\sigma_1)}\alpha_k^{(\sigma_1)x} & \cdots & a_{1n}^{(\sigma_1)}\alpha_1^{(\sigma_1)x}+\cdots+a_{kn}^{(\sigma_1)}\alpha_k^{(\sigma_1)x} \\ \vdots & \ddots & \vdots \\ a_{11}^{(\sigma_n)}\alpha_1^{(\sigma_n)x}+\cdots+a_{k1}^{(\sigma_n)}\alpha_k^{(\sigma_n)x} & \cdots & a_{1n}^{(\sigma_n)}\alpha_1^{(\sigma_n)x}+\cdots+a_{kn}^{(\sigma_n)}\alpha_k^{(\sigma_n)x} \end{vmatrix} \\ &= \sum_{\pi}\varepsilon_\pi(a_{1\pi(1)}^{(\sigma_1)}\alpha_1^{(\sigma_1)x}+\cdots+a_{k\pi(1)}^{(\sigma_1)}\alpha_k^{(\sigma_1)x})\cdots(a_{1\pi(n)}^{(\sigma_n)}\alpha_1^{(\sigma_n)x}+\cdots+a_{k\pi(n)}^{(\sigma_n)}\alpha_k^{(\sigma_n)x}),\end{aligned}$$

where π runs through the permutations of $1,\dots,n$ and ε_π is the sign of π. Then we have

$$\begin{aligned}\mathcal{D}(\sigma_1,\dots,\sigma_n;x) &= \sum_{i_1=1}^{k}\cdots\sum_{i_n=1}^{k}\left(\alpha_{i_1}^{(\sigma_1)}\cdots\alpha_{i_n}^{(\sigma_n)}\right)^x\sum_{\pi}\varepsilon_\pi a_{i_1\pi(1)}^{(\sigma_1)}\cdots a_{i_n\pi(n)}^{(\sigma_n)} \\ &= \sum_{i_1=1}^{k}\cdots\sum_{i_n=1}^{k}\mathcal{A}\binom{\sigma_1,\dots,\sigma_n}{i_1,\dots,i_n}^x\Delta\binom{\sigma_1,\dots,\sigma_n}{i_1,\dots,i_n}.\end{aligned}$$

□

Lemma 5.19. *When $M_1,\dots,M_n$ are linearly independent over $\mathbb{Q}$ there are certain $\sigma_1,\dots,\sigma_n$ in $1\le\sigma\le D$ and $i_1,\dots,i_n$ in $1\le i\le k$ such that*

$$\Delta\binom{\sigma_1,\dots,\sigma_n}{i_1,\dots,i_n}\neq 0.$$

Proof. By Lemma 5.16, we known that for any vector $\mathbf{v}\in K^n$ the vectors $\mathbf{v}^{(1)},\dots,\mathbf{v}^{(D)}$ span a rational subspace of $\mathbb{C}^n$. For each $1\le i\le k$ let V_i denote this rational subspace for the vector $\mathbf{a}_i$. Say that $V_1+\cdots+V_k$ is a proper subspace of $\mathbb{C}^n$. Then there are $c_1,\dots,c_n\in\mathbb{Q}$, not all zero, such that $c_1X_1+\cdots+c_nX_n=0$ holds on $V_1+\cdots+V_k$. Since $\mathbf{a}_i\in V_i$ for each $1\le i\le k$ we have that $c_1a_{i1}+\cdots+c_ka_{in}=0$ for each $1\le i\le k$. But this implies that $M_1,\dots,M_k$ are $\mathbb{Q}$-linearly dependent. Hence we have $V_1+\cdots+V_k=\mathbb{C}^n$, i.e. $\mathbb{C}^n$ is spanned by $\mathbf{a}_i^{(\sigma)}$ for $1\le i\le k$ and $1\le\sigma\le D$. Then there are certain vectors $\mathbf{a}_{i_1}^{(\sigma_1)},\dots,\mathbf{a}_{i_n}^{(\sigma_n)}$ spanning $\mathbb{C}^n$, which gives

$$\Delta\binom{\sigma_1,\dots,\sigma_n}{i_1,\dots,i_n}\neq 0.$$

□

By Lemma 5.19 there are n-tuples $u_1,\dots,u_n$ in $1\le u\le k$ and $\tau_1,\dots,\tau_n$ in $1\le\tau\le D$ such that

$$\Delta\binom{\tau_1,\dots,\tau_n}{u_1,\dots,u_n}\neq 0. \tag{5.60}$$

The n-tuple $u_1, \dots, u_n$ will be fixed from now on. After relabelling embeddings we may assume that $\tau_1 = 1$. By (5.60), we know that $\mathbf{a}_{u_2}^{(\tau_2)}$ does not lie in the subspace spanned by $\mathbf{a}_{u_1}^{(1)}, \mathbf{a}_{u_3}^{(\tau_3)}, \dots, \mathbf{a}_{u_n}^{(\tau_n)}$. By Lemma 5.17, there is a subset $\mathcal{S}_2$ of $\{1, \dots, D\}$ with $|\mathcal{S}_2| \geq D/n$ such that $\mathbf{a}_{u_2}^{(\sigma)}$ does not lie in this subspace when $\sigma \in \mathcal{S}_2$, in particular

$$\Delta \begin{pmatrix} 1, \sigma, \tau_3, \dots, \tau_n \\ u_1, u_2, u_3, \dots, u_n \end{pmatrix} \neq 0$$

whenever $\sigma \in \mathcal{S}_2$.

Let $\sigma_2 \in \mathcal{S}_2$ be given. Then $\mathbf{a}_{u_3}^{(\tau_3)}$ does not lie in the subspace spanned by the vectors $\mathbf{a}_{u_1}^{(1)}, \mathbf{a}_{u_2}^{(\sigma_2)}, \mathbf{a}_{u_4}^{(\tau_4)}, \dots, \mathbf{a}_{u_n}^{(\tau_n)}$. By Lemma 5.17 there is a set $\mathcal{S}_3(\sigma_2)$ of $\{1, \dots, D\}$ with $|\mathcal{S}_3(\sigma_2)| \geq D/n$ such that

$$\Delta \begin{pmatrix} 1, \sigma_2, \sigma_3, \tau_4, \dots, \tau_n \\ u_1, u_2, u_3, u_4, \dots, u_n \end{pmatrix} \neq 0$$

whenever $\sigma_3 \in \mathcal{S}_3(\sigma_2)$ for $\sigma_2 \in \mathcal{S}_2$.

Continuing in this way we inductively construct sets $\mathcal{S}_2, \mathcal{S}_3(\sigma_2), \dots, \mathcal{S}_n(\sigma_2, \dots, \sigma_{n-1})$ each of cardinality at least D/n such that $\mathcal{S}_j(\sigma_2, \dots, \sigma_{j-1})$ is defined when

$$\sigma_2 \in \mathcal{S}_2,\ \sigma_3 \in \mathcal{S}_3(\sigma_2),\ \dots,\ \sigma_{j-1} \in \mathcal{S}_{j-1}(\sigma_2, \dots, \sigma_{j-2}),$$

and such that

$$\Delta \begin{pmatrix} 1, \sigma_2, \dots, \sigma_n \\ u_1, u_2, \dots, u_n \end{pmatrix} \neq 0$$

whenever

$$\sigma_2 \in \mathcal{S}_2,\ \sigma_3 \in \mathcal{S}_3(\sigma_2),\ \dots,\ \sigma_n \in \mathcal{S}_n(\sigma_1, \dots, \sigma_{n-1}). \tag{5.61}$$

5.13 Selection of exponential equations

For the n-tuple $\boldsymbol{\sigma} = (\sigma_1, \dots, \sigma_n)$ in $1 \leq \sigma \leq D$ we set

$$f_{\boldsymbol{\sigma}}(x) = \sum_{i_1=1}^{k} \cdots \sum_{i_n=1}^{k} \Delta \begin{pmatrix} \sigma_1, \dots, \sigma_n \\ i_1, \dots, i_n \end{pmatrix} \mathcal{A} \begin{pmatrix} \sigma_1, \dots, \sigma_n \\ i_1, \dots, i_n \end{pmatrix}^x. \tag{5.62}$$

Then (5.58) becomes

$$f_{\boldsymbol{\sigma}}(x) = 0. \tag{5.63}$$

Let q be the number of nonzero summands in (5.62). Clearly $q \le k^n$. For each $1 \le i \le k$ write $\mathbf{a}_i = (a_1, \dots, a_{t_i}, 0, \dots, 0)$ with either $\mathbf{a}_i = (0, \dots, 0)$, in which case we set $t_i = 0$, or $a_{t_i} \neq 0$ and $t_i > 0$. Then, for $t = t_1 + \cdots + t_k$ we see that, by Lemma 5.7,

$$q \le t^{\sqrt{2t}}.$$

So we have $q \le T$ where

$$T = \min\{k^n, t^{\sqrt{2t}}\}.$$

The equation $f_{\boldsymbol{\sigma}}$ is of the type f considered in §5.8. According to Lemma 5.8, (5.63) will split with at most $G(T)$ exceptions. In order to avoid dependence on the degree of K we will select a small set of n-tuples $\boldsymbol{\sigma}$ for which we will study equation (5.63). Recall that we are assuming that $k \ge 2$ and $n \ge 2$. Moreover we may assume that $t \ge 2$ since $t = 1$ implies that we have only one summand and this case is trivial. In particular we have $T > k$, $T > n$, $T > t$ and $T \ge 4$.

Let $\mathcal{S}$ be the set of n-tuples $\boldsymbol{\sigma} = (\sigma_1, \dots, \sigma_n)$ with $\sigma_1 = 1$ and $\sigma_2, \dots, \sigma_n$ satisfying (5.61). When $\boldsymbol{\sigma} \in \mathcal{S}$ we have

$$\Delta\binom{\sigma_1, \dots, \sigma_n}{u_1, \dots, u_n} \neq 0,$$

so not all coefficients of $f_{\boldsymbol{\sigma}}$ will vanish. From now on we will restrict ourselves to $\boldsymbol{\sigma} \in \mathcal{S}$. This set $\mathcal{S}$, however, is still too large.

As in (5.50), we may write $f_{\boldsymbol{\sigma}} = f_{\boldsymbol{\sigma}1} + \cdots + f_{\boldsymbol{\sigma}g(\boldsymbol{\sigma})}$. We may suppose that $f_{\boldsymbol{\sigma}1}$ contains the summand

$$\Delta\binom{\sigma_1, \dots, \sigma_n}{u_1, \dots, u_n}\mathcal{A}\binom{\sigma_1, \dots, \sigma_n}{u_1, \dots, u_n}^x. \tag{5.64}$$

Let $\mathcal{I}(\boldsymbol{\sigma})$ be the set of n-tuples $(i_1, \dots, i_n)$ such that

$$\Delta\binom{\sigma_1, \dots, \sigma_n}{i_1, \dots, i_n} \neq 0 \text{ and } \mathcal{A}\binom{\sigma_1, \dots, \sigma_n}{i_1, \dots, i_n} \sim \mathcal{A}\binom{\sigma_1, \dots, \sigma_n}{u_1, \dots, u_n}. \tag{5.65}$$

Now $(u_1, \dots, u_n) \in \mathcal{I}(\boldsymbol{\sigma})$ and

$$f_{\boldsymbol{\sigma}1} = \sum_{(i_1,\dots,i_n)\in\mathcal{I}(\boldsymbol{\sigma})} \Delta\binom{\sigma_1, \dots, \sigma_n}{i_1, \dots, i_n}\mathcal{A}\binom{\sigma_1, \dots, \sigma_n}{i_1, \dots, i_n}^x.$$

First assume that $|\mathcal{I}(\boldsymbol{\sigma})| = 1$. Then $f_{\boldsymbol{\sigma}1}$ equals (5.64) thus $f_{\boldsymbol{\sigma}}$ contains a singleton. In this case it suffices to study (5.63) with this particular $\boldsymbol{\sigma}$ and, by Corollary 5.9, we have at most

$$G(T) < H(T)$$

solutions $x \in \mathbb{Z}$. In this case we put each solution into a class by itself choosing m large enough to satisfy condition (b) of the proposition.

We may henceforth assume that $|\mathcal{I}(\boldsymbol{\sigma})| > 1$ for each $\boldsymbol{\sigma} \in \mathcal{S}$. Since there are at most k^n n-tuples $(i_1, \dots, i_n)$ and $\mathcal{I}(\boldsymbol{\sigma})$ is a set of at most T of them, the number of possibilities for $\mathcal{I}(\boldsymbol{\sigma})$ is $\le k^{nT}$. Say we have $\sigma_1, \dots, \sigma_{n-1}$ with $\sigma_1 = 1$ and $\sigma_1, \dots, \sigma_{n-1}$ satisfying (5.61). Then for some $\sigma_n \in \mathcal{S}_n(\sigma_2, \dots, \sigma_{n-1})$ we set

$$\mathcal{I}(\sigma_1, \dots, \sigma_{n-1}) = \mathcal{I}(\sigma_1, \dots, \sigma_n)$$

and

$$\mathcal{S}'_n(\sigma_2, \dots, \sigma_{n-1}) = \{\sigma'_n \in \mathcal{S}_n(\sigma_2, \dots, \sigma_{n-1}) : \mathcal{I}(\sigma_2, \dots, \sigma_{n-1}, \sigma'_n) = \mathcal{I}(\sigma_2, \dots, \sigma_n)\}.$$

Note that regardless of our choice of σ_n we have $(u_1, \dots, u_n) \in \mathcal{I}(\sigma_1, \dots, \sigma_{n-1})$ and that $\mathcal{S}'_n(\sigma_2, \dots, \sigma_{n-1})$ is nonempty since it contains σ_n. Also note that

$$|\mathcal{S}_n(\sigma_2, \dots, \sigma_{n-1})| \le |\mathcal{S}'_n(\sigma_2, \dots, \sigma_{n-1})| k^{nT},$$

since there are at most k^{nT} possibilities for $\mathcal{I}(\boldsymbol{\sigma})$. Hence, given $\sigma_1, \dots, \sigma_{n-1}$ with $\sigma_1 = 1$ and $\sigma_2, \dots, \sigma_{n-1}$ satisfying (5.61), there is a set $\mathcal{I}(\sigma_1, \dots, \sigma_{n-1})$ such that $\mathcal{I}(\sigma_1, \dots, \sigma_{n-1}) = \mathcal{I}(\sigma_1, \dots, \sigma_{n-1}, \sigma_n)$ whenever σ_n is in the subset $\mathcal{S}'_n(\sigma_1, \dots, \sigma_{n-1})$ of $\mathcal{S}_n(\sigma_1, \dots, \sigma_{n-1})$ of cardinality

$$\ge k^{-nT} |\mathcal{S}_n(\sigma_2, \dots, \sigma_{n-1})| \ge k^{-nT}(D/n) > D/T^{1+T^2} \ge D/T^{(17/16)T^2},$$

since $T \ge 4$.

Given $\sigma_1, \dots, \sigma_{n-2}$ with $\sigma_1 = 1$ and $\sigma_2, \dots, \sigma_{n-2}$ satisfying (5.61) there is a set $\mathcal{I}(\sigma_1, \dots, \sigma_{n-2})$ such that $\mathcal{I}(\sigma_1, \dots, \sigma_{n-2}) = \mathcal{I}(\sigma_1, \dots, \sigma_{n-2}, \sigma_{n-1})$ whenever σ_{n-1} is in a subset $\mathcal{S}'_{n-1}(\sigma_2, \dots, \sigma_{n-2})$ of $\mathcal{S}_{n-1}(\sigma_2, \dots, \sigma_{n-2})$ of cardinality $> D/T^{(17/16)T^2}$.

After carrying out $n-1$ such steps we obtain a set $\mathcal{I}$ of n-tuples $(i_1, \dots, i_n)$ and sets

$$\mathcal{S}'_2,\ \mathcal{S}'_3(\sigma_2),\ \dots,\ \mathcal{S}'_n(\sigma_2, \dots, \sigma_{n-1}), \tag{5.66}$$

where $\mathcal{S}'_j(\sigma_2, \dots, \sigma_{j-1})$ is defined for

$$\sigma_2 \in \mathcal{S}'_2,\ \sigma_3 \in \mathcal{S}_3(\sigma_2),\ \dots,\ \sigma_{j-1} \in \mathcal{S}'_{j-1}(\sigma_2, \dots, \sigma_{j-2}).$$

Each of the sets (5.66) has cardinality

$$> \frac{D}{T^{(17/16)T^2}}, \tag{5.67}$$

and when $\mathcal{S}'$ consists of $\boldsymbol{\sigma}$ with $\sigma_1 = 1$ and

$$\sigma_2 \in \mathcal{S}_2',\ \sigma_3 \in \mathcal{S}_3(\sigma_2),\ \ldots,\ \sigma_n \in \mathcal{S}_n'(\sigma_2, \ldots, \sigma_{n-1}),$$

then

$$\mathcal{I}(\boldsymbol{\sigma}) = \mathcal{I} \ \text{ when } \ \boldsymbol{\sigma} \in \mathcal{S}'.$$

For $2 \le j \le n$, let $\mathcal{T}_j$ be the set of numbers $i_j \ne u_j$ in $1 \le i_j \le k$ such that

$$(i_1, \ldots, i_j, u_{j+1}, \ldots, u_n) \in \mathcal{I} \tag{5.68}$$

for certain $i_1, \ldots, i_{j-1}$, where when $j = n$ (5.68) becomes $(i_1, \ldots, i_j) \in \mathcal{I}$.

Lemma 5.20. *If $i_j \in \mathcal{T}_j$ and $\alpha_{i_j} \not\sim \alpha_{u_j}$ then*

$$h\left(\frac{\alpha_{i_j}}{\alpha_{u_j}}\right) > \frac{1}{4T^7 \deg(\alpha_{i_j}/\alpha_{u_j})}.$$

Proof. By (5.65) we have that

$$\mathcal{A}\begin{pmatrix}\sigma_1, \ldots, \sigma_j, \sigma_{j+1}, \ldots, \sigma_n \\ i_1, \ldots, i_j, u_j, \ldots, u_n\end{pmatrix} \sim \mathcal{A}\begin{pmatrix}\sigma_1, \ldots, \sigma_n \\ u_1, \ldots, u_n\end{pmatrix},$$

for any $\boldsymbol{\sigma} \in \mathcal{S}'$. Thus

$$\alpha_{i_1}^{(\sigma_1)} \cdots \alpha_{i_j}^{(\sigma_j)} \alpha_{u_{j+1}}^{(\sigma_{j+1})} \cdots \alpha_{u_n}^{(\sigma_n)} \sim \alpha_{u_1}^{(\sigma_1)} \cdots \alpha_{u_n}^{(\sigma_n)},$$

which yields

$$\left(\frac{\alpha_{i_j}}{\alpha_{u_j}}\right)^{(\sigma_j)} \sim \left(\frac{\alpha_{u_1}}{\alpha_{i_1}}\right)^{(\sigma_1)} \cdots \left(\frac{\alpha_{u_{j-1}}}{\alpha_{i_{j-1}}}\right)^{(\sigma_{j-1})}. \tag{5.69}$$

This holds when $\sigma_1 = 1$, $\sigma_2 \in \mathcal{S}_2'$, $\ldots$, $\sigma_j \in \mathcal{S}_j'(\sigma_2, \ldots, \sigma_{j-1})$. Fix such $\sigma_2, \ldots, \sigma_{j-1}$ and let σ_j range through $\mathcal{S}_j'(\sigma_2, \ldots, \sigma_{j-1})$. The right hand side of (5.69) remains fixed so that the number of $(\alpha_{i_j}/\alpha_{u_j})^{(\sigma)}$, for $1 \le \sigma \le D$, that are $\sim$ to each other is at least $|\mathcal{S}_j'(\sigma_2, \ldots, \sigma_{j-1})| > D/T^{(17/16)T^2}$, by (5.67). In the notation of §5.9,

$$n_K\left(\frac{\alpha_{i_j}}{\alpha_{u_j}}\right) > \frac{D}{T^{(17/16)T^2}}. \tag{5.70}$$

Then, by Corollary 5.9

$$h\left(\frac{\alpha_{i_j}}{\alpha_{u_j}}\right) > \frac{1}{4((17/16)T^2 \log T)^3 \deg(\alpha_{i_j}/\alpha_{u_j})} > \frac{1}{4T^7 \deg(\alpha_{i_j}/\alpha_{u_j})},$$

since $T \ge 4$. □

For $2 \le j \le n$, let $\mathcal{T}_j^* = \{\alpha_{i_j}/\alpha_{u_j} : i_j \in \mathcal{T}_j\}$. Say $\mathcal{T}_j^* = \{\beta_1, \dots, \beta_r\}$. Since $i_j \ne u_j$ we have that $r < k$ and it is possible that $r = 0$ and $\mathcal{T}_j^* = \emptyset$. We know, by Lemma 5.20 and (5.70), that for each $1 \le s \le r$

$$n_K(\beta_s) > \frac{D}{T^{(17/16)T^2}} \quad \text{and} \quad h(\beta_s) > \frac{1}{4T^7 \deg(\beta_s)}. \tag{5.71}$$

Recall the definition of $G(\alpha : \beta : \gamma)$ in §5.9.

Lemma 5.21. *Set $l = 3T$ and suppose that*

$$D > \mathrm{e}^{2T^4}. \tag{5.72}$$

Take $2 \le j \le n$ and $\sigma_1, \dots, \sigma_{j-1}$ with $\sigma_1 = 1$, $\sigma_2 \in \mathcal{S}_2'$, …, $\sigma_{j-1} \in \mathcal{S}_{j-1}'(\sigma_2, \dots, \sigma_{j-2})$. Say $\mathcal{T}_j^* = \{\beta_1, \dots, \beta_r\}$. There is a subset $\mathcal{S}_j''(\sigma_2, \dots, \sigma_{j-1})$ of $\mathcal{S}_j'(\sigma_2, \dots, \sigma_{j-1})$ of cardinality l such that for any triple of distinct numbers $\phi, \psi, \omega \in \mathcal{S}_j''(\sigma_2, \dots, \sigma_{j-1})$ and $1 \le s \le r$,

$$|G(\beta_s^{(\phi)} : \beta_s^{(\psi)} : \beta_s^{(\omega)})| > \begin{cases} T^{-8T^3} \deg \beta_s & \text{when } \beta_s \not\sim 1, \\ T^{-8T^3} \mathrm{ord} \beta_s & \text{when } \beta_s \sim 1. \end{cases} \tag{5.73}$$

Proof. For ease of notation set $\mathcal{S}_j' = \mathcal{S}_j'(\sigma_2, \dots, \sigma_{j-1})$. When $r = 0$ condition (5.73) is vacuous. Since $|\mathcal{S}_j'| > D/T^{(17/16)T^2} > 3T = l$, by (5.67) and (5.72), we can find a subset of size l.

Suppose that $r > 0$. Set

$$\varepsilon = T^{-7T^3}. \tag{5.74}$$

Note that, since $T \ge 4$,

$$108 r \varepsilon^{1/2} T^3 T^{(17/16)T^2 l} < 108 T^{4-(5/16)T^3} < 1 \tag{5.75}$$

and

$$2 l^2 T^{(17/16)T^2 l} < 18 T^{4T^3+2} < \mathrm{e}^{2T^4} < D. \tag{5.76}$$

Take $\beta_s \in \mathcal{T}_j^*$ and assume $\beta_s \not\sim 1$. We know that the numbers $\beta_s^{(\sigma)}$ with $\sigma \in \mathcal{S}_j'$ are all $\sim$ to each other. Let $\mathcal{M}$ be the set of all σ in $1 \le \sigma \le D$ for which $\beta_s^{(\sigma)}$ are $\sim$ to these numbers. By Lemma 5.14 the number of ε-bad l-tuples $\mu_1, \dots, \mu_l$ in $\mathcal{M}$ is less than $\varepsilon^{1/2} l^3 D^l$. In particular the number of ε-bad l-tuples $\mu_1, \dots, \mu_n \in \mathcal{S}_j'$ is less than $\varepsilon^{1/2} l^l D^l$. On the other hand if $\beta_s \sim 1$ then by Lemma 5.15 the number of ε-unpleasant l-tuples is less than $2\varepsilon^{1/2} l^3 D^l$. Summing over $1 \le s \le r$ we see that the number of l-tuples which are ε-bad or ε-unpleasant for some β_s is

$$< 2 r \varepsilon^{1/2} l^3 D^l = 54 r \varepsilon^{1/2} T^3 D^l < \frac{1}{2} \left(\frac{D}{T^{(17/16)T^2}} \right)^l,$$

by (5.75). The number of l-tuples for which at least two elements are equal is

$$\leq \binom{l}{2} D^{l-1} < l^2 D^{l-1} < \frac{1}{2}\left(\frac{D}{T^{(17/16)T^2}}\right)^l,$$

by (5.76). Since $|\mathcal{S}'_j| \geq D/T^{(17/16)T^2}$, the number of all possible l-tuples is $\geq (D/T^{(17/16)T^2})^l$. Thus there is an l-tuple of distinct numbers $\mu_1, \ldots, \mu_l \in \mathcal{S}'_j$ which is not ε-bad or ε-unpleasant for any $\beta_1, \ldots, \beta_r$. By definition of ε-bad and ε-unpleasant, for any distinct i, j, k if $\beta_s \not\sim 1$ we have

$$|G(\beta_s^{(\mu_i)} : \beta_s^{(\mu_j)} : \beta_s^{(\mu_k)})| > \varepsilon n(\beta_s) = \varepsilon(\deg \beta_s) n_K(\beta_s)/D > \varepsilon(\deg \beta_s)/T^{(17/16)T^2} > T^{-8T^2} \deg \beta_s,$$

by (5.71) and (5.74), and if $\beta_s \sim 1$ we have

$$|G(\beta_s^{(\mu_i)} : \beta_s^{(\mu_j)} : \beta_s^{(\mu_k)})| > \varepsilon \mathrm{ord} \beta_s > T^{-8T^3} \mathrm{ord} \beta_s.$$

Setting $\mathcal{S}''_j(\sigma_2, \ldots, \sigma_{j-1}) = \{\mu_1, \ldots, \mu_l\}$ we have (5.73) for any $\phi, \psi, \omega \in \mathcal{S}''_j(\sigma_2, \ldots, \sigma_{j-1})$. □

Condition (5.72) can always be achieved by enlarging the field K if necessary. We will assume from now on that (5.72) holds. Define $\mathcal{S}''$ to be the set of n-tuples $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_n)$ with $\sigma_1 = 1$, $\sigma_2 \in \mathcal{S}''_2$, …, $\sigma_n \in \mathcal{S}''_n(\sigma_2, \ldots, \sigma_{n-1})$. We will investigate equations (5.63) with $\sigma \in \mathcal{S}''$. Note that

$$|\mathcal{S}''| = l^{n-1} < (3T)^n.$$

5.14 Conclusion

Now each equation (5.63) splits with at most $G(q) \leq G(T)$ exceptions. If we carry this out for each $\boldsymbol{\sigma} \in \mathcal{S}''$ we have

$$\leq |\mathcal{S}''| G(T) < (3T)^T \exp(3(6T)^{3T}) \tag{5.77}$$

exceptions. We place each such solution in a class by itself and take m large enough to satisfy condition (b) of the proposition.

For nonexceptional x, each equation (5.63) with $\boldsymbol{\sigma} \in \mathcal{S}''$ splits, so that x satisfies

$$f_{\boldsymbol{\sigma}1}(x) = 0,$$

for every $\boldsymbol{\sigma} \in \mathcal{S}''$, which can be written as

$$\sum_{(i_1,\ldots,i_n)\in\mathcal{I}} \Delta\binom{\sigma_1,\ldots,\sigma_n}{i_1,\ldots,i_n}\mathcal{A}\binom{\sigma_1,\ldots,\sigma_n}{i_1,\ldots,i_n}^x = 0. \tag{5.78}$$

Recall that each summand of (5.78) satisfies (5.65) and one of the summands has $(i_1,\ldots,i_n) = (u_1,\ldots,u_n)$. We must be careful because x might be a degenerate solution of (5.78).

Given $\boldsymbol{\sigma} \in \mathcal{S}''$ and a solution $x \in \mathbb{Z}$ of (5.78), there will be a subset $\mathcal{I}(\boldsymbol{\sigma}, x) \subseteq \mathcal{I}$ containing $(u_1,\ldots,u_n)$ such that

$$\sum_{(i_1,\ldots,i_n)\in\mathcal{I}(\boldsymbol{\sigma},x)} \Delta\binom{\sigma_1,\ldots,\sigma_n}{i_1,\ldots,i_n}\mathcal{A}\binom{\sigma_1,\ldots,\sigma_n}{i_1,\ldots,i_n}x = 0, \tag{5.79}$$

but that splits no further. Since

$$\Delta\binom{\sigma_1,\ldots,\sigma_n}{u_1,\ldots,u_n} \neq 0$$

we must have $|\mathcal{I}(\boldsymbol{\sigma}, x)| > 1$. Since $|\mathcal{I}| \leq T$ there are fewer than T n-tuples $(i_1,\ldots,i_n) \neq (u_1,\ldots,u_n)$ in $\mathcal{I}$. Hence, given $\sigma_1,\ldots,\sigma_{n-1}$, there will be an n-tuple

$$\mathbf{i}(\sigma_2,\ldots,\sigma_{n-1},x) \neq (u_1,\ldots,u_n)$$

such that $\mathbf{i}(\sigma_2,\ldots,\sigma_{n-1},x) \in \mathcal{I}(\boldsymbol{\sigma},x)$ for at least l/T of the numbers $\sigma_n \in \mathcal{S}_n''(\sigma_2,\ldots,\sigma_{n-1})$. Since $l = 3T$ we can take $\mathcal{S}_n^*(\sigma_2,\ldots,\sigma_{n-1},x)$ to consist of three such numbers. Now, given $\sigma_1,\ldots,\sigma_{n-2}$, there will be an n-tuple

$$\mathbf{i}(\sigma_2,\ldots,\sigma_{n-2},x)$$

such that $\mathbf{i}(\sigma_2,\ldots,\sigma_{n-2},x) = \mathbf{i}(\sigma_2,\ldots,\sigma_{n-2},\sigma_{n-1},x)$ for at least three of the numbers σ_{n-1}. Continuing in this manner we have the n-tuples

$$\mathbf{i}(x),\ \mathbf{i}(\sigma_2,x),\ \ldots,\ \mathbf{i}(\sigma_2,\ldots,\sigma_{n-1},x)$$

and three-element sets

$$\mathcal{S}_2^*(x),\ \mathcal{S}_2^*(\sigma_2,x),\ \ldots,\ \mathcal{S}_n^*(\sigma_2,\ldots,\sigma_{n-1},x).$$

Now let $\mathcal{S}^*(x)$ consist of $\boldsymbol{\sigma} = (\sigma_1,\ldots,\sigma_n)$ with

$$\sigma_1 = 1,\ \sigma_2 \in \mathcal{S}_2^*(x),\ \ldots,\ \sigma_n \in \mathcal{S}_n^*(\sigma_2,\ldots,\sigma_{n-1},x).$$

Then for any $\boldsymbol{\sigma} \in \mathcal{S}^*(x)$ we have

$$\mathbf{i}(x) \in \mathcal{I}(\boldsymbol{\sigma}, x).$$

Let Λ be a system of three-element sets $\mathcal{S}_2^*, \mathcal{S}_3^*(\sigma_2), \ldots, \mathcal{S}_n^*(\sigma_2, \ldots, \sigma_{n-1})$, where the set $\mathcal{S}_j^*(\sigma_2, \ldots, \sigma_{j-1})$ is defined when $\sigma_2 \in \mathcal{S}_2^*$, $\ldots$, $\sigma_{j-1} \in \mathcal{S}_{j-1}^*(\sigma_2, \ldots, \sigma_{j-2})$, and where, for $2 < j \leq n$, $\mathcal{S}_j^*(\sigma_2, \ldots, \sigma_{j-1}) \subset \mathcal{S}_j''(\sigma_2, \ldots, \sigma_{j-1})$. The number of possible choices for $\mathcal{S}_2^*$ is $\leq l^3$. For fixed $\sigma_2 \in \mathcal{S}_2^*$ the number of possible choices for $\mathcal{S}_3^*(\sigma_2)$ is $\leq l^3$, so carrying this out for each $\sigma_2 \in \mathcal{S}_2^*$ we have $\leq l^9$ choices for $\mathcal{S}_3^*(\sigma_2)$. Carrying on in this manner we see that the number of possibilities for a system Λ is

$$\leq l^3 l^9 \cdots l^{3^{n-1}} < l^{3^n}.$$

When $\mathbf{i}$ is an n-tuple and Λ is a system as above, let $C(\mathbf{i}, \Lambda)$ be the class of solutions $x \in \mathbb{Z}$ with $\mathbf{i}(x) = \mathbf{i}$ and

$$\mathcal{S}_2^*(x) = \mathcal{S}_2^*,\ \mathcal{S}_3^*(\sigma_2, x) = \mathcal{S}_3^*(\sigma_2),\ \ldots,\ \mathcal{S}_n^*(\sigma_2, \ldots, \sigma_{n-1}, x) = \mathcal{S}_n^*(\sigma_2, \ldots, \sigma_{n-1})$$

whenever

$$\sigma_2 \in \mathcal{S}_2^*,\ \sigma_3 \in \mathcal{S}_3^*(\sigma_2),\ \ldots,\ \sigma_n \in \mathcal{S}_n^*(\sigma_2, \ldots, \sigma_{n-1}). \tag{5.80}$$

The number of classes is less than

$$T l^{3^n} < T(3T)^{3^T}. \tag{5.81}$$

We now study solutions in a given class $C(\mathbf{i}, \Lambda)$. Let $j = j(\mathbf{i})$ be the number $1 \leq j \leq n$ such that

$$\mathbf{i} = (i_1, \ldots, i_j, u_{j+1}, \ldots, u_n)$$

and $i_j \neq u_j$. We now restrict $\boldsymbol{\sigma}$ satisfying (5.80) even further. We fix $\sigma_1 = 1$, $\sigma_2 \in \mathcal{S}_2^*$, $\ldots$, $\sigma_{j-1} \in \mathcal{S}_{j-1}^*(\sigma_2, \ldots, \sigma_{j-2})$. Then given a choice of the three values $\phi, \psi, \theta \in \mathcal{S}_j^*(\sigma_2, \ldots, \sigma_{j-1})$ we fix $\sigma_{j+1}, \ldots, \sigma_n$ so that (5.80) holds. We now have three n-tuples, which we will denote by $\boldsymbol{\sigma}_\phi, \boldsymbol{\sigma}_\psi, \boldsymbol{\sigma}_\theta$. We will study (5.79) for these three choices of $\boldsymbol{\sigma}$.

Since each $\mathcal{I}(\boldsymbol{\sigma}_\phi, x), \mathcal{I}(\boldsymbol{\sigma}_\psi, x), \mathcal{I}(\boldsymbol{\sigma}_\theta, x)$ are in $\mathcal{I}$, which has cardinality $\leq T$, the number of possibilities for each of $\mathcal{I}(\boldsymbol{\sigma}_\phi, x), \mathcal{I}(\boldsymbol{\sigma}_\psi, x), \mathcal{I}(\boldsymbol{\sigma}_\theta, x)$ is $\leq 2^T$. We then subdivide the class $C(\mathbf{i}, \Lambda)$ into

$$2^{3T} \tag{5.82}$$

subclasses $C(\mathbf{i}, \Lambda, \mathcal{I}_\phi, \mathcal{I}_\psi, \mathcal{I}_\theta)$ such that $\mathcal{I}(\boldsymbol{\sigma}_\phi, x) = \mathcal{I}_\phi$, $\mathcal{I}(\boldsymbol{\sigma}_\psi, x) = \mathcal{I}_\psi$ and $\mathcal{I}(\boldsymbol{\sigma}_\theta, x) = \mathcal{I}_\theta$ in our subclass. Let q_ϕ, q_ψ, q_θ denote the number of nonzero summands in (5.79) with $\boldsymbol{\sigma} = \boldsymbol{\sigma}_\phi, \boldsymbol{\sigma}_\psi, \boldsymbol{\sigma}_\theta$, respectively. Note that each of these numbers is $\leq T$.

Fix $\boldsymbol{\sigma}_\phi$ for the moment. Since no subsum of (5.79) vanishes we can apply Lemma 5.2. Let $\mathcal{A}_{\boldsymbol{\sigma}}(x)$ be the vector in q_ϕ dimensional space with components

$$\mathcal{A}\binom{\sigma_1,\ldots,\sigma_n}{i_1,\ldots,i_n}x,$$

where $(i_1,\ldots,i_n)\in\mathcal{I}_\phi$. By Lemma 5.2, there are vectors $\mathbf{c}_{\boldsymbol{\sigma}}^{(w)}$, with $1\le w\le B(q_\phi)$, such that $\mathcal{A}_{\boldsymbol{\sigma}}(x)$ is proportional to some $\mathbf{c}_{\boldsymbol{\sigma}}^{(w)}$ for every solution x. We subdivide $C(\mathbf{i},\Lambda,\mathcal{I}_\phi,\mathcal{I}_\psi,\mathcal{I}_\theta)$ according to the $\mathbf{c}_{\boldsymbol{\sigma}}^{(w)}$, $1\le w\le B(q_\phi)$, to which $\mathcal{A}_{\boldsymbol{\sigma}}(x)$ is proportional. Doing this for $\boldsymbol{\sigma}_\psi$ and $\boldsymbol{\sigma}_\theta$ as well, we obtain

$$\le B(q_\phi)B(q_\psi)B(q_\theta)\le B(T)^3$$

subclasses. Combining this with (5.81) and (5.82) we see that the total number of subclasses, which we will call "classes" from now on, is

$$\le T(3T)^{3^n}2^{3T}B(T)^3<2^{4T}T^{9T^2}(3T)^{3^T}<\exp(5T^3+3^TT). \tag{5.83}$$

Consider the solutions in one such class. For $\boldsymbol{\sigma}=\boldsymbol{\sigma}_\phi$ consider the components of $\mathcal{A}_{\boldsymbol{\sigma}}(x)$ corresponding to $\mathbf{i}=(i_1,\ldots,i_n)$ and $(u_1,\ldots,u_n)$, where $\mathbf{i}$ is as above. There is a fixed constant c_ϕ such that

$$\mathcal{A}\binom{\sigma_1,\ldots,\sigma_n}{i_1,\ldots,i_n}x=c_\phi\mathcal{A}\binom{\sigma_1,\ldots,\sigma_n}{u_1,\ldots,u_n}x$$

for every solution x in our class. By our definition of $j=j(\mathbf{i})$, this yields

$$(\alpha_{i_1}^{(\sigma_1)}\cdots\alpha_{i_{j-1}}^{(\sigma_{j-1})}\alpha_{i_j}^{(\phi)})^x=c_\phi(\alpha_{u_1}^{(\sigma_1)}\cdots\alpha_{u_{j-1}}^{(\sigma_{j-1})}\alpha_{u_j}^{(\phi)})^x$$

for $\boldsymbol{\sigma}=\boldsymbol{\sigma}_\phi$. Rewriting we have

$$\left(\left(\frac{\alpha_{i_j}}{\alpha_{u_j}}\right)^{(\phi)}\right)^x=c_\phi\left(\left(\frac{\alpha_{u_1}}{\alpha_{i_1}}\right)^{(\sigma_1)}\cdots\left(\frac{\alpha_{u_{j-1}}}{\alpha_{i_{j-1}}}\right)^{(\sigma_{j-1})}\right)^x.$$

An analogous relation holds when $\boldsymbol{\sigma}=\boldsymbol{\sigma}_\psi$ or $\boldsymbol{\sigma}=\boldsymbol{\sigma}_\theta$. Taking quotients we obtain

$$\left(\frac{(\alpha_{i_j}/\alpha_{u_j})^{(\phi)}}{(\alpha_{i_j}/\alpha_{u_j})^{(\psi)}}\right)^x=\frac{c_\phi}{c_\psi}\quad\text{and}\quad\left(\frac{(\alpha_{i_j}/\alpha_{u_j})^{(\phi)}}{(\alpha_{i_j}/\alpha_{u_j})^{(\theta)}}\right)^x=\frac{c_\phi}{c_\theta}.$$

Now $\alpha_{i_j}/\alpha_{u_j}$ is one of the numbers in $\beta_s\in\mathcal{T}_j^*$, so we have

$$\left(\frac{\beta_s^{(\phi)}}{\beta_s^{(\psi)}}\right)^x=\frac{c_\phi}{c_\psi}\quad\text{and}\quad\left(\frac{\beta_s^{(\phi)}}{\beta_s^{(\theta)}}\right)^x=\frac{c_\phi}{c_\theta}.$$

Hence if x and x' are two solutions in our class, then

$$\left(\frac{\beta_s^{(\phi)}}{\beta_s^{(\psi)}}\right)^{x-x'} = \left(\frac{\beta_s^{(\phi)}}{\beta_s^{(\theta)}}\right)^{x-x'} = 1.$$

So if $|G(\beta_s^{(\phi)} : \beta_s^{(\psi)} : \beta_s^{(\theta)})| = m$, then $x \equiv x' \pmod{m}$ for any two solutions x and x' in our class. Further, by Lemma 5.21, we have

$$m > \begin{cases} T^{-8T^3} \deg \beta_s & \text{if } \beta_s \not\sim 1, \\ T^{-8T^3} \mathrm{ord} \beta_s & \text{if } \beta_s \sim 1. \end{cases}$$

When $\beta_s \not\sim 1$, we have, by (5.71),

$$h(\beta_s^m) = mh(\beta_s) > T^{-8T^3}/(8T^7) > \mathrm{e}^{-3T^3} = \hbar(T).$$

When $\beta_s \sim 1$, we note that $m | \mathrm{ord} \beta_s$, so

$$\mathrm{ord}(\beta_s^m) = m^{-1} \mathrm{ord} \beta_s < T^{-8T^2} < \mathrm{e}^{3T^3} = \hbar(T)^{-1}.$$

Now $\beta_s = \alpha_i/\alpha_j$ for some $1 \le i, j \le k$ with $i \ne j$, and so for each of our classes we have satisfied conditions (a) and (b) of the proposition.

It only remains to show that the total number of classes is at most $H(T)$. By (5.77) and (5.83) the number of classes is bounded above by

$$(3T)^T \exp(3(6T)^{3T}) + \exp(5T^3 + 3^T T) < \exp(4(6T)^{3T}) = H(T).$$

References

[1] Berstel, J. *Sur le calcul des termes d'une suite récurrente linéaire, exposé fait à l'I.R.R.I.A.* (Rocquencourt) en mars 1974.

[2] Beukers, F., The multiplicity of binary recurrrences. *Compositio Math.* **40** (1980), 251-267.

[3] Beukers, F., The zero-multiplicity of ternary recurrences. *Compositio Math.* **77** (1991), 165-177.

[4] Beukers, F. & Tijdeman, R., On the multiplicities of binary complex recurrences. *Compositio Math.* **51** (1984), 193-213.

[5] Brindza, B., Pintér, A. & Schmidt, W. M., Multiplicities of binary recurrences. *Canad. Math. Bull.* **44** (2001), 19-21.

[6] Evertse, J. H., The number of solutions of linear equations in roots of unity, *Acta Arith.* **89** (1999), 45-51.

[7] Evertse, J. H. & Schlickewei, H. P., A quantitative version of the absolute subspace theorem, *J. Reine Angew. Math.* **548** (2002), 21-127.

[8] Evertse, J. H., Schlickewei, H. P. & Schmidt, W. M., Linear equations in variables which lie in a multipliciative group. *Ann. of Math. (2)* **155** (2002), 807-836.

[9] Hardy, G. H. & Wright, E. M., *An introduction to the theory of numbers.* Fifth edition. Oxford University Press, Oxford-New York, 1979.

[10] Kubota, K. K., On a conjecture of Morgan Ward. I. *Acta Arith.* **33** (1977), 11-28.

[11] Kubota, K. K., On a conjecture of Morgan Ward. II. *Acta Arith.* **33** (1977), 29-48.

[12] Lang, S., *Algebraic Number Theory*. Second edition. Graduate Texts in Math., 110. Springer-Verlag, New York, 1994.

[13] Lech, C., A note on recurring series, *Ark. Math.* **2** (1953), 417-421.

[14] Poorten, A. J. van der & Schlickewei, H. P., Zeros of recurrence sequences, *Bull. Austral. Math. Soc.* **44** (1991), 215-223.

[15] Schlickewei, H. P., Multiplicities of rcurrence sequences, *Acta. Math.* **176** (1996), 171-243.

[16] Schlickewei, H. P. & Schmidt, W. M., The number of solutions of polynomial exponential equations, *Compositio Math.* **120** (2000), 807-836.

[17] Schmidt, W. M., The zero multiplicity of linear recurrence sequences, *Acta Math.* **182** (1999), 243-282.

[18] Schmidt, W. M., Zeros of linear recurrence sequences, *Publ. Math. Debrecen* **56** (2000), 609-630.

[19] Shorey, T. N., Poorten, A. J. van der & Tijdeman, R., Applications of the Gel'fond-Baker Method to Diophantine Equations. *Transcendence Theory: Advances and Applications* (eds. Baker, A. & Masser, D.). Academic Press, London-New York-San Francisco, 1977, 59-77.

[20] Shorey, T. N. & Tijdeman, R., *Exponential diophantine equations*. Cambridge Tracts in Math., 87. Cambridge University Press, Cambridge-New York, 1986.

[21] Voutier, P., An effective lower bound for the height of algebraic numbers. *Acta Arith.* **74** (1996), 81-95.

[22] Ward, M., *Some diophantine problems connected with linear recurrences*. Report Institute Theory of Numbers (Univ. Colorado) (1959), 250-257.