Explicit Bounds for Linear Forms in the Exponentials of Algebraic Numbers

Cheng-Chao Huang
Institute of Software, Chinese Academy of Sciences
People’s Republic of China
chengchao@nj.iscas.ac.cn

ABSTRACT
In this paper, we study linear forms

\[ \lambda = \beta_1 e^{\alpha_1} + \cdots + \beta_m e^{\alpha_m}, \]

where \( \alpha_i \) and \( \beta_i \) are algebraic numbers. An explicit lower bound for the absolute value of \( \lambda \) is proved, which is derived from "théorème de Lindemann–Weierstrass effectif" via constructive methods in algebraic computation. Besides, the existence of \( \lambda \) with an explicit upper bound is established on the result of counting algebraic numbers.

CCS CONCEPTS
• Computing methodologies → Number theory algorithms.

KEYWORDS
Lindemann–Weierstrass theorem, algebraic computation, transcendental number theory, computational number theory

1 INTRODUCTION
The study of transcendental number theory originated from the attention of Liouville [23] to a class of numbers, viz. transcendental numbers that satisfy no algebraic equation with integer coefficients. In 1844, the existence of transcendental numbers is shown for the first time by Liouville numbers constructed in the form of series, which violate the lower bound for the approximation of algebraic numbers: For an irrational algebraic number \( x \) of degree \( n \), there exists a constant \( c(x) > 0 \) such that \( |x - \frac{p}{q}| < \frac{c(x)}{q^n} \) holds for all integers \( p \) and \( q > 0 \). In 1874, Cantor [10] also showed the existence of transcendental numbers by proving that the set of algebraic numbers is countable while the set of real numbers is uncountable.

In the same period, the exponential function became a topic of interest in transcendental number theory. In 1873, Hermite [18] proved the transcendence of Euler’s number \( e \) by using auxiliary functions. Subsequently, Lindemann [22] proved that \( e^{\alpha} \) is transcendental for nonzero algebraic numbers \( \alpha \). In particular, the transcendence of \( \pi \) is shown since \( e^{\pi} \) is algebraic, which gave the negative answer to the ancient Greek question — “Squaring the Circle”.

More generally, transcendental number theory is also concerned with the algebraic independence of numbers. A set of numbers \( \alpha_1, \ldots, \alpha_m \) is algebraically independent over a number field \( K \) if there is no nonzero polynomial \( P \) in \( n \) variables with coefficients in \( K \) such that \( P(\alpha_1, \ldots, \alpha_m) = 0 \). Hereby, the transcendence of a number is a special case of \( Q \)-algebraic independence with \( m = 1 \).

On this route, in 1874, Hermite [18] considered the independence of exponentials and proved the \( Q \)-linear independence of \( e^{\alpha_1}, \ldots, e^{\alpha_m} \) for distinct rational numbers \( \alpha_1, \ldots, \alpha_m \). In 1882, a more general statement was sketched by Lindemann [22] and was later further proved rigorously by Weierstrass [38], which is known as Lindemann–Weierstrass theorem.

**Theorem 1.1 (Lindemann–Weierstrass).** For any distinct algebraic numbers \( \alpha_1, \ldots, \alpha_m \) and any nonzero algebraic numbers \( \beta_1, \ldots, \beta_m \), we have

\[ \beta_1 e^{\alpha_1} + \cdots + \beta_m e^{\alpha_m} \neq 0. \]

**Quantitative Aspects.** Transcendental number theory also investigates transcendental numbers in a quantitative way. Denote by \( \lambda \) the linear forms of exponentials of algebraic numbers, i.e.

\[ \lambda = \beta_1 e^{\alpha_1} + \cdots + \beta_m e^{\alpha_m}. \]

Notwithstanding \( \lambda \) is nonzero, how far it is from zero is a challenging problem. The study of the lower bound for such \( \lambda \) has attracted the attention of mathematicians.

In 1929, Siegel [35] presented the lower bound for a special case of the \( Q \)-linear forms \( \lambda \) with integer exponents. Specifically, let the linear forms \( \lambda = a_0 + a_1 e + \cdots + a_m e^n \) with rational coefficients and \( a = \max(|a_0|, |a_1|, \ldots, |a_m|) \). Then there exists a positive number \( e \) independent with \( m \) and the coefficients, for any \( a \geq a(m) \) we have

\[ |\lambda| \geq a^{-m} c(m)\log(m+1)/\log\log a. \]

In 1931, this result has been further improved by Mahler [25] to

\[ |\lambda| \geq a^{-m-\mu m}/\log\log a \]

for any \( \epsilon > 0 \) and \( c(\epsilon) \), where \( \mu = m\log(m\epsilon) - (m+1)\log\frac{2m+1}{\epsilon} + 1 \).

Upon the other hand, there is an equivalent formulation of Lindemann–Weierstrass theorem [6], which demonstrates \( e^{\alpha_1}, \ldots, e^{\alpha_m} \) are algebraically independent over \( Q \) when \( \alpha_1, \ldots, \alpha_m \) are \( Q \)-linear independent. Namely, \( P(e^{\alpha_1}, \ldots, e^{\alpha_m}) \neq 0 \) for any nonzero polynomial \( P \in \mathbb{Z}[x_1, \ldots, x_m] \). From this perspective, the \( Q \)-linear independence of the exponents provides useful properties to establish the lower bound for \( |P(e^{\alpha_1}, \ldots, e^{\alpha_m})| \).
In 1932, Mahler [25] gave a nontrivial lower bound for such polynomials: For a polynomial $P \in \mathbb{Z}[x_1, \ldots, x_m]$ of degree $\leq d$ and height $\leq H$, there exists a constant $H_0 = H_0(d, \alpha_1, \ldots, \alpha_m)$ such that

$$\log|P(e^{\alpha_1}, \ldots, e^{\alpha_m})| \geq -cdm\log H$$

for $H \geq H_0$ and a certain constant $c = c(\alpha_1, \ldots, \alpha_m)$. In 1994, Ably [1] improved the result by using criteria for algebraic independence [32],

$$\log|P(e^{\alpha_1}, \ldots, e^{\alpha_m})| \geq -cdm\log H + \exp(Cd m \log(d + 1)),$$

where $c = 2^{2m^3 + 18m^2 + 25m + 4}m^{m^2 + m + 2}(4D + m + 1)m^{m^2 + m + 1}$, $D = [\mathbb{Q}(\alpha_1, \ldots, \alpha_m) : \mathbb{Q}]$, and $C = C(\alpha_1, \ldots, \alpha_m)$.

Effective Aspects. The concept of "effective results" in number theory means their content can be effectively computed. The effective results are important and practical, in which the computable constants can actually be applied to solve other problems. However, it is usually difficult, in general, to prove such effective results. In indirect forms of proof, the implied constant often cannot be made computable, and the result based on Landau notation only assert the existence for such constant.

Until 1998, Sert [34] further improved Ably’s last result, and gave the first (to the best of our knowledge) effective version of the Lindemann–Weierstrass theorem ("théorème de Lindemann–Weierstrass effectif" in French), which is a breakthrough in transcendental number theory. The theorem provide a lower bound for $|P(e^{\alpha_1}, \ldots, e^{\alpha_m})|$, which can be computed in an effective manner.

Back to the subject of this paper, we focus on the linear forms

$$\lambda = \beta_1 e^{\alpha_1} + \cdots + \beta_m e^{\alpha_m},$$

where $\alpha_i$ and $\beta_i$ are algebraic numbers of bounded degrees and heights. On the one hand, our purpose is to provide a nontrivial lower bound, by which the absolute value of all such $\lambda$ are bounded from below. One the other hand, we intend to give a nontrivial upper bound, there exists a nonzero $\lambda$ whose absolute value is bounded from above by it. Moreover, both the lower bound and the upper bound obtained are expressed in an explicit way. For the former, we construct an exponential polynomial $P$ equivalent to $\lambda$ such that the effective Lindemann–Weierstrass theorem can be applied. To this end, we compute a linearly independent base of the field $\mathbb{Q}(\alpha_1, \ldots, \alpha_m)$, and the main technique here is related to the computation over algebraic extension. For the latter, we construct such $\lambda$ as the difference between two distinct linear forms. By Dirichlet’s pigeonhole principle, we bound the difference from above, that is established on the result of counting algebraic numbers. The main results are stated as follows:

**Theorem 1.2 (Main Result A).** For any distinct algebraic numbers $\alpha_1, \ldots, \alpha_m$ and nonzero algebraic numbers $\beta_1, \ldots, \beta_m$ with the maximal degree $d$ and the maximal Weil height $H$, we have

$$\log|\beta_1 e^{\alpha_1} + \cdots + \beta_m e^{\alpha_m}| \geq -e^{\delta \delta \mu} - r' m^d e^{6\delta \mu}(mh + 39 \log m + e^6),$$

in which

- $\delta = d^{2m}$,
- $\mu = m^d d^{2m} (\frac{2d}{\delta} + 3)$,
- $R = r' m^d e^{6\delta \mu}$, and $r' = 12(\frac{2}{7})^{\delta \delta^2} + 16(1 + 6d^2)(\frac{2}{7})^{\delta \delta^2} \log(9\delta^2)$ + 80(\frac{2}{7})^{\delta \delta^2} \mu$,
- $r = 82(\frac{2}{7})^{\delta \delta^2 + 2}$,

where $m = |\alpha_1| + \cdots + |\alpha_m|$, $H = |\beta_1| + \cdots + |\beta_m|$.

This work is mainly to provide an explicit version of the Lindemann–Weierstrass theorem, which is important to transcendental and computational number theory and closely related to theoretical computer science. Note that the Lindemann–Weierstrass theorem plays an important role in the study of decision problems for the first-order logic or the continuous systems involving exponential functions. It is utilised to prove the existence of the common root of two transcendental equations [3, 8, 11, 13, 30, 39] and the decidability of the sign of a transcendental numbers in such linear forms [5, 16, 29, 40]. It is also closely related to some fundamental problems in algebraic computation such as deciding the sign of polynomials at algebraic numbers. Even giving the lower bound for the absolute value of a polynomial at non-root rational numbers of bounded heights is challenging [17]. Additionally, the Lindemann–Weierstrass theorem is generalised by Schanuel’s conjecture [4], which is also widely applied in the field mentioned above [2, 12, 19, 28, 36]. Therefore, we believe the research and the results presented in this paper will potentially inspire or promote the study of these problems, especially from the perspective of computational complexity.

## 2 PRELIMINARY

In this section, we briefly review some algebraic notions, definitions, and properties, especially for some measurements of the size of polynomials and algebraic numbers. Meanwhile, we also deduce some basic results, which will be used in the analysis afterwards.

### 2.1 Polynomials and Algebraic Numbers

Let $f \in \mathbb{C}[x]$ be a polynomial

$$f(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0,$$

where $a_d \neq 0$ is called the leading coefficient of $f$ and $d = \text{deg}(f) > 0$ is the degree of $f$. The size of $f$ can be measured by the $p$-norm of the coefficient vector $(a_d, \ldots, a_0)$. Specifically, the $\infty$-norm is called the height of the polynomial:

$$H(f) = \max\{|a_0|, \ldots, |a_d|\},$$

the $1$-norm is called the length of the polynomial:

$$L(f) = |a_0| + \cdots + |a_d|.$$
the $p$-norm can also be defined in a similar way according to the coefficient vector identified with $f$.

For a commutative ring $\mathcal{R}$, the semi-norm [15] can be defined by a function $v : \mathcal{R} \to \mathbb{R}_{\geq 0}$. By further defining $v(\sum_{i=0}^{d} a_i x^i) = \Sigma_{i=0}^{d} v(a_i)$, it can be extended to the semi-norm for the polynomial ring $\mathcal{R}[x]$ and generalised to the multivariate polynomials in $\mathcal{R}[x_1, \ldots, x_n]$ via the induction on $m$. Then, the semi-norm of the resultant of two polynomials can be bounded.

**Theorem 2.1 (Theorem 2 of [15]).** Let $f$ and $g$ be polynomials over a commutative ring $\mathcal{R}$ with semi-norm $v$. Then

$$v(\text{Res}(f, g)) \leq v(f)^{\deg(g)} v(g)^{\deg(f)}.$$

Note that the length $L$ is a semi-norm function. Thus, by considering $f, g \in \mathbb{Z}[x, y]$ as univariate polynomials in $y$ over the commutative ring $\mathbb{Z}[x]$, we have the following corollary.

**Corollary 2.2.** Let $f$ and $g$ be polynomials in $\mathbb{Z}[x, y]$. Then

$$L(\text{Res}_y(f, g)) \leq L(f)^{\deg_y(g)} L(g)^{\deg_y(f)}.$$  

Let $\mathbb{Q}$ denote the field of algebraic numbers. A complex number $\alpha$ is algebraic if it is a root of a polynomial in $\mathbb{Z}[x]$. The defining polynomial of $\alpha$ is the unique polynomial of least degree, which vanishes at $\alpha$ and has co-prime integer coefficients. Here, $\alpha$ is said to be of the same degree and height of $f$. If $f$ is monic, viz. the leading coefficient is 1, then $\alpha$ is called an algebraic integer.

### 2.2 Absolute Logarithmic Height

Let $\mathcal{K}$ be a number field. For $\alpha \in \mathcal{K}$, define $H_\mathcal{K}(\alpha) = \prod_{v \in M_\mathcal{K}} \max\{|\alpha|_v\}^{d_v}$, where $M_\mathcal{K}$ is the set of normalised absolute value of $\mathcal{K}$ and $d_v$ is the degree of the completion of $\mathcal{K}$ at $v$ over $\mathbb{R}$ [37]. When $\alpha$ is an algebraic number, the absolute logarithmic height (or Weil height) $h : \mathbb{Q} \to [0, \infty)$ is defined by

$$h(\alpha) = \frac{1}{[\mathcal{K} : \mathbb{Q}]} \log H_\mathcal{K}(\alpha),$$  

and $e^{h(\alpha)}$ is called the absolute multiplicative height. Note that the Weil height does not depend on the choice of the number field $\mathcal{K}$ containing $\alpha$. Notably, for any nonzero rational number $\alpha = a/b$ in lowest terms, $h(\alpha) = \log \max\{|a|, |b|\}$.

**Property 2.1 (Property 3.3 of [37]).** Let $\alpha_1$ and $\alpha_2$ be two algebraic numbers, then

$$h(\alpha_1 \alpha_2) \leq h(\alpha_1) + h(\alpha_2),$$

$$h(\alpha_1 + \alpha_2) \leq \log 2 + h(\alpha_1) + h(\alpha_2).$$

For any algebraic number $\alpha \neq 0$ and any integer $n$, $h(\alpha^n) = |n|h(\alpha)$.

**Lemma 2.3 (Lemma 3.11 of [37]).** For an algebraic number $\alpha$ of degree $d$, we have

$$\frac{1}{d} \log H(\alpha) - \log 2 \leq h(\alpha) \leq \frac{1}{d} \log H(\alpha) + \frac{1}{2d} \log (d + 1).$$

For any vector $\alpha = (\alpha_1, \ldots, \alpha_m) \in \mathbb{K}^m$, define $H_\mathcal{K}(\alpha) = \prod_{v \in M_\mathcal{K}} \max\{|\alpha_i|_v\}^{d_v}$, and its Weil height can be further defined as Equation (2) when $\alpha_1, \ldots, \alpha_m$ are algebraic. By this definition,

$$H_\mathcal{K}(\alpha) \leq \prod_{i=1}^{m} \prod_{v \in M_\mathcal{K}} \max\{|\alpha_i|_v\}^{d_v} = \prod_{i=1}^{m} H_\mathcal{K}(\alpha_i).$$

Then, we have the following lemma:

**Lemma 2.4.** Let $\alpha = (\alpha_1, \ldots, \alpha_m) \in \mathbb{K}^m$. Then

$$h(\alpha) \leq \sum_{i=1}^{m} h(\alpha_i).$$

Let $f \in \mathbb{C}[x]$ be a nonzero polynomial of degree $d$ in the form $f(x) = a_d \prod_{i=1}^{d} (x - \alpha_i)$. The Mahler’s measure of $f$ is defined by

$$M(f) = |a_d| \prod_{i=1}^{d} \max\{1, |\alpha_i|\}.$$  

For each algebraic number $\alpha$ with defining polynomial $f \in \mathbb{Z}[x]$, its Mahler’s measure is define by $M(\alpha) = M(f)$.

**Lemma 2.5 (Lemma 3.10 of [37]).** Let $\alpha$ be an algebraic number of degree $d$. Then $h(\alpha) = \frac{1}{d} \log M(\alpha)$.

**Corollary 2.6.** Let $f \in \mathbb{Z}[x]$ be a polynomial of degree $d$ and Weil height $h$. Then each root $\alpha$ of $f$ satisfies $|\alpha| \leq e^{dh}$.

The corollary follows from the definition of Mahler’s measure, since $h$ can be expressed as

$$h = \frac{1}{d} \log |a_d| + \frac{1}{d} \sum_{i=1}^{d} \max\{0, \log|\alpha_i|\}.$$  

**Lemma 2.7.** For an algebraic number $\alpha$ of degree $d$, we have

$$\frac{1}{d} \log L(\alpha) - \log 2 \leq h(\alpha) \leq \frac{1}{d} \log L(\alpha).$$

The lemma follows from the property that $2^{-d} L(f) \leq M(f) \leq L(f)$ [26]. Note that Property 2.1, Lemma 2.3, and Lemma 2.7 will be applied frequently in the proofs afterwards. For simplicity, sometimes we may omit the references to them.

### 2.3 Discriminant of Algebraic Extension

Let $f \in \mathcal{K}[x]$ be a polynomial of the form (1). The discriminant of $f$ is defined by

$$\text{disc}(f) = \frac{(\alpha, f, f')}{a_d} \text{Res}(f, f').$$

**Lemma 2.8 (Theorem 1 of [27]).** Let $f \in \mathcal{C}[x]$ be a polynomial of degree $d$. Then

$$|\text{disc}(f)| \leq a_d^d M(f)^{2d-2}.$$  

By Lemma 2.5, we immediately have the following corollary.

**Corollary 2.9.** Let $f \in \mathbb{Z}[x]$ be a polynomial of degree $d$ and Weil height $h$. Then

$$|\text{disc}(f)| \leq a_d^{2d e^{(d-1)h}}.$$  

### 3 PRIMITIVE ELEMENT OF ALGEBRAIC EXTENSION

Recall the primitive element theorem, which is a fundamental result about field extension:

**Theorem 3.1 (Theorem 4.1.8 of [14]).** Let $\mathcal{K}$ be a finite extension of $\mathbb{Q}$ with $[\mathcal{K} : \mathbb{Q}] = n$. Then there exists an element $\theta \in \mathcal{K}$ such that

$$\mathcal{K} = \mathbb{Q}(\theta).$$

The $\theta$ is called a primitive element, whose defining polynomial is an irreducible polynomial of degree $n$.  


Let \( \alpha_1, \ldots, \alpha_m \) be \( m \) distinct algebraic numbers. According to Theorem 3.1, the algebraic extension \( \mathbb{Q}(\alpha_1, \ldots, \alpha_m) \) generated by them is a simple extension with a certain primitive element \( \theta \). We intend to give the upper bounds for the degree and the Weil height of such \( \theta \) respectively. To this end, the classic algebraic algorithm SIMPLE is invoked to construct the primitive element.

### 3.1 For Two Generators

In 1982, Loos [24] presented the algorithm SIMPLE for computing a simple extension over \( \mathbb{Q} \). Let \( \alpha \) and \( \beta \) be two algebraic numbers represented by their defining polynomials and isolating intervals, respectively. The primitive element \( \theta \) of the algebraic extension \( \mathbb{Q}(\alpha, \beta) \) can be constructed.

Denote by \( A \) and \( B \) the defining polynomials of \( \alpha \) and \( \beta \). In the algorithm SIMPLE, the resultant \( r(x, t) = \text{Res}_y(A(x - ty), B(y)) \) is constructed such that it has the root \( \theta = \alpha + \beta t \), the constant \( t \) can be further chosen to ensure that \( r(x, t) \) has no multiple roots, and \( r(x, t) \) is exactly the defining polynomial of \( \theta \). The upper bound for such constant \( t \) is given by the lemma below.

**Lemma 3.2** ([Theorem 4.10 of [41]].) There is at least an integer \( t \) among \( \deg(A) \deg(B)(\deg(B) - 1) \) distinct integers such that \( r(x, t) \) is square-free.

Following the constructive procedure in the algorithm SIMPLE, we can give the bounds for the degree and the Weil height of such \( \theta \).

**Lemma 3.3.** Let \( \alpha \) and \( \beta \) be two algebraic numbers represented by their defining polynomials \( A \) and \( B \) with the maximal degree \( d \) and the maximal Weil height \( h \). Then, there exists a primitive element \( \theta \) of the algebraic extension \( \mathbb{Q}(\alpha, \beta) \) satisfying

\[
\deg(\theta) \leq d^2 \quad \text{and} \quad h(\theta) \leq 2dh + 3\log d + 2d\log 2.
\]

**Proof.** We consider the positive integer \( t \) as a fixed constant. Then, the bound for the degree of \( \theta \) is obvious since \( \deg(r(x, t)) \leq \deg_x(A(x - ty)) \deg_y(B(y)) \). Without loss of generality, we consider the polynomial \( A \) of the form (1). For the first term of \( A(x - ty) \), we have

\[
\begin{align*}
L(A(x - ty)) &\leq \sum_{k=0}^{d} |a_k|(t + 1)^k \leq \sum_{k=0}^{d} |a_k|^2 \cdot \sum_{k=0}^{d} (t + 1)^{2k} \\
&\leq L \cdot \left( \frac{(t + 1)^2(d+1) - 1}{(t + 1)^2 - 1} \right) \leq L(t + 1)^d \left( 1 + \frac{1}{d} \right)^{2d}.
\end{align*}
\]

From Lemma 3.2, we have \( 1 \leq t \leq d(d - 1) \). By Corollary 2.2,

\[
\begin{align*}
\log L(r) &\leq 2d\log L + d^2\log(t + 1) + \frac{1}{2}d\log(1 + \frac{1}{d}) \\
&\leq 2d\log L + d^2\log(d - d^2 + 1) + \frac{1}{2}d\log 2 \\
&\leq 2d\log L + 3d^2\log d. \quad (d \geq 2)
\end{align*}
\]

With \( \deg(\theta) \geq d \), the proof is completed by Lemma 2.7. \( \square \)

**Remark 3.1.** In Section 5 of [24], Loos also gave the bound for the length of \( \theta \) without the proof. That is \( L(\theta) = O(2^{d^2}) \), in which \( L \) denotes the maximal length of \( \alpha \) and \( \beta \). By Lemma 2.7, it is not hard to check this bound is consistent with the result we obtained. However, it cannot be further used to infer explicit results since it is established on the Landau notation.

### 3.2 For Multiple Generators

Towards the situation of the algebraic extension generated by multiple algebraic numbers, we construct the primitive element by recursively applying the algorithm SIMPLE on two primitive elements of algebraic extensions generated by fewer algebraic numbers. Intuitively, we demonstrate the procedure by a tree structure in Figure 1. By regarding the \( m \) generators \( \alpha_1, \ldots, \alpha_m \) as the leaf nodes, a full binary tree with the minimal depth can be constructed from these elements to the root \( \theta \), where each non-leaf node is a primitive element computed from its two children. By applying Lemma 3.3 along this procedure, we can further bound the degree and the Weil height of the primitive element \( \theta \) constructed.

**Lemma 3.4.** Let \( \alpha_1, \ldots, \alpha_m \) be \( m \) algebraic numbers with the maximal degree \( n \) and the maximal Weil height \( h \). Then, there exists a primitive element \( \theta \) of the algebraic extension \( \mathbb{Q}(\alpha_1, \ldots, \alpha_m) \) satisfying

\[
\deg(\theta) \leq d^{2m} \quad \text{and} \quad h(\theta) \leq md^{2m}(\frac{2h}{d} + 3).
\]

**Proof.** We indicate the layer index of the nodes by \( 0, 1, \ldots, \ell \) from the layer of leaves to the root, and denote by \( d_i \) and \( h_i \) the maximal degree and the maximal Weil height of the elements at the layer of index \( i \). By Lemma 3.3, we have \( d_i \leq d_i^2 \leq d^2 \) and \( h_i \leq 2d_{i-1}h_{i-1} + D_{i-1} \), where \( D_i = 3d_i\log d_i + 2d_i\log 2 \).

So, the upper bound for the Weil height of \( \theta \) can be inferred as \( h_\ell \leq 2d_{\ell-1}(\ldots(2d_1(2d_0h_0 + D_0) + D_1) \cdots + D_{\ell-1}) \), which can be expanded as the sum of \( h' \) and \( h'' \) where

\[
\begin{align*}
h' &= 2^\ell h_0 \prod_{i=0}^{\ell-1} d_i \leq 2^\ell h_0 d_\ell^{2^\ell-1} = 2^\ell h d^{2^\ell-1}, \\
h'' &= \sum_{i=0}^{\ell-1} \left( D_i 2^{2^\ell-2} \prod_{k=i+1}^{\ell} d_k \right) \\
&\leq d^{\ell^2} 2^{2^\ell-2} \sum_{i=0}^{\ell-1} \left( 2^{3\log d + 2\log 2} \right) \\
&\leq 3d^{\ell^2} 2^{2^\ell-2}. \quad (d \geq 2)
\end{align*}
\]

Then, the proof is completed by \( \ell = \lceil \log_2 m \rceil + 1 \). \( \square \)
Remark 3.2. It should be noted that the rational univariate reduction can also be regarded as an effective version of the primitive element theorem which has been around since the work of Kronecker. The set of the defining polynomial of the generators can be considered as a system, and some similar bounds for the primitive element can be derived from the \( r \)-resultant (see [7] and Gap Theorem in Section 3.3 of [9]).

Remark 3.3. Note that in the proofs of Lemma 3.3 and 3.4, \( d \geq 2 \) is applied to scale the inequalities. However, we omit this condition to make the results more generalised because it is easy to check that the bounds obtained are still valid when \( d = 1 \) by considering \( \theta = 1 \) as the primitive element.

4 FACTORISATION OVER ALGEBRAIC EXTENSION

To convert the linear forms \( \lambda \) into the form of exponential polynomial with \( \mathbb{Q} \)-linearly independent exponents, we intend to represent the exponents \( a_1, \ldots, a_m \) by linear combinations of a basis consisting of the powers of a primitive element of \( \mathbb{Q}(a_1, \ldots, a_m) \). To this aim, the technique utilised here is to factorise the defining polynomial \( f_i(x) \) of each exponent \( a_i \) into monic irreducible factors over the algebraic extension.

In 1983, Lenstra [20] presented an algorithm for factorising polynomial over algebraic extension, which is a generalisation of the factorisation over \( \mathbb{Q} \) [21]. Specifically, for an algebraic integer \( \theta \), any polynomial \( f \) over \( \mathbb{Q}(\theta) \) can be factorised into monic irreducible factors in \( \frac{\mathbb{Z}}{\mathbb{Z}[\theta]}[x] \), where \( T \) is a positive integer. Note that a monic polynomial \( g \) in \( \frac{\mathbb{Z}}{\mathbb{Z}[\theta]}[x] \) can be represented by \( a_d \theta^d + \sum_{i=0}^{d-1} a_i \theta^i x^i \), which is identified by the \( (d+1) \)-dimensional coefficient vector. Then, the upper bound for the 2-norm of the monic factors has been provided in the proof of Proposition 3.1.1 in [20], which can be stated as below.

Theorem 4.1. Let \( \theta \) be an algebraic integer with the defining polynomial \( p_\theta \) of degree \( d_\theta \). Let \( f \in \frac{\mathbb{Z}}{\mathbb{Z}[\theta]}[x] \) with positive integer \( t \) be a monic polynomial of degree \( d \). Then, \( f \) can be factorised into the monic irreducible factors in \( \frac{\mathbb{Z}}{\mathbb{Z}[\theta]}[x] \), where \( T = t|\text{disc}(p_\theta)| \) and the 2-norm of each factor of degree \( d \leq d_\theta \) is at most

\[
H(f) (2(d+1))^{d_\theta(d_\theta-1)\frac{1}{2}}\left(\frac{1}{T}\right)^\frac{1}{2}\cdot|\text{disc}(p_\theta)|^{\frac{1}{2}}.
\]

Consider an algebraic integer \( \theta \) which is a primitive element of \( \mathbb{Q}(a_1, \ldots, a_m) \). The defining polynomial of each \( a_i \) can be factorised over \( \mathbb{Q}(\theta) \). For each \( a_i \), the monic irreducible factor in the form \( x - \frac{1}{T} p_i(\theta) \) with \( p_i(x) \in \mathbb{Z}[x] \) can be obtained. Then, we can further provide the upper bounds for \( T \) and the length of each \( p_i \).

Lemma 4.2. Let \( a_1, \ldots, a_m \) be \( m \) algebraic numbers with the maximal degree \( d \) and the maximal Weil height \( h \). Then there exists a primitive element \( \theta \) of \( \mathbb{Q}(a_1, \ldots, a_m) \) such that \( a_i = \frac{1}{T} p_i(\theta) \) for \( i = 1, \ldots, m \), where \( T \) is a positive integer and each \( p_i(x) \in \mathbb{Z}[x] \) is a polynomial satisfying

\[
T \leq e^{4md^m(\frac{2h}{d}+3)} \quad \text{and} \quad L(p_i) \leq e^{6md^m(\frac{2h}{d}+3)}.
\]

Proof. Let \( \theta \) be the primitive element of \( \mathbb{Q}(a_1, \ldots, a_m) \) constructed in Section 3. Note that the defining polynomial \( p_\theta \) of \( \theta \) may not be monic. So, we further choose the algebraic integer \( \theta = l_\theta \theta \) as a new primitive element, where \( l_\theta \) is the leading coefficient of \( p_\theta \). Denote by \( p_\theta \) its defining polynomial of degree \( d_\theta \) and Weil height \( h_\theta \). Then, it is obvious that

\[
d_\theta = d_\theta \leq d^{2m}.
\]

By Property 2.1, we can further infer that

\[
h_\theta = h(l_\theta \theta) \leq \log d_\theta + h(\theta) \leq \log h(\theta) + h(\theta) \leq d^{2m} \left(\frac{2h}{d} + 3\right) + 2 \log 2 + m d^{2m} \left(\frac{2h}{d} + 3\right)
\]

\[
\leq 2md^{2m} \left(\frac{2h}{d} + 3\right). \quad (d \geq 2)
\]

Note that the upper bound for \( h(\theta) \) is also valid when \( d = 1 \).

Let \( f_i \) be the defining polynomial of each \( a_i \) with the leading coefficient \( l_i \). We choose \( t = \prod_{i=1}^{m} l_i \) such that every \( f_i/l_i \) is a monic polynomial in \( \frac{\mathbb{Z}}{\mathbb{Z}[\theta]}[x] \). By Theorem 4.1, all the monic irreducible factors each \( f_i/l_i \) are in \( \frac{\mathbb{Z}}{\mathbb{Z}[\theta]}[x] \) with the common \( T = t|\text{disc}(p_\theta)| \).

Thus, by Corollary 2.9, we have

\[
T \leq \prod_{i=1}^{m} H(f_i) \cdot |\text{disc}(p_\theta)| \leq e^{md(\log 2)} \left(\frac{2h}{d} + 3\right)^{2md} |\text{disc}(p_\theta)| \leq e^{4md^{2m} \left(\frac{2h}{d} + 3\right) - (4md^m (\frac{2h}{d} + 3) - 2md^m \log d + \log 2)}.
\]

Note that the factorisation of \( f_i(l_i) \) is valid when \( d = 1 \).

Let \( L(p_i) \leq d_\theta \frac{1}{2} \| p_i \|_2 \leq d_\theta \frac{1}{2} \| x - \frac{1}{T} p_i(\theta) \|_2 \|

and by Theorem 4.1, we have \( \log L(p_i) \leq \log L_1 + \log L_2 \) where

\[
\log L_1 = \log(\| p_\theta \|_2^{(2d_\theta-1)} |\text{disc}(p_\theta)|^{\frac{1}{2}}),
\]

\[
= 2(d_\theta - 1) \log |p_\theta|_2 + t |\text{disc}(p_\theta)|^{\frac{1}{2}}
\]

\[
\leq d_\theta \log d_\theta \left(\frac{2h}{d} + 3\right) - (4md^m (\frac{2h}{d} + 3) + 2(d_\theta^m - 1)) |\text{disc}(p_\theta)|^{\frac{1}{2}}.
\]

\[
\log L_2 = \log(H(f_1) + \frac{1}{2} \log(2(d_\theta + 1)d_\theta^m (d_\theta - 1)^{d_\theta-1}) + \frac{1}{2}) \log(\frac{2d_\theta}{d})
\]

\[
\leq \log(H(f_1) + 2 \log d_\theta + \frac{1}{2} \log(2(d_\theta + 1)(d_\theta - 1)^{d_\theta-1}) + d_\theta \log d_\theta
\]

\[
\leq d(h + \log 2) + 4md \log d + \frac{1}{2} \log(2d + 2)
\]

\[
+ \frac{1}{2} (d_\theta^m - 1) \log(d_\theta^m - 1) + d_\theta \log 2.
\]

Then, the result follows by combining \( \log L_1 \) and \( \log L_2 \).

5 PROOF OF MAIN RESULT A

For the linear forms \( \lambda \), we intend to rewrite it into the form as \( P(e^{\alpha_1}, \ldots, e^{\alpha_M}) \), where \( P(x_1, \ldots, x_M) \) is a multivariate polynomial over \( \mathbb{Q}(\lambda_1, \ldots, \lambda_M) \), and the new exponents \( \alpha_1, \ldots, \alpha_M \) are \( \mathbb{Q} \)-linear independent. Then, the effective Lindemann–Weierstrass theorem can be applied to analyse the lower bound for \( |\lambda| \).
5.1 Constructing the Exponential Polynomial

Following Section 4, the algebraic integer $\theta$ is a primitive element of $\mathbb{Q}(\alpha_1, \ldots, \alpha_m)$, and the defining polynomials of $\alpha_1, \ldots, \alpha_m$ can be factorised into monic irreducible factors in $\mathbb{Q}(\theta)[x]$. As mentioned previously, for each exponent $\alpha_i$, there exists a polynomial $p_i \in \mathbb{Z}[x]$ such that $\alpha_i = \frac{1}{\theta} p_i(\theta)$. Namely, $\frac{1}{\theta}, \frac{1}{\theta^2}, \ldots, \frac{1}{\theta^{d_0-1}}$ form a basis, by which every $\alpha_i$ can be $\mathbb{Z}$-linearly expressed.

Without loss of generality, for $i = 1, \ldots, m$, we write

$$p_i(x) = c_{i,0} + c_{i,1}x + \cdots + c_{i,d_0-1}x^{d_0-1},$$

by which each $e^{\alpha_i} = e^{\frac{1}{\theta} p_i(\theta)}$ can be expanded as

$$e^{\alpha_i} = e^{\frac{1}{\theta} C(i,0)} e^{\frac{1}{\theta} C(i,1)} \cdots e^{\frac{1}{\theta} C(i,d_0-1)}.$$

Correspondingly, we further define the multivariate polynomial

$$P_i(x_0, x_1, \ldots, x_{d_0-1}) = x_0^{C(i,0)} x_1^{C(i,1)} \cdots x_{d_0-1}^{C(i,d_0-1)};$$

such that $e^{\alpha_i} = P_i \left( e^{\frac{1}{\theta}}, e^{\frac{1}{\theta^2}}, \ldots, e^{\frac{1}{\theta^{d_0-1}}} \right)$. Then, the linear forms can be expressed as

$$\lambda = \sum_{i=1}^m \beta_i P_i \left( e^{\frac{1}{\theta}}, e^{\frac{1}{\theta^2}}, \ldots, e^{\frac{1}{\theta^{d_0-1}}} \right).$$

Note that each $P_i$ here is still a Laurent polynomial, which may contain negative exponents caused by the negative coefficients in $p_i$. To make these exponents positive, we product each $P_i$ with a monomial with a sufficiently large degree. Specifically, for $j = 0, \ldots, d_0-1$, denote by $\hat{c}_j$ the maximal of the absolute values of negative coefficients of $x^j$ in $p_1, \ldots, p_m$, viz. $\hat{c}_j = \max_{i=1}^m |c_{i,j}|$ where the brackets denote the indicator function. Then, we write

$$C(x_0, x_1, \ldots, x_{d_0-1}) = \prod_{j=0}^{d_0-1} x_j^{\hat{c}_j}$$

and $P = \sum_{i=1}^m \beta_i P_i$.

Now, $P$ is a multivariate polynomial in $\mathbb{Z}[x_0, x_1, \ldots, x_{d_0-1}]$, and $\lambda$ can be represented by the production of $\chi'$ and $\chi''$ where

$$\chi' = C^{-1} \left( e^{\frac{1}{\theta}}, e^{\frac{1}{\theta^2}}, \ldots, e^{\frac{1}{\theta^{d_0-1}}} \right),$$

$$\chi'' = P \left( e^{\frac{1}{\theta}}, e^{\frac{1}{\theta^2}}, \ldots, e^{\frac{1}{\theta^{d_0-1}}} \right).$$

In what follows, we will give the lower bounds for $\chi'$ and $\chi''$ and combine them together to deduce the result.

5.2 Analysing the Bounds

Lower Bound for $\chi'$: Noting that $C(x_0, x_1, \ldots, x_{d_0-1})$ is a monomial, we can analyse the lower bound for $\chi'$ in a straightforward way. Noting the degree of $C$ in each $x_j$ comes from the absolute value of a certain coefficient in $p_i$, we have

$$\deg_{x_j}(C) = \hat{c}_j \leq \max_{i} L(p_i).$$

Moreover, by Corollary 2.6, we bound the absolute value of $\theta$ as

$$|\theta| \leq e^{\deg(\theta) h(\theta)} \leq e^{2mdm \left( \frac{2h}{d} + 3 \right)}.$$

Then, with the fact that $T \geq 1$, we have

$$\log |\chi'| = \log \left| C^{-1} \left( e^{\frac{1}{\theta}}, e^{\frac{1}{\theta^2}}, \ldots, e^{\frac{1}{\theta^{d_0-1}}} \right) \right|$$

$$\geq -\log \prod_{j=0}^{d_0-1} e^{\frac{c_j}{\theta^j}} = -\sum_{j=0}^{d_0-1} \frac{c_j}{\theta^j} |\theta|^j$$

$$\geq -\max L(p_i) \sum_{j=0}^{d_0-1} |\theta|^j.$$

For the case that $|\theta| \geq 2$, we have

$$\sum_{j=0}^{d_0-1} |\theta|^j \leq |\theta|^{d_0} \leq e^{2mdm \left( \frac{2h}{d} + 3 \right)}.$$

For the case that $|\theta| < 2$, it is obviously that $\sum_{j=0}^{d_0-1} |\theta|^j < 2^{d_0}$, that means the upper bound above is still valid. Then, with the bound for $L(p_i)$ from Lemma 4.2, we immediately have

$$\log |\chi'| \geq -e^{2mdm \left( \frac{2h}{d} + 3 \right)}.$$

Lower Bound for $\chi''$: Recall that $\chi''$ is in the form of exponential polynomial with $\mathbb{Q}$-linearly independent exponents. So, the effective Lindemann–Weierstrass theorem can be applied to analyse its lower bound. To be self-contained, we present this theorem as below (with slight adjustment on the notations).

**Theorem 5.1** (Sert, Theorem 3 of [34]). Let $\alpha_1, \ldots, \alpha_m \in \mathbb{K}$ be linear independent over $\mathbb{Q}$, and $\alpha = (\alpha_1, \ldots, \alpha_m)$. Let $P \in \mathbb{K}[X_1, \ldots, X_m]$ be a nonzero polynomial of degree $\leq dp$ ($dp \geq 1$) with the coefficients $\beta = (\beta_1, \ldots, \beta_m)$. Then

$$\log |P(e^{\alpha_1}, \ldots, e^{\alpha_m})|$$

$$\geq -rdp \left( h(\beta) + \frac{39}{32d^2} \log |\beta| + e^{rdp^3+d_0^3+72d^3} \right),$$

in which $D$ is the degree of $\mathbb{K}$ over $\mathbb{Q}$, $\Delta_\beta$ is the discriminant of $\mathbb{Q}(\beta_1, \ldots, \beta_m)$, and

$\hat{\alpha} = \max \{1, \max |\alpha_i|\}$

$r = 41 \cdot 2^{-3M+1} \cdot 2^{M+1} \cdot 2^{M+1}$

$r' = 2^{-3M+1} \cdot 2^{M+1} \cdot 2^{M+1}$

$r'' = (1+6d)2^{-3M+3} \cdot 2^{M+1} \cdot 2^{M+1} \log(9MD)$

$+ 2^{-3M+3} \cdot 2^{M+1} \cdot 2^{M+1} \log(9MD)$

$r''' = (1+6d)2^{-3M+3} \cdot 2^{M+1} \cdot 2^{M+1} \log(9MD)$

Then, according the bounds in Lemma 3.4 and 4.1, we give the explicit upper bounds related to the following objects, that appear in effective Lindemann–Weierstrass theorem as parameters.

- For the algebraic extensions:
  - Let $K$ be the algebraic extension of $\mathbb{Q}$ generated by the exponents $\frac{1}{\theta}, \frac{1}{\theta^2}, \ldots, \frac{1}{\theta^{d_0-1}}$ and all the coefficients in $P$, which implies $K \subseteq \mathbb{Q}((\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_m))$. By Lemma 3.4, we have
    $$D = |K : \mathbb{Q}| \leq d^{4M}.$$
  - Furthermore, let $\delta'$ (degree $d_0'$ and Weil height $h'_{\delta}$) be the primitive element of $\mathbb{Q}(\beta_1, \ldots, \beta_m)$. Then, the discriminant of $\mathbb{Q}(\delta')$ is equal to the discriminant of the defining polynomial of $\delta'$. By
Corollary 2.9 and Lemma 3.4, we have
\[
\log|\Delta_2| = \log|\text{disc}(Q(\theta'))| \\
\leq d_P \log d_P + 2d_\theta (d_T - 1) h_\theta \\
\leq 2md_2m \log d + 2d_2m (d_2m - 1) m d_2m (2h + 3) \\
\leq 2md_2m (2h + 3).
\]

- For the polynomial:
Let \( P \) be the polynomial we constructed in Equation (5). Denote by \( M \) the number of variables of \( P \), and we have
\[
M \leq d_\theta \leq d_2m.
\]
Recall the form of \( P \), in which each \( c_{i,j} \) is the coefficient of \( x^i \) in \( p_i(x) \). Then, we can define \( \lambda' = \arg \max_i \sum_j c_{i,j} \), which implies \( P_i \) has the maximal degree among \( P_1, \ldots, P_m \). Thus, with the fact that \( C \) and each \( P_i \) are monomials, we have
\[
d_P \leq \deg(C) + \deg(P_i).
\]

Thus, by Lemma 4.2, we have
\[
d_P \leq m e^{6md_2m (2h + 3)}.
\]
Note that the coefficients in \( P \) are exactly the coefficients \( \beta_1, \ldots, \beta_m \) appearing in the linear forms \( \lambda \). So, by Lemma 2.4, we have
\[
h(\beta) \leq m \sum_{i \neq i'} L(p_i).
\]

- For the exponents:
Let \( \alpha = (\frac{1}{2}, \frac{1}{2}, \ldots, \frac{1}{2}) \theta^{-1} \). For the case \( |\theta| \geq 1 \), we have
\[
\max |a_i| \leq |\theta|^{d_\theta} \leq e^{2md_2m (2h + 3)}.
\]
Obviously, the bound above also holds when \( |\theta| < 1 \). Moreover, according to Property 2.1, we have
\[
h(\frac{1}{\theta}) \leq h(T) + i h(\theta) = \log T + i h_\theta.
\]
Then, by combining this with Lemma 2.4, we have
\[
h(\alpha) \leq \sum_{i=0}^{d_2-1} h(\frac{1}{\theta} \theta^i) \leq d_\theta \log T + d_\theta (d_\theta - 1) h_\theta \\
\leq 4md_2m (2h + 3) + d_2m (d_2m - 1) m d_2m (2h + 3) \\
\leq 5md_2m (2h + 3).
\]

Finally, for simplicity, we write
\[
\delta = d_2m \quad \text{and} \quad \mu = md_2m (2h + 3),
\]
by which these bounds obtained can be rewritten as
\[
D \leq 8\delta, \quad M \leq 2\delta, \quad d_P \leq me^{6\mu}, \quad \hat{\alpha} \leq e^{2\delta}, \quad h(\alpha) \leq 5\delta^2, \quad h(\beta) \leq mh, \quad \log |\Delta_2| \leq 2\mu.
\]
Then, by substituting all these bounds into Theorem 5.1, we have
\[
\log |\lambda''| \geq -r m^{6\delta^2}(m + 39\frac{\delta}{\mu} + e^{\delta}),
\]
in which
\[
R = r m^{6\delta^2} \mu + r'' m^{4\delta^2} (\log m + 6\mu) + 72e^{2\delta},
\]
\[
r' = 12(\frac{9}{2})^{\delta} \delta^{3\delta + 2} + 16(1 + 6\delta^2)(\frac{9}{2})^{\delta} \delta^{3\delta} \log (9\delta^3) + 80(\frac{9}{2})^{\delta} \delta^{3\delta + 4}(1 + 6\delta) \mu,
\]
\[
r'' = (1 + 6\delta^2)(\frac{1}{2})^{\delta} \delta^{3\delta}.
\]
Combining the lower bound \( \log |\lambda''| \geq -e^{6\delta^2} \) in Inequality (6), we immediately complete the proof of Main Result A.

6. PROOF OF MAIN RESULT B
In this section, for algebraic numbers \( a_i \) and \( b_i \) of bounded degrees and heights, we establish a nontrivial upper bound that there exists a nonzero \( \lambda = \beta_1 e^{\alpha_1} + \cdots + \beta_m e^{\alpha_m} \) whose absolute value is bounded from above by it. We construct such \( \lambda \) by the difference between two distinct linear forms, then the upper bound can be given via Dirichlet’s pigeonhole principle.

6.1 Constructing Linear Forms
Denote by \( \overline{Q}_d(H) \) the set of algebraic numbers having degree \( d \) over \( Q \) and the absolute multiplicative height at most \( H \). Now, we consider the set \( \Lambda \) which consists of all the linear forms \( \sum_i \beta_i e^{\alpha_i} \) satisfying the following conditions:
- the linear form contains at most \( \ell \) terms,
- any \( a_i \) and \( b_i \) come from \( \overline{Q}_d(H_1) \) and \( \overline{Q}_d(H_2) \), respectively,
- the absolute values of \( a_i \) and \( b_i \) are less than or equal to 1.

Let \( \overline{Q}_d(H) \) be the set of algebraic numbers with degree \( d \), the maximal absolute multiplicative height \( H \), and the maximal absolute value 1. Then, we can count the number of the elements in \( \Lambda \).

Consider the linear forms contain exactly \( k \) terms. Noting that the exponents \( a_1, \ldots, a_k \) in the linear forms are distinct, they can be chosen by \( k \)-combinations of the elements in \( \overline{Q}_d(H_1) \). The coefficient of each \( e^{\alpha_i} \) can be chosen as any nonzero element in \( \overline{Q}_d(H_2) \). So we derive that
\[
|\Lambda| \geq \sum_{k=1}^{\ell} N_2^k \left( \frac{N_1}{k} \right)^k,
\]
in which \( N_1 = |\overline{Q}_d(H_1)| \) and \( N_2 = |\overline{Q}_d(H_2) \setminus \{0\}| \). Then, with the assumption that \( N_1 \geq \ell + 1 \) and \( N_2 \geq 1 \), we have
\[
|\Lambda| \geq \sum_{k=1}^{\ell} N_2^k \left( \frac{N_1}{k} \right)^k \geq \sum_{k=1}^{\ell} N_2^k \left( \frac{N_1}{\ell} \right)^k
\]
\[
= \left( \frac{N_1 N_2}{\ell} \right)^{\ell} \left( 1 - \frac{N_1 N_2}{\ell} \right)^{\ell - 1} \left( \frac{N_1 N_2}{\ell} \right)^{\ell}. \tag{8}
\]
In order to apply the pigeonhole principle, we should ensure that for any \( \lambda_1, \lambda_2 \in \Lambda \), the difference \( \lambda_1 - \lambda_2 \) is a linear form satisfying the conditions: (i) it contains at most \( m \) terms, and (ii) its exponents and coefficients are of degrees \( d \) and absolute multiplicative heights \( \leq H \). Constructively, we can choose the setting as follows:

\[
\ell \geq \left\lceil \frac{\ell}{2} \right\rceil, \quad \text{since} \quad \lambda_1 - \lambda_2 \text{ has at most } 2\ell \text{ terms}, \quad d_1 = d \quad \text{and} \quad H_1 = H, \quad \text{since all the exponents in } \lambda_1 - \lambda_2 \text{ directly come from } \lambda_1 \text{ and } \lambda_2, \quad d_2 = \sqrt{\ell} \quad \text{and} \quad H_2 = \sqrt{H^2}, \quad \text{since the coefficient in } \lambda_1 - \lambda_2 \text{ may come from the difference between two terms with the same } e^{\alpha i}.
\]

### 6.2 Analysing the Bound

For each linear form \( \lambda = \sum \beta_i e^{\alpha_i} \) in \( \Lambda \), we can bound its absolute value as

\[
|\lambda| \leq \sum_{i=1}^{\ell} |\beta_i| e^{\alpha_i} \leq c\ell \leq \frac{1}{2} em,
\]

because \( \lambda \) contains at most \( \ell \leq \frac{e m}{2} \) terms and the absolute values of \( \alpha_i \) and \( \beta_i \) are at most 1. Thus, we can define

\[
\Omega = \left\{ x + yi \in \mathbb{C} \mid x, y \in [-\frac{1}{2}em, \frac{1}{2}em] \right\}
\]

such that \( \Lambda \subset \Omega \). Note that \( \Omega \) indicates the square in the complex plane, which is centered at the origin and has the length \( em \). We further split \( \Omega \) into \( t \times t \) grid such that each cell is a square with the same length \( em^{-1/2} \). Then, it is obvious that each \( \lambda \in \Lambda \) will be contained by one of these cells (see Figure 2).

![Figure 2: Each element of \( \lambda \) is contained by the circle centered at the origin and with radius \( ct \). When \( |\lambda| \geq t^2 + 1 \), two distinct elements of \( \Lambda \) will be contained by the same cell.](image)

By Dirichlet’s pigeonhole principle, if \( |\lambda| \geq t^2 + 1 \) holds, then we have that there exists at least one cell containing more than one element of \( \Lambda \). In other words, there exist \( \lambda_1, \lambda_2 \in \Lambda \) such that

\[
|\lambda_1 - \lambda_2| \leq \frac{\sqrt{2}em}{t}.
\]

Thus, by Inequality (8), let

\[
t = \left\lfloor \sqrt{\left( \frac{N_1 N_2}{c} \right)^\ell} \right\rfloor
\]

such that \( t^2 \) is a positive integer less than \( |\lambda| \).

Note the fact that \( \log x - \log |x| < 1 \) for any \( x \geq 1 \). Then, by Inequality (9), we immediately obtain the upper bound as

\[
\log|\lambda_1 - \lambda_2| \leq -\log t + \log(\sqrt{2}em)
\]

\[
\leq -\log \left( \frac{N_1 N_2}{t^\ell} \right) + \log(\sqrt{2}em) + 1
\]

\[
\leq -\frac{1}{2} \log \frac{N_1 N_2}{t^\ell} + \log m + \log \sqrt{2} + 2.
\]

To make this upper bound explicit, the remaining issue is to provide the lower bounds for the numbers of elements in \( \overline{Q}_d(H_1) \) and \( \overline{Q}_d(H_2) \), respectively.

As a case of one-dimensional of Northcott’s theorem [31], it is well known that \( \overline{Q}_d(H) \) contains finitely many elements, and counting these elements is also an important problem in number theory. In 1993, Schmidt [33] first proved the explicit lower bound for the number of the elements in \( \overline{Q}_d(H) \).

**Lemma 6.1 (Schmidt, Theorem of [33]).** Let \( \overline{Q}_d(H) \) be the set of algebraic numbers with degree \( d \) and the maximal absolute multiplicative height \( H \). Then

\[
|\overline{Q}_d(H)| > 6^{-d(d+1)}H^{d(d+1)} \quad \text{when } H^d \geq 2.
\]

In our situation, we focus on the elements in \( \overline{Q}_d(H) \) whose absolute values are less than or equal to 1. Consider any nonzero algebraic number \( \alpha \in \overline{Q}_d(H) \) with \( |\alpha| > 1 \), and denote by \( f(x) \) the defining polynomial of \( \alpha \). It is not hard to check that \( \alpha^{-1} \) is a root of the polynomial \( g(z) = z^d f(\tfrac{1}{z}) \).

Also, by Property 2.1, we further have \( h(\alpha^{-1}) = h(\alpha) \), that implies \( \alpha^{-1} \) is also contained in \( \overline{Q}_d(H) \). With the fact that \( |\alpha^{-1}| = |\alpha|^{-1} \), we immediately infer that \( |\overline{Q}_d(H)| \geq \frac{1}{2} |\overline{Q}_d(H)| \). Thus, according to Theorem 6.1, we finally have

\[
|\overline{Q}_d(H)| > \frac{1}{2} 6^{-d(d+1)}H^{d(d+1)} \quad \text{when } H^d \geq 2.
\]

Therefore, we can write

\[
n_1 = \frac{1}{2} 6^{-d(d+1)}H^{d(d+1)},
\]

\[
n_2 = \frac{1}{2} 6^{-d(d-1)} \sqrt{H^2 (d(d-1)) d^2},
\]

such that \( N_1 \) and \( N_2 \) are positive integers greater than \( n_1 \) and \( n_2 \), respectively. This complete the proof of Main Result B.

**Remark 6.1.** There are some conditions here to make the result hold. On the one hand, we need \( n_1 \geq t \) and \( n_2 \geq 1 \), which imply the assumptions \( N_1 \geq t + 1 \) and \( N_2 \geq 2 \) for Inequality (8). The aim is to ensure that we have enough algebraic numbers to construct the linear forms. Besides, they can also imply the conditions \( H_1^d \geq 2 \) and \( H_2^d \geq 2 \) required as in Lemma 6.1.

On the other hand, we have \( m \geq 2 \), which comes from the setting that \( \ell = \left\lceil \frac{\ell}{2} \right\rceil \) to ensures that \( \ell \) is nonzero. However, with the fact that \( \lim_{\ell \to 0} \ell \log \ell = 0 \), the upper bound we obtained is also clearly valid for the case \( m = 1 \). So, for simplicity, we omit this condition in the result. Actually, the situation of the linear forms containing one term is trivial because \( \log e^{\alpha i} \) reaches its minimal absolute value when both \( |\alpha| \) and \( |\beta| \) reach their minimal values, respectively.
