1 Introduction

There have been two approaches to linear forms in the logarithms of algebraic numbers: the first is the Gelfond-Baker method (with improvements using commutative algebra), the second is the Schneider-Laurent method. Both approaches use auxiliary functions which, in the latter, are called interpolation determinants.

Consider the special case that \( \Lambda = \sum_{j=1}^{n} b_j \log \alpha_j \neq 0 \) with \( \alpha_j = a_{j,1}/a_{j,2} \) (\( j = 1, \ldots, n \)) and all \( a_{j,1}, a_{j,2}, b_j \) integers.

The former method yields

\[
\log |\Lambda| > -C_1 B \prod_{j=1}^{n} \log a_j
\]

for some constant \( C_1 \) independent of \( \{\alpha_j, b_j : j = 1, \ldots, n\} \), where \( B \geq \max\{b_1, \ldots, b_n, 4\} \) and \( a_j \geq \max\{|a_{j,1}|, |a_{j,2}|, 4\} \).

In contrast, the latter yields

\[
\log |\Lambda| > -C_2 B^2 \prod_{j=1}^{n} \log a_j
\]

for some constant \( C_2 \) independent of \( \{\alpha_j, b_j : j = 1, \ldots, n\} \).

For the latter approach to be worthwhile it therefore behoves one to obtain a far smaller value for \( C_2 \) than \( C_1 \). This is especially true since the size of integer solutions of certain Diophantine equations is often bounded in terms of either of these constants.

The main constraint in lowering the value of \( C_2 \) is the non-vanishing of the interpolation determinant; that is, ensuring that the interpolation matrix has full row rank. Essentially, this boils down to a result about sets (related to grids) of zeros of polynomials.
Let $L$ be a grid in $\mathbb{Q}^{n-1}$; that is, $L = \mathbb{Z}^{n-1} + \mathbb{Z}(\beta_1, \ldots, \beta_{n-1})$ for some $\beta_1, \ldots, \beta_{n-1} \in \mathbb{Q}$. Let $\beta_j = b_j/b_n$ for $j = 1, \ldots, n - 1$ with $b_1, \ldots, b_n \in \mathbb{Z}$ all non-zero. We may consider $L$ as the $\mathbb{Z}$-submodule of $\mathbb{Q}^{n-1}$ generated by $(1, 0, \ldots, 0)$, $(0, 1, 0, \ldots, 0)$, $(0, 0, 1)$ and $(\beta_1, \ldots, \beta_{n-1})$. Let $\alpha_1, \ldots, \alpha_n$ be positive rational numbers that are multiplicatively independent. Suppose that $\{b_1, \ldots, b_n\}$ satisfies no linear dependence relation over $\mathbb{Z}$ with “small” coefficients. Let $R_1, \ldots, R_n \in \mathbb{Z}^+$ and $L^*$ be the subset of $\mathbb{Q}^n$ given by:

$$L^* = \{(r_1 + r_3\beta_1, r_2 + r_3\beta_{n-1}, \alpha_1^{r_1} \cdot \alpha_n^{r_n}) : 0 \leq r_j \leq R_j (j = 1, \ldots, n)\}.$$ 

If $L^*$ is a set of zeros of $P(X_1, \ldots, X_n) \in \mathbb{T}[X_1, \ldots, X_n]\{0\}$, then the total degree of $P$ must be quite large in terms of the size of $L^*$.

We will make this precise in the next section and then use Bézout’s Theorem and permutations to prove the result in the special case that $n = 3$, and explain how to extend the theory to the more complicated (combinatorially messier) case that $n = 4$. This was the essential new ingredient in [BBGMS] and [E] and is the part that most naturally belongs in these proceedings.

In the last section we will compare $C_1$ and $C_2$ in a special case (one of the few where this approach is very advantageous) and give an application to Catalan’s Conjecture (that no two consecutive integers other than 8 & 9 can both be proper powers).

It should be noted that the value of $C_2$ is very much better when $n = 2$ (see [LMN]) since the required lemma concerning polynomials is in a single variable and so quite sharp: a polynomial of degree $n$ cannot have more than $n$ roots in any subset of a field. Things become more interesting (and require extra techniques) only when $n \geq 3$ — a common phenomenon with linear forms in logarithms.

### 2 The Main Theorem ($n = 3$)

We first consider the easier case that $n = 3$ and later discuss the modifications that are needed for $n = 4$.

So let $b_1, b_2, b_3$ be fixed non-zero integers and $\beta_j = b_j/b_3$ ($j = 1, 2, 3$). Let $L$ be the grid generated by $\beta_1$ and $\beta_2$; that is, $L = \mathbb{Z}^2 + \mathbb{Z}(\beta_1, \beta_2)$, the union of $|b_3|$ lattices in $\mathbb{Q}^2$. Let $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{Q}_+$ and $R_1, R_2, R_3 \in \mathbb{Z}_+$. Let $L^* = \{(r_1 + r_3\beta_1, r_2 + r_3\beta_2, \alpha_1^{r_1} \cdot \alpha_2^{r_2} \cdot \alpha_3^{r_3}) : 0 \leq r_j \leq R_j (j = 1, 2, 3)\}$. 

2
We define \((b_1, b_2, b_3) \subseteq \mathbb{Z}^3\) to be \((R_1, R_2, R_3)\)-linearly dependent over \(Z\) if there are \(d_j \in \mathbb{Z}\) \((j = 1, 2, 3)\) not all zero such that \(\sum_{j=1}^3 d_j b_j = 0\) with \(|d_1|, |d_2| \leq R_3\) and \(|d_3| \leq \min\{R_1, R_2, R_3\}\); and if \(d_3 = 0\), then \(|d_1| \leq R_2\) and \(|d_2| \leq R_1\). Note that the definition refers to the ordered triple \((b_1, b_2, b_3)\) not just the set \(\{b_1, b_2, b_3\}\).

**Theorem A (Improved Zero Estimate)**

Suppose that \(\{\alpha_1, \alpha_2, \alpha_3\}\) is multiplicatively independent and \(b_1, b_2, b_3\) are non-zero integers. Let \(D_1, D_2, R_1, R_2, R_3, S_1, S_2, S_3, T_1, T_2, T_3 \in \mathbb{Z}_+\) be at least 4, and \(\beta_j = b_j / b_3\) \((j = 1, 2)\). Let \(L^* = \{(r_1 + r_3 \beta_1, r_2 + r_3 \beta_2, \alpha_1^r \alpha_2^s \alpha_3^t) : 0 \leq r_j \leq R_j \ (j = 1, 2, 3)\}\). Assume that \(D_1 \geq 2D_2\), \(S_2 \geq S_1\) and \(S_j + T_j < R_j\) for \(j = 1, 2, 3\). IF

\[
\begin{align*}
(1) & \quad 4(S_1 + 1)(S_2 + 1) \geq S_3 + 1, \\
(2) & \quad 4(S_1 + 1)(S_3 + 1) \geq S_2 + 1, \\
(3) & \quad (S_1 + 1)(S_2 + 1)(S_3 + 1) \geq 8(D_1 + D_2 + 1)^2, \text{ and} \\
(4) & \quad (T_1 + 1)(T_2 + 1)(T_3 + 1) > 12D_1^2 D_2,
\end{align*}
\]

THEN no non-zero polynomial \(P(X, Y, Z) \in \mathbb{Q}[X, Y, Z]\) with \(\deg_X(P) + \deg_Y(P) \leq D_1\) and \(\deg_Z(P) \leq D_2\) can have \(L^*\) as its set of zeros unless \((b_1, b_2, b_3)\) is \((R_1, R_2, R_3)\)-linearly dependent.

This Zero Estimate is similar to (but sharper than) Philippon’s [P]. The proof follows from elementary theory of algebraic groups and improved combinatorial estimates. The latter is obtained by an analysis of the intersection of translates of hypersurfaces under the group \(\mathbb{Q}^2 \times \mathbb{Q}^*\); and it is the action of this latter group on an appropriate set that allows us to use orbits and stabilisers to improve Philippon’s Zero Estimate.

### 3 Background: algebraic geometry

As is standard, if \(\mathcal{P}\) is a set of polynomials in \(n\) commuting variables over a field \(K\), we will write \(\mathcal{V}(\mathcal{P})\) for the set of points of \(K^n\) at which each \(P \in \mathcal{P}\) is zero, and call \(\mathcal{V}(\mathcal{P})\) an algebraic set. If \(\mathcal{P}\) is generated by a single irreducible polynomial, then \(\mathcal{V}(\mathcal{P})\) is called a variety.

Throughout we will work in the group \(G = \mathbb{Q}^{n-1} \times \mathbb{Q}^*\); that is, additive on the first \(n - 1\) coordinates and multiplicative on the last. Accordingly, if \(x = (x_1, ..., x_n)\) and \(y = (y_1, ..., y_n)\) belong to \(\mathbb{Q}^{n-1} \times \mathbb{Q}^*\), we will write \(x + y\) for \((x_1 + y_1, ..., x_{n-1} + y_{n-1}, x_n y_n)\) and \(-x\) for \((-x_1, ..., -x_{n-1}, 1/x_n)\). We will write \(t_x\) for the map \(y \mapsto y + x\).
A subgroup of $G$ that is also an algebraic set is called an algebraic subgroup; it has the form $U \times T_m$ for some vector subspace $U$ of $\mathbb{Q}^{n-1}$ and non-negative integer $m$, where $T_m$ is the set of $m^{th}$ roots of unity; $T_0 = \mathbb{Q}^*$ (please see [H]).

An algebraic set is said to be irreducible if it cannot be written as the union of a finite number of proper algebraic subsets. Every algebraic set can be written as a finite union of irreducible algebraic subsets [H, Corollary I.1.6]. As usual, we can define the dimension of an irreducible set and define the dimension of an algebraic set to be the maximum of the dimensions of its irreducible components.

A polynomial $P(X_1, \ldots, X_n) \in \mathbb{Q}[X_1, \ldots, X_n]$ is said to have bidegree at most $(D_1, D_2)$ if $\deg X_1(P) \leq D_2$ and any monomial term $X_1^{k_1} \cdots X_n^{k_n}$ with non-zero coefficient has $k_1 + \ldots + k_{n-1} \leq D_1$.

Let $\mathbb{Q}[X_1, \ldots, X_n] \leq (D_1, D_2)$ denote the set of all elements of $\mathbb{Q}[X_1, \ldots, X_n]$ of bidegree at most $(D_1, D_2)$.

For any subset $E$ of $\mathbb{Q}^n$, let $\mathcal{F}(E, \mathbb{Q})$ denote the set of all functions from $E$ into $\mathbb{Q}$. Consider the $\mathbb{Q}$-linear map $\text{res}_E : \mathbb{Q}[X_1, \ldots, X_n] \rightarrow \mathcal{F}(E, \mathbb{Q})$ which maps each $P \in \mathbb{Q}[X_1, \ldots, X_n]$ to the restriction to $E$ of the polynomial map from $\mathbb{Q}^n$ to $\mathbb{Q}$ induced by $P$.

We let $H(E; D_1, D_2) = \text{dim}(\mathbb{Q}[X_1, \ldots, X_n] \leq (D_1, D_2))$.

Let $\overline{E}$ be the smallest algebraic set containing $E$. Since $\text{res}_\mathbb{Q}$ and $\text{res}_E$ have the same kernels, we get $H(\overline{E}; D_1, D_2) = H(E; D_1, D_2)$. Moreover, if $D_1, D_2$ are not too small, then $H(E; D_1, D_2)$ coincides with the value at $(D_1, D_2)$ of a polynomial whose total degree is $n^* = \text{dim}(\overline{E})$:

$$H(E; D_1, D_2) = \sum_{i+j \leq n^*} a_{i,j} D_1^i D_2^j.$$ 

This polynomial is called the Hilbert-Samuel bihomogeneous polynomial of $E$. We denote by $\mathcal{H}(E; D_1, D_2)$ the product of $n^*$! and the homogeneous part of the Hilbert-Samuel polynomial of $E$ of total degree $n^*$ evaluated at $(D_1, D_2)$. So

$$\mathcal{H}(E; D_1, D_2) = n^*! \sum_{i+j = n^*} a_{i,j} D_1^i D_2^j \quad (n^* = \text{dim}(\overline{E})).$$

We require the following facts:

**Lemma 3.1** With the above notation:
(i) \( \mathcal{H}(G; D_1, D_2) = nD_1^{n-1}D_2. \)

(ii) Let \( \mathcal{U} \) be a vector subspace of \( \mathbb{V}^{n-1} \) of dimension \( d_1 \) and \( m \) be a non-negative integer. If the subgroup \( T_m \) of \( \mathbb{V}^* \) has rank \( 1 - d_2 \), then

\[
\frac{(d_1 + d_2)!}{d_1!d_2!} D_1^{d_1}D_2^{d_2} \leq \mathcal{H}(\mathcal{U} \times T_m; D_1, D_2).
\]

(iii) If \( \mathcal{V} \) is a non-empty algebraic subset of \( G \) and \( g \in G \), then \( \mathcal{V} + g \) is an algebraic set of the same dimension as \( \mathcal{V} \) and

\[
\mathcal{H}(\mathcal{V} + g; D_1, D_2) = \mathcal{H}(\mathcal{V}; D_1, D_2).
\]

(iv) If \( H \) is an algebraic subgroup of \( G \) and \( E \) is a finite non-empty union of translates of \( H \) in \( G \), then \( E \) is an algebraic subset of \( G \) and

\[
\mathcal{H}(E; D_1, D_2) = |E/H|\mathcal{H}(H; D_1, D_2).
\]

(v) If \( \mathcal{V} \) and \( \mathcal{X} \) are algebraic subsets of \( G \), let

\[
E = \{ g \in G : g + \mathcal{V} \subseteq \mathcal{X} \}.
\]

Then \( E \) is an algebraic set which is defined by polynomials of no greater bidegree than those defining \( \mathcal{X} \).

(vi) If \( E \) is a non-empty algebraic subset of \( G \) defined by polynomials of bidegree at most \( (D_1, D_2) \), then \( \mathcal{H}(E; D_1, D_2) \leq \mathcal{H}(G; D_1, D_2) \).

A proof can be found, for example, in [W, Chapter 8].

4 Proof of the Zero Estimate

Let \( \mathcal{L}_1 = \{(s_1 + s_3\beta_1, s_2 + s_3\beta_2) : 0 \leq s_i \leq S_i, (i = 1, 2, 3)\} \) and \( \mathcal{L}_2 = \{(t_1 + t_3\beta_1, t_2 + t_3\beta_2) : 0 \leq t_i \leq T_i, (i = 1, 2, 3)\} \); let \( \mathcal{L}_1^* = \{(s_1 + s_3\beta_1, s_2 + s_3\beta_2, \alpha_1^{s_1}\alpha_2^{s_2}\alpha_3^{s_3}) : 0 \leq s_i \leq S_i, (i = 1, 2, 3)\} \) and \( \mathcal{L}_2^* = \{(t_1 + t_3\beta_1, t_2 + t_3\beta_2, \alpha_1^{t_1}\alpha_2^{t_2}\alpha_3^{t_3}) : 0 \leq t_i \leq T_i, (i = 1, 2, 3)\} \).

Write the polynomial \( P(X, Y, Z) \) as a product of its irreducible factors \( P_1, P_2, ..., P_k \) and assume that none of these are a scalar multiple of \( Z \).

Then \( Z_0 \), the set of zeros of \( P \), is an algebraic set that is the union of the \( k \) varieties \( \mathcal{V}(P_i) (i = 1, ..., k) \); so \( Z_0 = \bigcup_{i=1}^{k} \mathcal{V}(P_i) \).

Let \( Z_1 = \bigcap_{\delta \in \mathcal{L}_1^*} (Z_0 - \delta) \bigcap_{\delta \in \mathcal{L}_2^*} \bigcup_{i=1}^{k} (\mathcal{V}(P_i) - \delta) \). Thus

\[
Z_1 = \bigcup_{\Lambda_1 \cup ... \cup \Lambda_k = \mathcal{L}_1^*} \bigcap_{i=1}^{k} \bigcap_{\delta \in \Lambda_i} (\mathcal{V}(P_i) - \delta),
\]
Assume that $(\Lambda_1, \ldots, \Lambda_k)$ ranges over pairwise disjoint subsets of $\mathcal{L}_1^*$ whose union is $\mathcal{L}_1^*$.

Note that $\dim(\mathcal{Z}_1) \leq \dim(\mathcal{Z}_0) \leq 2$; and $\mathcal{L}_2^* \subseteq \mathcal{Z}_1$ by the hypothesis of the theorem.

Assume that $(b_1, b_2, b_3)$ is not $(R_1, R_2, R_3)$-linearly dependent, whence the projection of $\mathcal{L}_j^*$ onto $\mathcal{L}_j$ is injective ($j = 1, 2$).

### 4.1 A Preliminary Result

**Lemma 4.1** Assume that $\{b_1, b_2, b_3\}$ is not $(S_1, S_2, S_3)$-linearly dependent. Under the hypotheses of Theorem A, the number of elements of $\mathcal{L}_1$ lying on a common line is bounded by $M = 2\sqrt{(S_1 + 1)(S_2 + 1)(S_3 + 1)}$.

**Proof:** This is a tedious counting argument. Suppose that there is a line $\ell$ of slope $m$ for which the lemma is false. By the Dirichlet Box Principle, there are $\sigma_i \in \mathcal{L}_1 \cap \ell$ with $\sigma_i = (x_i, y_i) + z_i(\beta_1, \beta_2)$ ($i = 1, \ldots, 6$) such that

- $\sigma_1 \neq \sigma_2$,
- $\sigma_3 \neq \sigma_4$,
- $\sigma_5 \neq \sigma_6$,
- $x_1 = x_2$,
- $y_3 = y_4$,
- $z_5 = z_6$.

Simple slope calculations give

$$m = \frac{(z_2 - z_1)\beta_2 + (y_2 - y_1)}{(z_2 - z_1)\beta_1} = \frac{(z_4 - z_3)\beta_2}{(z_4 - z_3)\beta_1 + (x_4 - x_3)} = \frac{y_6 - y_5}{x_6 - x_5}.$$

Now $(z_4 - z_3)b_1 + (x_4 - x_3)b_3 \neq 0$ since $\{b_1, b_2, b_3\}$ is not $(S_1, S_2, S_3)$-linearly dependent. Thus $m$ must be finite (so $z_2 \neq z_1$) and we obtain

$$(z_2 - z_1)(y_6 - y_5)b_1 = (z_2 - z_1)(x_6 - x_5)b_2 + (y_2 - y_1)(x_6 - x_5)b_3. \quad (*)$$

We may assume that $\sigma_1, \sigma_2$ are chosen so that $|z_2 - z_1|$ is minimal with respect to $x_1 = x_2$; similarly that $|x_6 - x_5|$ is minimal with respect to $z_5 = z_6$. By the minimality of $|z_2 - z_1|$, for each $x \in \{0, \ldots, S_1\}$, there are at most $2(S_3 + 1)/|z_2 - z_1|$ different values of $z$ for which there is $y \in \{0, \ldots, S_2\}$ such that $(x, y) + z(\beta_1, \beta_2) \in \ell$; for such values of $z$, there is exactly one value of $y$ since $m$ is finite. Hence there are at most

$$2(S_1 + 1)(S_3 + 1)/|z_2 - z_1|$$

points in $\mathcal{L}_1 \cap \ell$. Thus $2(S_1 + 1)(S_3 + 1)/|z_2 - z_1| > 2\sqrt{(S_1 + 1)(S_2 + 1)(S_3 + 1)}$, whence

$$|z_2 - z_1| < \sqrt{(S_1 + 1)(S_3 + 1)/(S_2 + 1)}.$$
Similarly,
\[ |y_2 - y_1| < \sqrt{(S_1 + 1)(S_2 + 1)/(S_3 + 1)}. \]

Interchanging the roles of \( x \) and \( z \) in the above argument gives
\[ |x_6 - x_5| < \sqrt{(S_1 + 1)(S_3 + 1)/(S_2 + 1)} \quad \& \quad |y_6 - y_5| < \sqrt{(S_2 + 1)(S_3 + 1)/(S_1 + 1)}. \]

Consequently, \(|(y_2 - y_1)(x_6 - x_5)| < S_1 + 1, (y_6 - y_5)(z_2 - z_1)| < S_3 + 1 \) and \(|(x_6 - x_5)(z_2 - z_1)| < S_3 + 1 \) (using \( S_1 \leq S_2 \)). From (*) we deduce that \( \{b_1, b_2, b_3\} \) is \((S_1, S_2, S_3)\)-linearly dependent, the desired contradiction. //

### 4.2 Permutations

Let \( \Lambda_i = \{t_1, \ldots, t_{n_i}\} \), and for each \( j = 1, \ldots, n_i \), let \( \mathcal{H}_j \) be the hypersurface \( \mathcal{V}(P_i \circ t_j) \). We next show that \( \mathcal{H}_{j_1} \neq \mathcal{H}_{j_2} \) if \( j_1 \neq j_2 \) by considering setwise stabilisers.

**Lemma 4.2** Let \( P_i(X, Y, Z) \) be an irreducible polynomial (not a scalar multiple of \( Z \)) and \( \delta, \sigma \in \Lambda_i \) be distinct. If \( \mathcal{V}(P_i \circ t_\delta) = \mathcal{V}(P_i \circ t_\sigma) \), then the bidegree of \( P_i \) is at most \((1, 0)\). Hence \( \dim(\mathcal{H}_{j_1}) \cap \dim(\mathcal{H}_{j_2}) \leq 1 \).

**Proof:** Since \( \mathcal{V}(P_i \circ t_\delta) = \mathcal{V}(P_i \circ t_\sigma) \), we have \( P_i \circ t_\delta = c(P_i \circ t_\sigma) \) for some \( c \in \mathbb{Q}^* \). Write \( P_i(X, Y, Z) = \sum_{j,k,\ell} c_{j,k,\ell} X^j Y^k Z^\ell \), and \( \delta \& \sigma \) as \((s_1 + s_3 \beta_1, s_2 + s_3 \beta_2, \alpha_1^{s_1} \alpha_2^{s_2} \alpha_3^{s_3}) \) & \((s_1^{\delta} + s_3^{\delta} \beta_1, s_2^{\delta} + s_3^{\delta} \beta_2, \alpha_1^{s_1} \alpha_2^{s_2} \alpha_3^{s_3})\) respectively. By comparing any term with \( \ell \) maximal (and then \( j + k \) maximal) gives \( c = (\alpha_1^{s_1 - s_1} \alpha_2^{s_2 - s_2} \alpha_3^{s_3 - s_3})^\ell \). Among the terms in \( P_i \) with \( c_{j,k,\ell} \neq 0 \) choose any of highest power (existence since \( Z \) does not divide \( P_i \)). Comparing both sides we get \( c = 1 \). Since \( \{\alpha_1, \alpha_2, \alpha_3\} \) is multiplicatively independent, we get \( \ell = 0 \); i.e., \( P_i \) has bidegree \((D, 0)\) for some \( D \).

Since \( P_i \) is not constant, there exists \((x_0, y_0, z_0) \in \mathcal{V}(P_i)\). Since \( P_i \circ t_\delta = P_i \circ t_\sigma \), it follows that \( \mathcal{V}(P_i) \) contains the infinite subset \((x_0, y_0, z_0) + Z(\delta - \sigma) \). Let \( \mathcal{W} \) be the projection of \( \mathcal{V}(P_i) \) to the first two coordinates. Since \( P_i \) has bidegree \((D, 0)\), infinitely many points on the line \((x_0, y_0) + \)
$(\delta - \sigma)$ are contained in the variety $W_i$. By Bézout’s Theorem, $W_i$ is this line, whence the bidegree of $P_i$ is $(1, 0)$. //

Let $C_i = \bigcap_{\delta \in \Lambda_i} (\mathcal{V}(P_i) - \delta)$, $A = \{ i \in \{1, ..., k \} : P_i \text{ has bidegree} (1, 0) \}$, and $\kappa = |A|$. Then

$$|L_1^*| = \sum_{i=1}^{k} |\Lambda_i| \leq \kappa M + \sum_{i=1}^{k} |\Lambda_i|.$$  

Since $P$ has bidegree at most $(D_1, D_2)$, we have $\kappa \leq D_1 + D_2$; and, by hypothesis (3), $\kappa M < |L_1^*|$; so the complement of $A$ is non-empty. Our goal in this section is to establish

**Proposition 4.3** \(\dim(C_i) = 0\) if either

(i) \(i \in A\) and \(|\Lambda_i| > M\), or

(ii) \(i \notin A\) and \(|\Lambda_i| \geq 2\).

**Proof:** Assume that \(\dim(C_i) \neq 0\).

(i) If $P_i(X, Y, Z)$ has bidegree $(1, 0)$, then the projection $W_i$ of $\mathcal{V}(P_i) - \delta$ to the first two coordinates is a line for each $\delta \in \Lambda_i$. Since $\dim(C_i) \geq 1$ and the projections of all $\delta \in \Lambda_i$ lie on the same translate of the line $W_i$, by Lemma 4.1 we get $|\Lambda_i| \leq M$.

(ii) By Lemma 4.2, if $|\Lambda_i| \geq 2$, then $\dim(C_i) = 1$. By Bézout’s Theorem (\cite[Theorem I.7.7]{H}), $\mathcal{H}_{j_1} \cap \mathcal{H}_{j_2}$ has at most $N_i^2$ irreducible components, where $N_i = \deg(P_i)$. To complete the proof of the proposition we will need three easy lemmata to bound the size of $\Lambda_i$ where $i \notin A$.

**Lemma 4.4** Assume the above notation and hypotheses.

Let $\tau_{j_1}, \tau_{j_2}, \tau_{j_3}, \tau_{j_4} \in \Lambda_i$. If $C_i$ is a component of $\mathcal{H}_{j_1} \cap \mathcal{H}_{j_2} \cap \mathcal{H}_{j_3} \cap \mathcal{H}_{j_4}$ and $\tau_{j_2} - \tau_{j_1} = \tau_{j_4} - \tau_{j_3}$, then $t_{\tau_{j_3} - \tau_{j_1}}(C_i)$ is a component of $\mathcal{H}_{j_1} \cap \mathcal{H}_{j_2}$.

**Proof:** Let $v \in C_i$. Then $P_i \circ t_{\tau_{j_p}}(v) = 0$ for $p = 1, 2, 3, 4$.

Hence $P_i \circ t_{\tau_{j_1}}(t_{\tau_{j_3} - \tau_{j_1}}(v)) = 0$, whence $t_{\tau_{j_3} - \tau_{j_1}}(v) \in \mathcal{H}_{j_1}$.

Similarly $P_i \circ t_{\tau_{j_2}}(t_{\tau_{j_3} - \tau_{j_1}}(v)) = P_i \circ t_{\tau_{j_4}}(v) = 0$, whence $t_{\tau_{j_3} - \tau_{j_1}}(v) \in \mathcal{H}_{j_2}$. //

We are now ready to consider orbit sizes.
Lemma 4.5  With the above notation and hypotheses, if $\delta, \sigma \in \Lambda_i$ and $t_\delta(C_i) = t_\sigma(C_i)$, then $\delta = \sigma$.

Proof: Let $F = \{g \in G : C_i + g = C_i\}$, an algebraic subgroup of $G$. Hence $F = \mathcal{U} \times \mathcal{T}_m$ for some vector subspace $\mathcal{U}$ of $\mathbb{Q}^2$ and non-negative integer $m$. Note that $\delta - \sigma \in F$ by hypothesis. If $\delta \neq \sigma$, then $m = 0$ since $\{\alpha_1, \alpha_2, \alpha_3\}$ is multiplicatively independent. Since the projection of $\Lambda_i$ onto the first two coordinates is injective, $\dim(\mathcal{U}) \geq 1$. Thus $\dim(C_i) \geq 2$, the desired contradiction. \hfill \Box

Lemma 4.6  With the above notation and hypotheses, the set $\Lambda_i$ cannot contain $N_i^2 + 1$ distinct pairs $(\tau_{j_1}, \tau_{j_2})$ such that $\tau_{j_1} - \tau_{j_2}$ is a non-zero constant independent of $j$.

Proof: We argue by reductio ad absurdum. Since $\mathcal{H}_{j_1} \cap \mathcal{H}_{j_2}$ has at most $N_i^2$ components, either $t_{\tau_{j_1} - \tau_{j_2}}(C_i) = C_i$ or $t_{\tau_{j_1} - \tau_{j_2}}(C_i) = t_{\tau_{j_4} - \tau_{j_3}}(C_i)$ by the Dirichlet Box Principle. The latter case contradicts Lemma 4.4 and the former contradicts Lemma 4.5. \hfill \Box

We can now complete the proof of the proposition.

Proof of Proposition completed: Let $n_i = |\Lambda_i|$. The number of distinct ordered pairs of distinct elements of $\Lambda_i$ is $n_i(n_i - 1)$, whereas the number of possible non-zero values for $\tau_{j_1} - \tau_{j_2}$ is at most $(2S_1 + 1)(2S_2 + 1)(2S_3 + 1) - 1$ ($\tau_{j_1}, \tau_{j_2} \in \Lambda_i$). By Lemma 4.6 and the Dirichlet Box Principle,

$$n_i(n_i - 1) \leq N_i^2((2S_1 + 1)(2S_2 + 1)(2S_3 + 1) - 1).$$

Since $4N_i^2 > 1$, the quadratic formula gives

$$n_i \leq \frac{1}{2} + 2N_i \sqrt{2\left((S_1 + \frac{1}{2})(S_2 + \frac{1}{2})(S_3 + \frac{1}{2})\right)}.$$  

Since there are at most $D_1/2$ factors with bidegree $(d, 0)$ for some positive $d$ and $\sum_{i \notin A} N_i \leq D_1 + D_2 - \kappa$, we have

$$\sum_{i \notin A} |\Lambda_i| = \sum_{i \notin A} n_i \leq$$
\[
\leq \frac{1}{2} \left( \frac{1}{2} D_1 + D_2 \right) + 2\sqrt{2}(D_1 + D_2 - \kappa) \sqrt{(S_1 + \frac{1}{2})(S_2 + \frac{1}{2})(S_3 + \frac{1}{2})}.
\]

Hence, by (†), we get
\[
|L^*_1| \leq M\kappa + \frac{1}{2}(\frac{1}{2} D_1 + D_2) + 2\sqrt{2}(D_1 + D_2 - \kappa) \sqrt{(S_1 + \frac{1}{2})(S_2 + \frac{1}{2})(S_3 + \frac{1}{2})}.
\]

The right-hand side is clearly maximal when $\kappa = 0$. Thus $|L^*_1| \leq \sqrt{2}(D_1 + D_2)M$. This contradicts (3) since $|L^*_1| = (S_1 + 1)(S_2 + 1)(S_3 + 1)$. Consequently, the proposition is established. //

4.3 Pointwise Stabilisers and Algebraic sets

We now use the results on algebraic sets to complete the proof of the theorem. We first shew:

Lemma 4.7 Under the hypotheses of the theorem, there exist a vector subspace $U$ of $\mathbb{Q}^2$ of dimension $d_1$ and a subgroup $T_m$ of $\mathbb{Q}^*$ of rank $1 - d_2$ with $d_1 + d_2 \leq 2$ such that
\[
\frac{(d_1 + d_2)!}{d_1!d_2!} \left| \frac{L^*_2 + (U \times T_m)}{U \times T_m} \right| \leq 3(2D_1)^{2-d_1}D_2^{1-d_2}.
\]

Proof: Since $L^*_1 + L^*_2 \subseteq Z_0$, we know $L^*_2 \subseteq Z_1$.

Let $Z_2 = \bigcap_{\delta \in L^*_2} (Z_1 - \delta)$. Then $Z_2$ is an algebraic subset of $Z_1$ and contains $(0, 0, 1)$. Since $\dim(Z_1) = 0$ (by the proposition), \{(0, 0, 1)\} is an irreducible component of both $Z_1$ and $Z_2$. Moreover, $L^*_2 \subseteq E$ where $E = \{g \in G : g + (0, 0, 1) \in Z_1\}$. Let $H$ be the stabiliser of $(0, 0, 1)$ in $G$ and $O$ be the orbit of $(0, 0, 1)$ under $E$. Since $O \subseteq Z_1$ and $Z_1$ is an algebraic set of dimension 0, it follows that $O$ is finite. The natural map between $E/H$ and $O$ is clearly a bijection, whence $E$ is a finite union of translates of $H$. But $(L^*_2 + H)/H \subseteq E/H$. The result now follows from Lemma 3.1. //

10
We can now complete the proof of the theorem.

Proof: Let $H$ be the stabiliser of $(0, 0, 1)$ in $G$. Then $H = U \times T_m$ for some integer $m \geq 0$. Since $\dim(\mathcal{Z}_1) = 0$ and $(0, 0, 1) \in \mathcal{Z}_1$, we must have $U = \{0\}$ and $m = 1$. Thus $H$ is the trivial group. By Lemma 4.7, $|L^*_2| \leq 12D_1^2D_2$. This contradicts hypothesis (4) and so completes the proof of the theorem. //

5 The Main Theorem ($n = 4$)

In this context, we say that $(b_1, b_2, b_3, b_4) \subset \mathbb{Z}^4$ is $(R_1, R_2, R_3, R_4)$-linearly dependent over $\mathbb{Z}$ if there are at least two of which are not zero such that $\sum_{j=1}^4 d_j b_j = 0$ with $|d_1|, |d_2| \leq \max\{R_3, R_4\}$, $|d_3| \leq \max\{R_2, R_4\}$ and $|d_4| \leq \max\{R_1, R_3\}$.

Theorem B (Improved Zero Estimate) Suppose that $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ is multiplicatively independent and $b_1, b_2, b_3, b_4$ are non-zero integers. Let $D_1, D_2, R_1, ..., R_4, S_1, ..., S_4, T_1, ..., T_4, U_1, ..., U_4 \in \mathbb{Z}_+$ be at least 4, and $\beta_j = b_j/b_4$ ($j = 1, 2, 3$). Let

$L^* = \{(r_1 + r_4\beta_1, r_2 + r_4\beta_2, r_3 + r_4\beta_3, \alpha_1 r_1\alpha_2 r_2\alpha_3 r_3) : 0 \leq r_j \leq R_j (j = 1, 2, 3, 4)\}$.

Assume that $D_1 \geq 2D_2$, $S_3 \geq S_2 \geq S_1$ and $S_j + T_j + U_j < R_j$ for $j = 1, 2, 3, 4$. Let

$M_L = \max\{2S_3 + 1, 2S_4 + 1, 2[(2S_2 + 1)(2S_3 + 1)(2S_4 + 1)]^{1/2}\}$ and

$M_{\Pi} = \max\{(2S_2 + 1)(2S_3 + 1), (2S_3 + 1)(2S_4 + 1),
2[(2S_1 + 1)(2S_2 + 1)(2S_3 + 1)^2(2S_4 + 1)]^{1/2},
2[(2S_1 + 1)^2(2S_2 + 1)^3(2S_3 + 1)(2S_4 + 1)^2]^{1/3}\}$.

IF

(1) $\prod_{i=1}^4 (S_i + 1) > (D_1 + D_2)M_{\Pi}$,

(2) $\prod_{i=1}^4 (S_i + 1) > 16(D_1 + D_2)^2(M_L + 1)$,
Thus we obtain that $P$ some of the irreducible factors of
analogue of Lemma 4.2 together with Hypothesis (1) now ensure that
the number of elements of $D$ (analagously to Lemma 4.1 but with considerably more “finessing”) that
Let $X$ now mean that each non-zero monomial term has the sum of its degrees
is either increasing or decreasing. Thus

$$
\sum_{i=1}^{3} \deg_{X_i}(P) \leq D_1 \text{ and } \deg_{X_4}(P) \leq D_2 \text{ can have } \mathcal{L}^* \text{ as its set of zeros unless } (b_1, b_2, b_3, b_4) \text{ is } (R_1, R_2, R_3, R_4)\text{-linearly dependent.}
$$

As in the introduction, we can define $\mathcal{L}_1 = \{(s_1 + s_4 \beta_1, s_2 + s_4 \beta_2, s_3 + s_4 \beta_3) : 0 \leq s_i \leq S_i \ (i = 1, 2, 3, 4)\}$, $\mathcal{L}_2 = \{(t_1 + t_4 \beta_1, t_2 + t_4 \beta_2, t_3 + t_4 \beta_3) : 0 \leq t_i \leq T_i \ (i = 1, 2, 3, 4)\}$ and $\mathcal{L}_3 = \{(u_1 + u_4 \beta_1, u_2 + u_4 \beta_2, u_3 + u_4 \beta_3) : 0 \leq u_i \leq U_i \ (i = 1, 2, 3, 4)\}$. Let $\mathcal{L}^*_1 = \{(s_1 + s_4 \beta_1, s_2 + s_4 \beta_2, s_3 + s_4 \beta_3, \alpha_1^{s_1} \alpha_2^{s_2} \alpha_3^{s_3} \alpha_4^{s_4}) : 0 \leq s_i \leq S_i \ (i = 1, 2, 3, 4)\}$, $\mathcal{L}^*_2 = \{(t_1 + t_4 \beta_1, t_2 + t_4 \beta_2, t_3 + t_4 \beta_3, \alpha_1^{t_1} \alpha_2^{t_2} \alpha_3^{t_3} \alpha_4^{t_4}) : 0 \leq t_i \leq T_i \ (i = 1, 2, 3, 4)\}$ and $\mathcal{L}^*_3 = \{(u_1 + u_4 \beta_1, u_2 + u_4 \beta_2, u_3 + u_4 \beta_3, \alpha_1^{u_1} \alpha_2^{u_2} \alpha_3^{u_3} \alpha_4^{u_4}) : 0 \leq u_i \leq U_i \ (i = 1, 2, 3, 4)\}$.

In the proof for $n = 3$ we used permutation groups to obtain conditions that ensured that the algebraic set $\mathcal{Z}_1$ had zero dimension and so shared a maximal irreducible component with $\mathcal{Z}_2$. We need to generalise this approach for $n = 4$. We work in the group $\mathbb{Q}^3 \times \mathbb{Q}^*$ (additive on the first three coordinates, multiplicative on the last). Bidegree $(D_1, D_2)$ will now mean that each non-zero monomial term has the sum of its degrees in $X_1, X_2 \& X_3$ at most $D_1$ and $X_4$-degree at most $D_2$.

We assume that $(b_1, ..., b_4)$ is not $(R_1, R_2, R_3, R_4)$-linearly dependent. Let $\mathcal{D}$ be the set of differences of pairs of points of $\mathcal{L}_1$. We can show (analagously to Lemma 4.1 but with considerably more “finessing”) that the number of elements of $\mathcal{D}$ that lie on a single straight line is at most $M_L$ and on a single plane is at most $M_P$. As for $n = 3$, the natural analogue of Lemma 4.2 together with Hypothesis (1) now ensure that some of the irreducible factors of $P$ have bidegree not equal to $(1, 0)$. Thus we obtain that $\dim(\mathcal{Z}_1) \leq 2$ under Hypothesis (1).

Assume that $\dim(\mathcal{Z}_1) = 2$. Lemmata 4.4 - 4.6 hold equally in this context and allow us to obtain (as in Section 4.2 with the same meaning for $\kappa$) that

$$
|\mathcal{L}_1| \leq \kappa M_P + (D_1 + D_2 - \kappa) \left(\frac{1}{2} + 4[(M_L + 1) \prod_{i=1}^{4} (S_i + \frac{1}{2})]^{1/2}\right).
$$

The right hand side of this inequality is a linear function in $\kappa$ and so is either increasing or decreasing. Thus

$$
|\mathcal{L}_1| \leq (D_1 + D_2)M_P \text{ or }
$$
\[|\mathcal{L}| \leq (D_1 + D_2)4[(M_L + 1) \prod_{i=1}^{4} (S_i + 1)]^{1/2}.\]

The first possibility is excluded by Hypothesis (1) and the second by Hypothesis (2). Hence \(\dim(\mathcal{Z}_1) \leq 1.\)

If \(\dim(\mathcal{Z}_1) = \dim(\mathcal{Z}_2),\) then we get the Improved Zero Estimate \((n = 4)\) as before using the natural analogue of Lemma 4.7 obtained from Lemma 3.1. If \(\dim(\mathcal{Z}_1) \neq \dim(\mathcal{Z}_2),\) then \(\dim(\mathcal{Z}_1) = 1\) and \(\dim(\mathcal{Z}_2) = 0.\)

In this case we can define \(\mathcal{Z}_3\) analogously to the prior \(\mathcal{Z}_j\) (using \(\mathcal{L}_j^*\)) with \(\mathcal{Z}_3 \subseteq \mathcal{Z}_2 \subseteq \mathcal{Z}_1 \subseteq \mathcal{Z}_0,\) the crucial point being that \(\mathcal{L}_3^* \subseteq \mathcal{Z}_2 (\mathcal{L}_1^* + \mathcal{L}_2^* + \mathcal{L}_3^* \subseteq \mathcal{Z}_0).\) Necessarily, \(\mathcal{Z}_3\) has the same dimension as \(\mathcal{Z}_2,\) viz. 0, and we can again employ Lemma 3.1 and the technique of proof of Lemma 4.7 to obtain the desired Improved Zero Estimate.

More cases have to be considered in all of the computations, but again the ideas are essentially the same — stabilisers and orbits. Only the details are messier! For a full account (with details and improvements on the results in the above outline), please see [E] or the preprint of the same.

### 6 Extensions

It is possible to extend the ideas above in two ways.

The first is to permit non-zero \(\alpha_1, \ldots, \alpha_n\) to be algebraic numbers that are not necessarily rational. Let \(D = [\mathbb{Q}(\alpha_1, \ldots, \alpha_n); \mathbb{Q}].\) Then the constants \(C_1\) and \(C_2\) must be replaced by \(D^{n+2}\) times new constants that are independent of \(\{D, \alpha_j, b_j : j = 1, \ldots, n\}.\) The above proof goes through unchanged; only the deduction of the constant needs modification. Again please see [E] for the details.

The second possible extension is to linear forms in more than 4 logarithms of algebraic numbers. In essence, the Improved Zero Estimate becomes weaker as \(n\) increases as conditions (3) and (4) above have to be replaced by \(n - 2\) conditions. This dependence on \(n\) gives far weaker results than those obtained by Alan Baker’s far more powerful extrapolation technique. However, for small values of \(n\) (2, 3 & 4) it is very useful for solving Diophantine equations as we now illustrate.
A Comparison and Application

In 1844, E. Catalan conjectured that the only two consecutive natural numbers that are both proper powers are 8 and 9. So it is enough to consider the equation $x^p - y^q = 1$ where $p, q$ are positive prime whole numbers and $x, y$ are positive integers. We will call the case $(x, y, p, q) = (3, 2, 2, 3)$ the trivial solution, and seek only non-trivial solutions. In 1850, Lebesgue [L] showed that $q \neq 2$ and in 1965 Ko Chao [K] showed that $p \neq 2$. In 1921, Nagell [N] ruled out $p = 3$ and also $q = 3$, and in 1960 Cassells proved that $p|y$ and $q|x$. In 1976, R. Tijdeman [T] used an ingenious argument involving linear forms in logarithms of algebraic numbers to prove that the number of solutions is finite and bounded by an explicit constant given by A. Baker’s work. In his proof, Tijdeman had to consider the special case that $\Lambda = q\log q - p\log p + q\log(r/s)$ with $p, q$ distinct primes exceeding 3 and $r, s \in \mathbb{Z}_+$ with $p|r, q|s \& s \leq 2r$. As shewn in [BGO], the constant $C_1$ in the Baker-Wüstholz approach can be taken to be at most $9.55 \times 10^9$ whereas the permutation approach leads to a constant $2.61 \times 10^5$ — with an extra $B$ (please see [BBGMS] for a full table for 3 variables and [E] for the extension to 4 variables). The permutation approach drops the upper bound for $p$ and $q$ in Catalan’s equation dramatically; indeed, it is shewn in [BGO] that $\min\{p, q\} < 3.31 \times 10^{12}$ and $\max\{p, q\} < 4.13 \times 10^{17}$.

In recent work, [M] has further reduced these bounds to $7.15 \times 10^{11}$ and $7.78 \times 10^{16}$ by tweaking the deduction of the constant from the improved zero estimate in [BBGMS].

Cyclotomic considerations are also possible, the culmination of which is due to P. Mihailescu [Mi]: $p^{r-1} \equiv 1 \pmod{q^2}$ \& $q^{r-1} \equiv 1 \pmod{p^2}$.

Using this result and others, Mignotte & Roy [MR] have shown that $p, q > 10^7$. Since the linear forms in logarithms gives $M < 2.77m\log m[2.333 + \log(M/\log m)]^2$ where $M = \max\{p, q\}$ and $m = \min\{p, q\}$, there is every reason to hope that improved zero estimates for polynomials will finally answer Catalan’s Conjecture completely.

8 References


[N] T. Nagell, Des equations indeterminees $x^2 + x + 1 = y^n$ et $x^2 + x + 1 = 3y^n$, Norak Mat. Forenings Skrifter I 2 (1921), 1-14.


Authors’ addresses:

C. D. Bennett
Department of Mathematics & Statistics,
Bowling Green State University,
Bowling Green,
Ohio 43403,
USA

cbennet@bgsu.edu

L. K. Elderbrock
Department of Mathematics and Computer Science,
Northern Kentucky University,
Highland Heights,
Kentucky 41099,
USA.
elderbrockl@nku.edu

A. M. W. Glass
Department of Pure Mathematics & Mathematical Statistics,
Centre for Mathematical Sciences,
Wilberforce Rd.,
Cambridge CB3 0WB,
England.
amwg@dpmms.cam.ac.uk