Journal de Théorie des Nombres de Bordeaux

CURTIS D. BENNETT
JOSEF BLASS
A. M. W. GLASS
DAVID B. MERONK
RAY P. STEINER

Linear forms in the logarithms of three positive rational numbers

Journal de Théorie des Nombres de Bordeaux, tome 9, n° 1 (1997), p. 97-136

http://www.numdam.org/item?id=JTNB 1997 9 1 97 0>

© Université Bordeaux 1, 1997, tous droits réservés.

L'accès aux archives de la revue « Journal de Théorie des Nombres de Bordeaux » (http://jtnb.cedram.org/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.



Article numérisé dans le cadre du programme Numérisation de documents anciens mathématiques http://www.numdam.org/

Linear forms in the logarithms of three positive rational numbers

par Curtis D. BENNETT, Josef BLASS, A.M.W GLASS, DAVID B. MERONK et RAY P. STEINER*

To Hassoon S. Al-Amiri upon his retirement

RÉSUMÉ. Dans cet article, nous donnons une minoration de la dépendance linéaire de trois nombres rationnels positifs valable sous certaines conditions faibles d'indépendance linéaire des coefficients des formes linéaires. Soit $\Lambda = b_2 \log \alpha_2 - b_1 \log \alpha_1 - b_3 \log \alpha_3 \neq 0$ avec b_1, b_2, b_3 des entiers positifs et $\alpha_1, \alpha_2, \alpha_3$ des rationnels multiplicativement indépendants supérieurs à 1. Soit $\alpha_j = \alpha_{j1}/\alpha_{j2}$ où α_{j1}, α_{j2} sont des entiers positifs premiers entre eux (j=1,2,3). Soit $a_j \geq \max\{\alpha_{j1},e\}$ et supposons que $\gcd(b_1,b_2,b_3)=1$. Soit

$$b' = \left(\frac{b_2}{\log \alpha_1} + \frac{b_1}{\log \alpha_2}\right) \left(\frac{b_2}{\log \alpha_3} + \frac{b_3}{\log \alpha_2}\right)$$

et supposons que $B \ge \max\{10, \log b'\}$. Nous démontrons que, soit $\{b_1, b_2, b_3\}$ est (c_4, B) -linéairement dépendant sur \mathbb{Z} (relativement à (a_1, a_2, a_3)), ou bien

$$\Lambda > \exp\Big\{-CB^2\Big(\prod_{j=1}^3 \log a_j\Big)\Big\},$$

où c_4 et $C=c_1c_2\log\rho+\delta$ sont donnés dans les tables de la Section 6. Ici nous dirons que b_1,b_2,b_3 sont (c,B)-lineairement dépendants sur $\mathbb Z$ si $d_1b_1+d_2b_2+d_3b_3=0$ pour certains $d_1,d_2,d_3\in\mathbb Z$ non tous nuls tels que ou bien (i) $0<|d_2|\leq cB\log a_2\min\{\log a_1,\log a_3\},|d_1|,|d_3|\leq cB\log a_1\log a_3$, ou bien (ii) $d_2=0$ et $|d_1|\leq cB\log a_1\log a_2$ et $|d_3|\leq cB\log a_2\log a_3$.

Nous obtenons en particulier $c_4 < 9146$ and C < 422321 pour tout $B \ge 10$, et si $B \ge 100$ nous avons $c_4 \le 5572$ et $C \le 260690$. Des informations plus précises sont données dans les tables de la Section 6.

Nous démontrons ce résultat en modifiant les méthodes de P. Philippon, M. Waldschmidt, G. Wüstholz, et al. En particulier, par un argument combinatoire, nous prouvons que soit une certaine variété algébrique est de dimension nulle, ou bien $\{b_1, b_2, b_3\}$ sont linéairement dépendants sur \mathbb{Z} ,

Manuscrit reçu le 26 octobre 1995

^{*} The authors are grateful to NSF and MSRI for partial funding. We wish to thank Alan Baker FRS for the invitation to participate in the Transcendental Number Theory program at MSRI last year, and the staff there for their warm hospitality. This paper grew out of several discussions there.

avec de petits coefficients de dépendance. Cela nous permet d'améliorer le Lemme de zéros de Philippon, nous conduisant au fait que le déterminant d'interpolation reste non nul sous des conditions plus faibles.

ABSTRACT. In this paper we prove a lower bound for the linear dependence of three positive rational numbers under certain weak linear independence conditions on the coefficients of the linear forms. Let $\Lambda = b_2 \log \alpha_2 - b_1 \log \alpha_1 - b_3 \log \alpha_3 \neq 0$ with b_1, b_2, b_3 positive integers and $\alpha_1, \alpha_2, \alpha_3$ positive multiplicatively independent rational numbers greater than 1. Let $\alpha_j = \alpha_{j1}/\alpha_{j2}$ with α_{j1}, α_{j2} coprime positive integers (j = 1, 2, 3). Let $a_j \geq \max\{\alpha_{j1}, e\}$ and assume that $\gcd(b_1, b_2, b_3) = 1$. Let

$$b' = \Big(\frac{b_2}{\log \alpha_1} + \frac{b_1}{\log \alpha_2}\Big) \Big(\frac{b_2}{\log \alpha_3} + \frac{b_3}{\log \alpha_2}\Big)$$

and assume that $B \ge \max\{10, \log b'\}$. We prove that either $\{b_1, b_2, b_3\}$ is (c_4, B) -linearly dependent over \mathbb{Z} (with respect to (a_1, a_2, a_3)) or

$$\Lambda > \exp\Big\{-CB^2\Big(\prod_{j=1}^3 \log a_j\Big)\Big\},$$

where c_4 and $C=c_1c_2\log\rho+\delta$ are given in the tables of Section 6. Here b_1,b_2,b_3 are said to be (c,B)-linearly dependent over $\mathbb Z$ if $d_1b_1+d_2b_2+d_3b_3=0$ for some $d_1,d_2,d_3\in\mathbb Z$ not all 0 with either

(i) $0 < |d_2| \le cB \log a_2 \min\{\log a_1, \log a_3\}, |d_1|, |d_3| \le cB \log a_1 \log a_3$, or

(ii) $d_2 = 0$ and $|d_1| \le cB \log a_1 \log a_2$ and $|d_3| \le cB \log a_2 \log a_3$.

In particular, we obtain $c_4 < 9146$ and C < 422,321 for all values of $B \ge 10$, and for $B \ge 100$ we have $c_4 \le 5572$ and $C \le 260,690$. More complete information is given in the tables in Section 6.

We prove this theorem by modifying the methods of P. Philippon, M. Waldschmidt, G. Wüstholz, et al. In particular, using a combinatorial argument, we prove that either a certain algebraic variety has dimension 0 or $\{b_1, b_2, b_3\}$ are linearly dependent over $\mathbb Z$ where the dependence has small coefficients. This allows us to improve Philippon's zero estimate, leading to the interpolation determinant being non-zero under weaker conditions.

In the 1930's Gel'fond and Schneider independently studied linear forms in the logarithms of two algebraic numbers in order to answer Hilbert's 7^{th} problem, a special case of which is: Is $2^{\sqrt{2}}$ transcendental? The study of linear forms in the logarithms of more than two algebraic numbers is far more complicated. The great pioneer work of Alan Baker came in the 1960's. He proved that any finite set of logarithms of non-zero algebraic numbers is linearly dependent over $\bar{\mathbb{Q}}$ (the field of algebraic numbers) if and only if it is linearly dependent over \mathbb{Q} (the field of rational numbers).

Moreover, he showed that if

$$\Lambda = b_0 + \sum_{j=1}^n b_j \log \alpha_j$$

is not zero and

$$(b_0,\ldots,b_n,\alpha_1,\ldots,\alpha_n)\in \bar{\mathbb{Q}}^{n+1}\times (\bar{\mathbb{Q}}^*)^n,$$

then $|\Lambda|$ can be explicitly bounded away from zero. He improved this in [1] (in the case that $b_0 = 0$ and b_1, \ldots, b_n are rational integers) to:

$$|\Lambda| > \exp\{-C(\log b) \Big(\prod_{j=1}^n \log a_j\Big) (\log \log a)\}$$

for some explicitly computed large constant C. Here

$$egin{aligned} \log b & \geq \max\{4, h(b_j): j=0,\ldots,n\}, \ D & = [\mathbb{Q}(lpha_1,\ldots,lpha_n):\mathbb{Q}], \ a_j & \geq \max\{e, h(lpha_j), |\loglpha_j|/D\} \ (j=1,\ldots,n), \ \mathrm{and} \ \ a & \geq \max\{4, a_j: j=1,\ldots,n\}. \end{aligned}$$

Further, $h(\alpha)$ is the absolute logarithmic height of α , and for any field K, K^* denotes the multiplicative group of non-zero elements of K.

For the rest of the paper, we will assume that $b_0 = 0$ and b_1, \ldots, b_n are rational integers.

From these results, one can derive upper bounds on the size of the solutions of many Diophantine equations by a function \mathcal{C} dependent upon C and the particular equation (see e.g., [26], [28] and [8]); the smaller the value of C, the smaller the potential solution set (though $\mathcal{C}(C)$ is typically very large). For this (and other) reasons, many mathematicians have spent the better part of the last 25 years in an attempt to decrease the value of C and extend Baker's work to other contexts (e.g., the theory of linear forms in p-adic logarithms [24], [38], [39], [6], and elliptic logarithms [25], [23], [27]).

By 1990 successive work by Baker, Waldschmidt and others, [1], [29], [3] had reduced C to $n^{2n+1}(24e^2)^n2^{20}D^{n+2}$. The next major breakthrough, the use of algebraic groups and algebraic varieties, was developed in the 1980's. Impetus for this work came from Nesterenko [20], who used derivations on polynomial rings to study the zeros of certain E- functions. Later

Brownawell and Masser [4] developed this idea further and Masser [15] and Masser and Wüstholz [16], [17], [18] replaced the idea of derivations by the use of ring homomorphisms. Wüstholz [34] developed these ideas further in our setting and achieved significant results on zero and "multiplicity" estimates that were later refined by Philippon [21] and Denis [5]. The explicit application to the theory of linear forms in logarithms was given by Wüstholz [35], [36], [37] and Philippon and Waldschmidt [22]. Finally, Baker and Wüstholz [2] and Waldschmidt [32] combined the new ideas with the previous methods of Gel'fond & Baker and Schneider, respectively (for $b_0 = 0$ and all b_i 's are rational integers). Baker and Wüstholz obtained $C = 18(n+1)!n^{n+1}(32D)^{n+2}\log(2nD)$. This is currently the best result known and is an improvement on Waldschmidt's independent 1993 paper [32] by a factor of approximately n^{n+1} .

Recently, Michel Laurent [11], [12], [13] developed a new technique, Interpolation Determinants; this replaces (and is somewhat analogous to) the construction of an auxiliary function. In the case of two logarithms with $b_0 = 0$, Laurent, Mignotte and Nesterenko [14] obtain C < 50 if b' > 16 and C approaches 15.2 as b' approaches infinity, where $b' = \frac{b_1}{\log a_2} + \frac{b_2}{\log a_1}$ (in the case that α_1 and α_2 are rational numbers greater than 1, and all logarithms are principal). This was a significant improvement on the previous bound of 270 given by Mignotte and Waldschmidt [19]. Unfortunately, in both papers $\log b$ is replaced by $(\log b')^2$. In the case $b_0 = 0$ and n > 2 Waldschmidt [33] obtained upper bounds on C by this method. Again $\log b'$ is replaced by $(\log b')^2$, though this can be circumvented at the expense of a larger value of C [32].

As already noted, to obtain solutions of certain Diophantine equations, one needs smaller values of C. This motivates our study of linear forms in the logarithms of <u>three</u> algebraic numbers. (All our assumptions will be motivated by such considerations.) As Gel'fond [7, page 177] stated in 1952, non-trivial effective estimates for linear forms in <u>three</u> or more logarithms of algebraic numbers would lead to great advances in the theory of numbers, in particular the computation of explicit bounds for the solution set of certain exponential Diophantine equations. Indeed, he showed how to apply these ideas to the solution of Thue equations. At that time, the necessary estimates were known for the case of two logarithms but the transition to three logarithms presented considerable difficulty and had not been carried out. Baker's insight provided the original method and solution for the case of three logarithms (and the more general case involving n logarithms). The purpose of this paper is to concentrate on the particular case of linear forms in the logarithms of 3 positive rational numbers with integer coefficients

and $b_0=0$. The treatment of the general case $(n\geq 3, \log n)$ logarithms of algebraic numbers, and algebraic coefficients) by interpolation determinants is considered by Lisa Elderbrock in her Ph.D. dissertation. For n=3, an extra D^5 is needed, but the constant is reduced by approximately D^3 .

Often, bounding solutions of Diophantine equations involves bounding the coefficients of the logarithms in the resulting linear forms; see [26] for several examples. If these coefficients satisfy a linear dependence relation over $\mathbb Z$ with "small" coefficients, then we usually obtain much sharper bounds on the size of solutions (to the Diophantine equation) than those provided by bounding the linear form in logarithms away from 0. Consequently, we will always assume that the coefficients of the linear form are not "strongly linearly dependent" over $\mathbb Z$.

To simplify matters, we assume that $\{\alpha_1, \alpha_2, \alpha_3\}$ is a multiplicatively independent set of positive rational numbers and that $\{b_1, b_2, b_3\}$ is a set of coprime integers. Let $\Lambda = b_1 \log \alpha_1 + b_2 \log \alpha_2 + b_3 \log \alpha_3 \neq 0$. If all $b_j \log \alpha_j (j=1,2,3)$ are positive, then $\Lambda > b_1 \log \alpha_1 + b_2 \log \alpha_2$. Using [14], we can bound Λ "far" away from 0 in this (two logarithm) case. Similarly if all $b_j \log \alpha_j$ are negative, $|\Lambda|$ can be bounded "far" away from 0. Furthermore, since $b_j \log \alpha_j = -b_j \log (1/\alpha_j)$, we can assume that each of $\alpha_1, \alpha_2, \alpha_3$ strictly exceeds 1, that b_1, b_2, b_3 are all positive integers with highest common factor 1, and

$$\Lambda = b_2 \log \alpha_2 - b_1 \log \alpha_1 - b_3 \log \alpha_3 \neq 0;$$

moreover, we may assume that $b_2 \log \alpha_2 \ge \max\{b_1 \log \alpha_1, b_3 \log \alpha_3\}$.

Let a_1, a_2, a_3 be real numbers greater than or equal to e; without loss of generality, let $a_1 \ge a_3$. Let

$$b' = \left(\frac{b_2}{\log a_1} + \frac{b_1}{\log a_2}\right) \left(\frac{b_2}{\log a_3} + \frac{b_3}{\log a_2}\right)$$

and $B \ge \log b'$. We say that $\{b_1, b_2, b_3\}$ is (c, B)-linearly dependent over \mathbb{Z} (with respect to (a_1, a_2, a_3)) if

$$d_1b_1 + d_2b_2 + d_3b_3 = 0$$

for some rational integers d_1, d_2, d_3 not all 0 with either

(i) $0 < |d_2| \le cB \log a_2 \min\{\log a_1, \log a_3\}$ and $|d_1|, |d_3| \le cB \log a_1 \log a_3$, or

(ii)
$$d_2 = 0$$
 and $\begin{cases} |d_1| \le cB \log a_1 \log a_2 \\ |d_3| \le cB \log a_2 \log a_3. \end{cases}$

We will prove:

THEOREM A. Let $\Lambda = b_2 \log \alpha_2 - b_1 \log \alpha_1 - b_3 \log \alpha_3 \neq 0$ with b_1, b_2, b_3 positive rational integers and $\alpha_1, \alpha_2, \alpha_3$ positive multiplicatively independent rational numbers greater than 1. Let $\alpha_j = \alpha_{j1}/\alpha_{j2}$ with α_{j1}, α_{j2} coprime positive integers (j = 1, 2, 3). Let $a_j \geq \max\{\alpha_{j1}, e\}(j = 1, 2, 3)$ and assume that $\gcd(b_1, b_2, b_3) = 1$. Let

$$b' = \left(\frac{b_2}{\log a_1} + \frac{b_1}{\log a_2}\right) \left(\frac{b_2}{\log a_3} + \frac{b_3}{\log a_2}\right)$$

and $B \ge \max\{10, \log b'\}$. THEN either $\{b_1, b_2, b_3\}$ is $(10^4, B)$ -linearly dependent over \mathbb{Z} (with respect to (a_1, a_2, a_3)) or

$$|\Lambda| > \exp\Big\{ - CB^2 \Big(\prod_{j=1}^3 \log a_j \Big) \Big\}$$

where $C = 4.5 \times 10^{5}$.

Theorem A follows at once from the more technical theorem:

THEOREM B. Let $\Lambda = b_2 \log \alpha_2 - b_1 \log \alpha_1 - b_3 \log \alpha_3 \neq 0$ with b_1, b_2, b_3 positive integers and $\alpha_1, \alpha_2, \alpha_3$ positive multiplicatively independent rational numbers greater than 1. Let $\alpha_j = \alpha_{j1}/\alpha_{j2}$ with α_{j1}, α_{j2} coprime positive integers (j=1,2,3). Let $a_j \geq \max\{\alpha_{j1},e\}(j=1,2,3)$, and assume that $\gcd(b_1,b_2,b_3)=1$. Let $b'=(\frac{b_2}{\log a_1}+\frac{b_1}{\log a_2})(\frac{b_2}{\log a_3}+\frac{b_3}{\log a_2})$ and assume that $B \geq \max\{B_0,\log b'\}$. Either $\{b_1,b_2,b_3\}$ is (c_4,B) - linearly dependent over $\mathbb Z$ (with respect to (a_1,a_2,a_3)) or

$$|\Lambda| > \exp\Big\{ - CB^2 \Big(\prod_{j=1}^3 \log a_j \Big) \Big\},$$

where $c_4 \& C = c_1 c_2 \log \rho + \delta$ are given by Table 2 in Section 6.

In comparison, Baker and Wüstholz [2] obtain

$$\Lambda > \exp\Big\{-C(\log b)\Big(\prod_{j=1}^3 \log a_j\Big)\Big\},\,$$

with $C \le 1.5 \times 10^{12}$, where $b = \max\{|b_j| : j = 1, 2, 3\}$.

Part of the technical difficulties to prove this theorem occur in Section 3. They arise when we try to take full advantage of the weak linear dependence. If we remove such assumptions, the easier portion of Section 3 yields a constant C (in both Theorems A and B) that is 8 times the value stated.

Clearly, the result of Baker and Wüstholz is much tighter than our theorems in terms of the parameters; so it is much nicer both theoretically and for large values of $\log b$ and $\log b'$ (since we have an extra $\log b'$ in our result). (Thus our table is only for $\log b' \leq 10^6$.) However, in many cases our result is more useful for applications, for example when solving certain Diophantine equations.

Our proof follows Laurent's original idea [11]. In Section 2.2, we consider the real-valued determinant of a certain matrix; this is akin to Baker's auxiliary function but (as in the case with Schneider's method) avoids "multiplicity" estimates caused by derivatives. In Section 2.3, we use the Maximum Modulus Principle to obtain an upper bound on this determinant (assuming that our non-zero linear form—actually a modification thereof—is "close" to 0). In this we improve the estimates of [33, Chapter 9] in the case of three logarithms. In Section 2.4 we give a lower bound on the absolute value of the determinant using an inequality of Liouville (assuming that the determinant is non-zero). In Section 2.5, we combine these results to obtain a contradiction (to a modified linear form being close to 0) under appropriate assumptions on certain parameters. Consequently we deduce that our modified linear form is not too close to 0.

In Section 3, we take fuller advantage of the theory of algebraic varieties in 3-space. We considerably refine the general theory of "zero" estimates in this setting by a careful analysis of the intersections of translates of hypersurfaces under the group $\bar{\mathbb{Q}}_+^2 \times \bar{\mathbb{Q}}_-^*$. Our contribution here is to use sets of different cardinalities to lower the dimension of certain algebraic sets and to eliminate one key case by a combinatorial argument. As a consequence of this analysis, we are able to deduce that our determinant is non-zero under considerably weaker hypotheses than had been used previously.

In Section 4, we determine constants that fit all our required specifications, and in Section 5 we show how these result in bounding our original linear form sufficiently away from 0. Finally, in Section 6 we provide computer-generated tables to complete the proof of Theorem B (and so Theorem A). These tables will be useful for anyone wishing to solve Diophantine equations that lead to linear forms in three logarithms.

Acknowledgements: It is a great pleasure to thank Alan Baker for greatly encouraging us to pursue this line of research specifically for three logarithms and Michel Waldschmidt for having previously provided us with a preprint of [33] which made it possible. We are also grateful to Michel Waldschmidt for finding a "howler" in an earlier version of this paper, and for suggesting improvements of a rough draft of the original manuscript.

We have been fortunate to receive the support of both throughout. We also owe a great thank you to Paul Voutier for the many hours he spent checking our results. We are especially grateful to him for pointing out a more felicitous proof of Lemma 2.2 for the case $\Lambda < 0$; our original proof resulted in an increase in the constant in the table by a factor of approximately 2 when Λ was negative.

S1. Background Definitions and Lemmata.

Throughout the paper we will use |A| to denote the cardinality of a set A. We will also use [a] to denote the greatest integer less than or equal to a real number a. So $[a] \le a < [a] + 1$.

1.1. A Combinatorial Fact.

We will need the following combinatorial result from [14] (where their K corresponds to our K^2 , and their S to our ST):

LEMMA 1.1. [14, Lemme 4]. Let K, L, R, S, &T be positive rational integers and $N = K^2L$. Let $\ell_n = [(n-1)/K^2](1 \le n \le N)$ and $(r_1, ..., r_N)$ be a sequence of integers belonging to the set $\{0, ..., R-1\}$. Suppose further that $N \le RST$, and for each $r \in \{0, ..., R-1\}, |\{j : r_j = r\}| \le ST$. Then

$$\Big|\sum_{n=1}^{N} \ell_n r_n - M\Big| \le G_R$$

where $M = (\frac{L-1}{2}) \sum_{n=1}^{N} r_n$ and $G_R = NLR/8$.

1.2. Algebraic Geometry.

Throughout, if K is a field, we use K[X,Y,Z] for the ring of polynomials (over K) in the commuting variables X,Y,Z. If $\mathcal{P} \subseteq K[X,Y,Z]$, we write $V(\mathcal{P})$ for the variety generated by \mathcal{P} , i.e.,

$$V(\mathcal{P}) = \{(x, y, z) \in K^3 : P(x, y, z) = 0 \text{ for all } P \in \mathcal{P}\}.$$

Any such set is also called an algebraic set.

We will need some background from algebraic groups. We will confine our attention to subgroups of $G = \bar{\mathbb{Q}}_+ \times \bar{\mathbb{Q}}_+ \times \bar{\mathbb{Q}}^*$, where the operation (denoted by +) is addition on the first two coordinates and multiplication on the third; so

$$(x_1, y_1, z_1) + (x_2, y_2, z_2) = (x_1 + x_2, y_1 + y_2, z_1 z_2).$$

A subgroup of G that is an algebraic set (the set of common zeros of a family of polynomials $\{P(X,Y,Z): P \in \mathcal{P}\}\$) is called an algebraic subgroup. Any algebraic subgroup of G has the form $\mathcal{U} \times \mathbb{Q}^*$, $\mathcal{U} \times \{1\}$ or $\mathcal{U} \times \mathcal{T}_m$ for some vector subspace \mathcal{U} of \mathbb{Q}^2 and positive integer m, where \mathcal{T}_m is the multiplicative group of m^{th} roots of unity [9]. For simplicity, we write \mathcal{T}_0 for $\bar{\mathbb{O}}^*$. An algebraic set \mathcal{S} is said to be *irreducible* if it cannot be written as the union of two algebraic sets properly contained in S. Every algebraic set can be written uniquely as a finite union of irreducible algebraic sets [9, Corollary I.1.6, and these constituent irreducible algebraic subsets of S are called its irreducible components. It is possible to define the dimension of an irreducible algebraic set so that points have dimension $0, \bar{\mathbb{Q}}^3$ has dimension 3 and if $V_1 \subsetneq V_2$ with V_1, V_2 irreducible algebraic sets, then dim V_1 < $\dim V_2$ (see, e.g., [10, Chapter 2]). These definitions coincide with the usual intuitive ideas: irreducible curves have dimension 1, irreducible surfaces dimension 2. The dimension of an algebraic set is just the maximum of the dimensions of its irreducible components.

In this setting, we define the bidegree of a polynomial $P(X,Y,Z) \in \bar{\mathbb{Q}}[X,Y,Z]$ to be at most (D_0,D_1) if $P(X,Y,Z) = \sum c_{ijk}X^iY^jZ^k$ with $c_{ijk} = 0$ whenever $i+j > D_0$ or $k > D_1$. Let $\bar{\mathbb{Q}}[X,Y,Z]_{\leq (D_0,D_1)}$ denote the set of polynomials in $\bar{\mathbb{Q}}[X,Y,Z]$ of bidegree at most (D_0,D_1) . For any subset E of $\bar{\mathbb{Q}} \times \bar{\mathbb{Q}} \times \bar{\mathbb{Q}}$, let $E^{\bar{\mathbb{Q}}}$ be the set of all maps from E to $\bar{\mathbb{Q}}$. Consider the $\bar{\mathbb{Q}}$ -linear map

$$\operatorname{res}_E: \bar{\mathbb{Q}}[X,Y,Z] \to {}^E\bar{\mathbb{Q}}$$

which maps each $P \in \overline{\mathbb{Q}}[X,Y,Z]$ to the restriction to E of the polynomial map from $\overline{\mathbb{Q}}^3$ to $\overline{\mathbb{Q}}$ induced by P. For each pair of non-negative integers (D_0, D_1) , let

$$H(E; D_0, D_1) = \dim_{\bar{\mathbb{Q}}}(\operatorname{res}_E \bar{\mathbb{Q}}[X, Y, Z]_{<(D_0, D_1)}).$$

If \bar{E} is the smallest algebraic set containing E, then as $\operatorname{res}_{\bar{E}}$ and $\operatorname{res}_{\bar{E}}$ have the same kernels, we obtain

$$H(E; D_0, D_1) = H(\bar{E}; D_0, D_1).$$

If D_0 and D_1 are not too small, then $H(E; D_0, D_1)$ coincides with the value at the point (D_0, D_1) of a polynomial whose (total) degree is $n = \dim(\bar{E})$:

$$H(E; D_0, D_1) = \sum_{i+j \le n} a_{ij} D_0^i D_1^j.$$

This polynomial is called the *Hilbert-Samuel bihomogeneous polynomial of* E. We denote by $\mathcal{H}(E; D_0, D_1)$ the product of n! and the *homogeneous* part of the Hilbert-Samuel bihomogeneous polynomial of E of total degree n evaluated at (D_0, D_1) . So

$$\mathcal{H}(E; D_0, D_1) = n! \sum_{i+j=n} a_{ij} D_0^i D_1^j \quad (n = \dim(\bar{E})).$$

We will require the following facts:

LEMMA 1.2. With the above notation:

- (i) $\mathcal{H}(G; D_0, D_1) = 3D_0^2 D_1$.
- (ii) Let \mathcal{U} be an algebraic subset $\overline{\mathbb{Q}}^2$ of dimension δ_0 , and m be a nonnegative integer. If the subgroup \mathcal{T}_m of $\overline{\mathbb{Q}}^*$ has dimension δ_1 , then

$$\frac{(\delta_0 + \delta_1)!}{\delta_0! \delta_1!} D_0^{\delta_0} D_1^{\delta_1} \leq \mathcal{H}(\mathcal{U} \times \mathcal{T}_m; D_0, D_1).$$

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

$$\mathcal{H}(\mathcal{V}+g;D_0,D_1)=\mathcal{H}(\mathcal{V};D_0,D_1).$$

(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

$$\mathcal{H}(E; D_0, D_1) = |E/H|\mathcal{H}(H; D_0, D_1).$$

- (v) If V and \mathfrak{X} are algebraic subsets of G and $E = \{g \in G : g + V \subseteq \mathfrak{X}\}$, then E is an algebraic set. Moreover, if \mathfrak{X} is defined by polynomials of bidgree at most (D_0, D_1) , then so is E.
- (vi) If E is a non-empty algebraic subset of G defined by polynomials of bidegree at most (D_0, D_1) , then

$$\mathcal{H}(E; D_0, D_1) \leq \mathcal{H}(G; D_0, D_1).$$

Part (i) is obvious (see [33, Chapter 8]). Parts (ii)-(vi), are Proposition 8.3, Lemmas 8.11, 8.12, 8.13, and Proposition 8.14 of [33], respectively.

1.3. The Multiplicity of a Zero.

Let K_0 and I be positive integers and ϕ_1, \ldots, ϕ_I be analytic functions in \mathbb{C} . Let $(k_i, m_i)(1 \leq i \leq I)$ be pairs of non-negative rational integers whose sum is at most K_0 . Let $\ell_1, \ell_2 \in \mathbb{C}$ and for each $i \in \{1, \ldots, I\}$, let

$$f_i(z,\zeta) = z^{k_i} \zeta^{m_i} \phi_i(\ell_1 z + \ell_2 \zeta).$$

Further let $\{(z_i, \zeta_i) : 1 \leq j \leq I\}$ be a set of elements of \mathbb{C}^2 .

Let \mathbb{N} denote the set of non-negative rational integers and for each $(k,m) \in \mathbb{N}^2$, let $\|(k,m)\| = k+m$. We define $\Theta(K_0,I)$ to be the minimum value of $\|(k_1,m_1)\|+\ldots+\|(k_I,m_I)\|$ as $((k_1,m_1)\ldots(k_I,m_I))$ ranges over all I-tuples of elements of \mathbb{N}^2 which are pairwise distinct with $m_1,\ldots,m_I \leq K_0$.

LEMMA 1.3. [33, Lemma 9.1]. The function of one complex variable x given by:

$$\Psi(x) = \det(f_i(xz_j, x\zeta_j))_{1 \le i, j \le I},$$

has a zero at x = 0 of multiplicity at least $\Theta(K_0, I)$.

We now slightly modify the proof of [33, Lemma 9.2] and get an improved lower bound on $\Theta(K_0, I)$:

LEMMA 1.4. Let K_0, L , and I be positive rational integers with $K_0 \ge 998, L \ge 18$, and $(K_0 + 2)^2 L/4 \ge I \ge .15 K_0^2 L$. Then

$$\Theta(K_0, I) \ge I^2 \Big(1 + \frac{3.8}{L} \Big) / 2(K_0 + 1).$$

Proof: The smallest value for the sum $||(k_1, m_1)|| + \ldots + ||(k_I, m_I)||$ is reached when we choose successively, for each integer $n = 0, 1, \ldots$ all the points in the domain

$$D_n = \{(k,m) \in \mathbb{N}^2 : m \le K_0, k+m = n\},\$$

and stop when the total number of points is I. Now

$$|D_n| = \begin{cases} n+1 & \text{if } n \le K_0 \\ K_0 + 1 & \text{if } n \ge K_0. \end{cases}$$

Hence the number of points that we get by varying n between 0 and, say, A-1 (with $A \geq K_0$) is

$$\sum_{n=0}^{K_0-1} (n+1) + \sum_{n=K_0}^{A-1} (K_0+1) = (A - K_0 + \frac{K_0}{2})(K_0+1)$$
$$= (A - \frac{K_0}{2})(K_0+1).$$

Moreover, if A is maximal such that this number is at most I, then

$$\begin{split} \Theta(K_0,I) &\geq \sum_{n=0}^{K_0-1} (n+1)n + \sum_{n=K_0}^{A-1} (K_0+1)n \\ &= \frac{(K_0-1)K_0(2K_0-1)}{6} + \frac{(K_0-1)K_0}{2} \\ &\qquad \qquad + \frac{(K_0+1)}{2} (A(A-1) - K_0(K_0-1)) \\ &\geq \frac{(K_0-1)K_0(2K_0+2)}{6} + \frac{(K_0+1)}{2} A(A-1) \\ &\qquad \qquad - \frac{K_0(K_0+1)(K_0-1)}{2} \\ &= \frac{(K_0+1)}{2} \{A(A-1) - \frac{1}{3} K_0(K_0-1)\}. \end{split}$$

Now A is maximal such that $(A - \frac{K_0}{2})(K_0 + 1) \leq I$; i.e. $A = \left[\frac{I}{K_0 + 1} + \frac{K_0}{2}\right]$. Note that, as desired,

$$A \ge \frac{I}{K_0 + 1} + \frac{K_0}{2} - 1 \ge K_0 \text{ since } I \ge (.15)K_0^2 18 \ge 2K_0^2 \ge \frac{(K_0 + 1)(K_0 + 2)}{2}.$$

Finally, we need to show that

$$A(A-1) - \frac{1}{3}K_0(K_0-1) \ge (\frac{I}{K_0+1})^2(1+\frac{3.8}{L}).$$

Since $A \geq \frac{I}{K_0+1} + \frac{K_0}{2} - 1$, we need only establish that

$$\left(\frac{I}{K_0+1} + \frac{K_0-2}{2}\right)\left(\frac{I}{K_0+1} + \frac{K_0-4}{2}\right) \ge \frac{K_0(K_0-1)}{3} + \left(\frac{I}{K_0+1}\right)^2\left(1 + \frac{3.8}{L}\right).$$

That is

$$\left(\frac{2K_0-6}{2}\right)\left(\frac{I}{K_0+1}\right)+\frac{(K_0-2)(K_0-4)}{4}\geq \frac{K_0(K_0-1)}{3}+\frac{3.8}{L}\left(\frac{I}{K_0+1}\right)^2.$$

Since the function $f(x) = (\frac{K_0-3}{K_0+1})x - \frac{3.8}{L}(\frac{x}{K_0+1})^2$ is decreasing as x increases in the indicated range $(x \ge (.15)K_0^2L)$, we need only check the truth of the inequality at the maximum value of I. Our inequality holds when $I = (K_0 + 2)^2L/4$ provided that

$$\frac{L}{4} \ge \frac{3.8}{16} \left(\frac{K_0 + 2}{K_0 + 1}\right)^2 L + \frac{L}{K_0 + 1} + \frac{1}{6}.$$

Since $K_0 \geq 998$, the righthand side is at most $(.239)L + \frac{1}{6}$. Hence the inequality holds if $(.011)L \geq \frac{1}{6}$. Our assumption that $L \geq 18$ guarantees this. \square

1.4. A Liouville Inequality.

We will need the following special case of an inequality that dates back to J. Liouville. (For a fuller account, see [33, Chapter III]).

LEMMA 1.5. [33, Lemma 3.14]. Let $\alpha_1, \alpha_2, \alpha_3$ be non-zero rational numbers; say $\alpha_j = \alpha_{j1}/\alpha_{j2}$ with α_{j1}, α_{j2} coprime rational integers (j = 1, 2, 3). Let $a_j \geq \max\{|\alpha_{j1}|, |\alpha_{j2}|, e\}(j = 1, 2, 3)$. Let $f(X, Y, Z) \in \mathbb{Z}[X, Y, Z]$ be such that $f(\alpha_1, \alpha_2, \alpha_3) \neq 0$. If $\deg_X f \leq K_1$, $\deg_Y f \leq K_2$ and $\deg_Z f \leq K_3$, then

$$|f(lpha_1,lpha_2,lpha_3)| \geq rac{1}{a_1^{K_1}a_2^{K_2}a_3^{K_3}}.$$

1.5. A Product of Factorials.

The purpose of this section is to derive a lower bound for $\prod_{k=1}^{K-1} (k!)$. The proof we give was kindly suggested to us by Paul Voutier.

LEMMA 1.6. For any integer $K \geq 6$, we have

$$\left(\prod_{k=1}^{K-1} (k!)\right)^{4/K(K-1)} \ge K^2/e^3.$$

Proof: A well-known and easy consequence of Stirling's Formula is

$$\log(k!) \ge (k + \frac{1}{2})\log k - k.$$

Hence

$$\begin{split} \sum_{k=1}^{K-1} \log(k!) &\geq \sum_{k=1}^{K-1} (k + \frac{1}{2}) \log k - \sum_{k=1}^{K-1} k \\ &= \sum_{k=1}^{K-1} k \log k + \frac{1}{2} \log((K-1)!) - \frac{(K-1)K}{2} \\ &\geq \sum_{k=1}^{K-1} k \log k + \frac{1}{2} (K - \frac{1}{2}) \log(K-1) - \frac{K-1}{2} - \frac{(K-1)K}{2}. \end{split}$$

By the Euler-Maclaurin Summation Formula,

$$\sum_{k=1}^{K-1} k \log k \ge \frac{(K-1)^2}{2} \log(K-1) - \frac{(K-1)^2}{4} + \frac{(K-1)}{2} \log(K-1).$$

Therefore

$$\frac{4}{K(K-1)} \sum_{k=1}^{K-1} \log(k!) \ge 2(\frac{K-1}{K}) \log(K-1) + \frac{2}{K} \log(K-1) + \frac{(2K-1)}{K(K-1)} \log(K-1) - \frac{(3K+1)}{K}$$
$$= (2 + \frac{2K-1}{K(K-1)}) \log(K-1) - \frac{1}{K} - 3.$$

Hence, in order to prove the lemma, it suffices to show (for $K \geq 6$) that

$$(2 + \frac{2K - 1}{K(K - 1)})\log(K - 1) - \frac{1}{K} > 2\log K.$$

This will certainly hold if

$$(2K+2)\log(K-1) > 2K\log K + 1.$$

If $f(x) = (2x + 2) \log(x - 1) - 2x \log x - 1$, then f''(x) < 0 if x > 1; and as $\lim_{x \to \infty} f'(x) = 0$, it follows that f'(x) > 0 for all x > 1. But f(6) > 0. Thus

$$(2K+2)\log(K-1) > 2K\log K + 1$$

for $K \geq 6$, proving the lemma. \square

S2. Analytic Results.

2.1. Preliminary Definitions.

Let $\alpha_1, \alpha_2, \alpha_3$ be multiplicatively independent rational numbers greater than 1; let $\alpha_j = \alpha_{j1}/\alpha_{j2}$ with α_{j1}, α_{j2} coprime positive rational integers (j=1,2,3). Let $a_j \geq \max\{\alpha_{j1},e\}$, and assume (without loss of generality) that $a_1 \geq a_3$. Let b_1,b_2,b_3 be positive rational integers with $\gcd(b_1,b_2,b_3)=1$. Let $\Lambda=b_2\log\alpha_2-b_1\log\alpha_1-b_3\log\alpha_3\neq 0$ with $b_2\log\alpha_2=\max\{b_j\log\alpha_j:j=1,2,3\}$.

Let K and L be positive integers, and $N=K^2L$. Let i be an index such that (k_i, m_i, ℓ_i) runs through all triples of integers with $0 \le k_i \le K-1$, $0 \le m_i \le K-1$, & $0 \le \ell_i \le L-1$. So each number $0, \ldots, K-1$ occurs KL times as a k_i , and similarly as an m_i ; and each number $0, \ldots, L-1$ occurs K^2 times as an ℓ_i .

Let R, S and T be positive rational integers with $RST \geq N = K^2L$.

2.2. The Interpolation Determinant.

The rest of Section 2 is an adaptation of Laurent's method of interpolations (see [13] or [14]). With the above definitions, let

$$\Delta = \det \left\{ \binom{r_jb_2 + s_jb_1}{k_i} \binom{t_jb_2 + s_jb_3}{m_i} \alpha_1^{\ell_ir_j} \alpha_2^{\ell_is_j} \alpha_3^{\ell_it_j} \right\}$$

where r_j, s_j, t_j are non-negative integers less than R, S, T, respectively, such that (r_j, s_j, t_j) runs through N distinct triples.

Suppose that these N distinct triples can be chosen so that $\Delta \neq 0$. Let $b_1, b_2, b_3 \in \mathbb{Z}^+$, and let $\beta_1 = b_1/b_2$, $\beta_3 = b_3/b_2$. Recall

$$\Lambda = b_2 \log \alpha_2 - b_1 \log \alpha_1 - b_3 \log \alpha_3.$$

Let

$$\lambda_i = \ell_i - \frac{L-1}{2}$$
 $\eta_0 = \frac{R-1}{2} + \beta_1 \frac{S-1}{2}$ $\zeta_0 = \frac{T-1}{2} + \beta_3 \frac{S-1}{2}$.

Let

$$b = (2b_2\eta_0)(2b_2\zeta_0) / \left(\prod_{k=1}^{K-1} k!\right)^{4/K(K-1)}.$$

Then $\sum_{i=0}^{N-1} \lambda_i = 0$ and

$$\alpha_1^{\lambda_i r_j} \alpha_2^{\lambda_i s_j} \alpha_3^{\lambda_i t_j} = \alpha_1^{\lambda_i (r_j + s_j \beta_1)} \alpha_3^{\lambda_i (t_j + s_j \beta_3)} e^{\lambda_i s_j \frac{\Lambda}{b_2}}$$

$$= \alpha_1^{\lambda_i (r_j + s_j \beta_1)} \alpha_3^{\lambda_i (t_j + s_j \beta_3)} (1 + \Lambda' \theta_{ij})$$

$$(2.1)$$

where

$$\Lambda' = |\Lambda| \max \left\{ rac{LRe^{LR|\Lambda|/2b_1}}{2b_1} \, , rac{LSe^{LS|\Lambda|/2b_2}}{2b_2} \, , rac{LTe^{LT|\Lambda|/2b_3}}{2b_3}
ight\}$$

and

$$\theta_{ij} = \frac{e^{\lambda_i s_j \Lambda/b_2} - 1}{\Lambda'}.$$

Since s_i, b_2, L and $|\Lambda|$ are all positive, $|\lambda_i| \leq \Lambda/2$ and $s_i \leq S$, we have

$$|\theta_{ij}| \le \frac{e^{LS|\Lambda|/2b_2} - 1}{(\frac{LS|\Lambda|}{2b_2})e^{LS|\Lambda|/2b_2}} = \frac{e^x - 1}{xe^x}$$

where $x = LS|\Lambda|/2b_2$. Now $\frac{e^x-1}{xe^x}$ decreases in $(0,\infty)$ and tends to 1 as $x \to 0^+$ by L'Hôpital's rule. Hence $|\theta_{ij}| \le 1$.

We wish to bound Λ away from 0. As a first step we bound Λ' away from 0. Under appropriate assumptions, we now show that $\Lambda' > 1/\rho^{KL}$, for an appropriate $\rho \geq e$. (We will use the Proposition 2.1 to show a similar result for $|\Lambda|$ in Section 5.)

PROPOSITION 2.1. Suppose that $K \geq 500$ and $L \geq 20$. With the above notation, if $\Delta \neq 0$, then $\Lambda' > 1/\rho^{KL}$ provided

$$\left(\frac{KL}{2} - (0.1K - 2)\right) \log \rho + 2(K - 1) \log 2 + 0.001 > (K - 1) \log b
+ (L/4)(\rho + 1)(R \log a_1 + S \log a_2 + T \log a_3) + 2 \log K^2 L.$$
(2A)

We will establish Proposition 2.1 by reductio ad absurdum. We will first obtain an upper bound on $|\Delta|$ (assuming that $\Lambda' \leq \frac{1}{\rho RL}$); the key tool will be an application of the Maximum Modulus Principle and the results in Subsection 1.3. We will next derive a lower bound on $|\Delta|$ (assuming that $\Delta \neq 0$) using Liouville's inequality (Subsection 1.4); however, assumption (2A) forces the lower bound to exceed the upper bound. This contradiction establishes the Proposition.

2.3. The Upper Bound for $|\Delta|$.

In this subsection, we prove:

LEMMA 2.2. If $K \geq 500$, $L \geq 20$ and $\Lambda' \leq 1/\rho^{KL}$, then

$$\begin{aligned} \log |\Delta| &\leq (M_1 + \rho G_1) \log \alpha_1 + (M_2 + \rho G_2) \log \alpha_2 \\ &+ (M_3 + \rho G_3) \log \alpha_3 + N \log N + (K - 1) \frac{N}{2} \log b \\ &- N(K - 1) \log 2 + \left((K - 1)N - \frac{NKL}{4} \left(1 + \frac{3.8}{L} \right) \right) \log \rho + 0.001. \end{aligned} \tag{2U}$$

Proof: Let $z_j = r_j + s_j \beta_1 - \eta_0$ and $\zeta_j = t_j + s_j \beta_3 - \zeta_0$. So $|z_j| \leq \eta_0$ and $|\zeta_j| \leq \zeta_0$. Observe that

$$\binom{r_jb_2+s_jb_1}{k_i}=\frac{b_2^{k_i}}{k_i!}z_j^{k_i}+\text{terms in }z_j\text{ of degree less than }k_i,$$

and similarly for $\binom{t_j b_2 + s_j b_1}{m_i}$. Hence, using the multilinearity of determinants, we obtain that

$$\Delta = \det\left(\frac{b_2^{k_i+m_i}}{k_i!m_i!}z_j^{k_i}\zeta_j^{m_i}\alpha_1^{\ell_i r_j}\alpha_2^{\ell_i s_j}\alpha_3^{\ell_i t_j}\right). \tag{2.2}$$

Let

$$M_1 = \frac{L-1}{2} \sum_{j=1}^{N} r_j$$
, $M_2 = \frac{L-1}{2} \sum_{j=1}^{N} s_j$, $M_3 = \frac{L-1}{2} \sum_{j=1}^{N} t_j$. (2.3)

By (2.2), (2.3), and the definition of λ_i , it follows that

$$\Delta = \alpha_1^{M_1} \alpha_2^{M_2} \alpha_3^{M_3} \det \left(\frac{b_2^{k_i + m_i}}{k_i! m_i!} z_j^{k_i} \zeta_j^{m_i} \alpha_1^{\lambda_i (r_j + s_j \beta_1)} \alpha_3^{\lambda_i (t_j + s_j \beta_3)} (1 + \Lambda' \theta_{ij}) \right).$$

Since $\sum_{i=0}^{N-1} \lambda_i = 0$, we deduce that

$$\Delta = \alpha_1^{M_1} \alpha_2^{M_2} \alpha_3^{M_3} \det \left(\frac{b_2^{k_i + m_i}}{k_i! m_i!} z_j^{k_i} \zeta_j^{m_i} \alpha_1^{\lambda_i z_j} \alpha_3^{\lambda_i \zeta_j} (1 + \Lambda' \theta_{ij}) \right).$$

So, by expansion of this determinant as a "polynomial" in Λ' , we obtain

$$\Delta = \alpha_1^{M_1} \alpha_2^{M_2} \alpha_3^{M_3} \sum_{I \subseteq \mathcal{N}} \Lambda'^{N-|I|} \Delta_I$$

where $\mathcal{N} = \{0, 1, ..., N-1\}$ and Δ_I is the determinant of the matrix \mathcal{M}_I whose (i, j) entry is

$$(\mathcal{M}_I)_{ij} = \begin{cases} \phi_i(z_j, \zeta_j) & \text{if } i \in I, \\ \theta_{ij}\phi_i(z_j, \zeta_j) & \text{if } i \notin I, \end{cases}$$

where

$$\phi_i(z,\zeta) = \frac{b_2^{k_i + m_i}}{k_i ! m_i !} z^{k_i} \zeta^{m_i} \alpha_1^{\lambda_i z} \alpha_3^{\lambda_i \zeta}.$$

Let

$$\Phi_I(x)_{ij} = \left\{ egin{array}{ll} \phi_i(xz_j, x\zeta_j) & & ext{if } i \in I, \ heta_{ij}\phi_i(xz_j, x\zeta_j) & & ext{if } i
otin I. \end{array}
ight.$$

Then, letting $\Psi_I(x) = \det \Phi_I(x)$, gives

$$|\Delta_I| = |\det \Phi_I(1)| = |\Psi_I(1)|.$$

By the Maximum Modulus Principle, if $\frac{\Psi_i(x)}{x^{J_I}}$ were analytic, then $|\Psi_I(1)| \leq \frac{1}{\rho^{J_I}} \max_{|x|=\rho} |\Psi_I(x)|$. Since $|z_j| \leq \eta_0$ and $|\zeta_j| \leq \zeta_0$, we obtain

$$\max_{|x|=\rho} |\Psi_I(x)| \leq N! \frac{b_2^{\sum k_i + \sum m_i}}{\prod k_i! \prod m_i!} (\rho \eta_0)^{\sum k_i} (\rho \zeta_0)^{\sum m_i} \max_{\sigma \in \operatorname{Sym}(\mathcal{N})} \left\{ \alpha_1^{\rho \sum \lambda_i z_{\sigma(i)}} \alpha_3^{\rho \sum \lambda_i z_{\sigma(i)}} \right\}$$

$$(2.4)$$

Define $G_1 = LRN/8$, $G_2 = LSN/8$ and $G_3 = LNT/8$. Now, by Lemma 1.1 and the fact that $\sum_{i=0}^{N-1} \lambda_i = 0$, we obtain

$$\begin{split} \sum_{i=0}^{N-1} \lambda_i z_{\sigma(i)} &= \sum_{i=0}^{N-1} \lambda_i (r_{\sigma(i)} + s_{\sigma(i)} \beta_1 - \eta_0) \\ &= \sum_{i=0}^{N-1} \lambda_i (r_{\sigma(i)} + s_{\sigma(i)} \beta_1) \\ &= \sum_{i=0}^{N-1} \left(\ell_i - \frac{L-1}{2} \right) r_{\sigma(i)} + \beta_1 \sum_{i=0}^{N-1} \left(\ell_i - \frac{L-1}{2} \right) s_{\sigma(i)} \\ &\leq G_1 + \beta_1 G_2. \end{split}$$

Similarly $\sum_{i=0}^{N-1} \lambda_i \zeta_{\sigma(i)} \leq G_3 + \beta_3 G_2$. Since α_1 and α_3 exceed 1, we deduce that

$$\alpha_1^{\rho \Sigma \lambda_i z_{\sigma(i)}} \alpha_3^{\rho \Sigma \lambda_i \zeta_{\sigma(i)}} \le \alpha_1^{\rho(G_1 + \beta_1 G_2)} \alpha_3^{\rho(G_3 + \beta_3 G_2)} \le \alpha_1^{\rho G_1} \alpha_2^{\rho G_2} \alpha_3^{\rho G_3} \quad (2.5^+)$$

if $\Lambda > 0$ (since $\Lambda = b_2(\log \alpha_2 - \beta_1 \log \alpha_1 - \beta_3 \log \alpha_3)$).

If
$$\Lambda < 0$$
, then $-\rho G_2 \Lambda/b_2 = \rho G_2 |\Lambda|/b_2 > 0$ and

$$\alpha_1^{\rho\beta_1G_2}\alpha_3^{\rho\beta_3G_2} = \alpha_2^{\rho G_2} \exp(-\rho G_2\Lambda/b_2).$$

Let $y=LS|\Lambda|/2b_2>0$. Then $\Lambda'\geq ye^y;$ so as $\Lambda'<\frac{1}{\rho^{KL}}$, we have that $\frac{1}{\rho^{KL}}\geq ye^y>y$. Hence $\rho G_2|\Lambda|/b_2=\frac{\rho N}{4}\frac{LS|\Lambda|}{2b_2}=\frac{\rho Ny}{4}<\frac{\rho K^2L}{4\rho^{KL}}$. Since $\rho\geq e,\ K\geq 500$ and $L\geq 20$, the expression $\frac{\rho K^2L}{4\rho^{KL}}$ decreases as r increases. Therefore $\frac{\rho K^2L}{4\rho^{KL}}\leq \frac{eK^2L}{4e^{KL}}$ $(K\geq 500, L\geq 20)$. Thus $\exp(-\rho G_2\Lambda/b_2)<\exp(.0009)<1.001$. Consequently,

$$\alpha_1^{\rho\beta_1G_2}\alpha_3^{\rho\beta_3G_2} \le 1.001\alpha_2^{\rho G_2}$$

Thus

$$\alpha_1^{\rho \Sigma \lambda_i z_{\sigma(i)}} \alpha_3^{\rho \Sigma \lambda_i \zeta_{\sigma(i)}} \leq \alpha_1^{\rho(G_1 + \beta_1 G_2)} \alpha_3^{\rho(G_3 + \beta_3 G_2)} \leq 1.001 \alpha_1^{\rho G_1} \alpha_2^{\rho G_2} \alpha_3^{\rho G_3} \quad (2.5^-)$$

if $\Lambda < 0$; that is, we have an extra 1.001 in the upper bound. Hence, for $\Lambda \neq 0$,

$$|\Delta| \leq 1.001 \alpha_{1}^{M_{1} + \rho G_{1}} \alpha_{2}^{M_{2} + \rho G_{2}} \alpha_{3}^{M_{3} + \rho G_{3}} (N!) 2^{N} \rho^{\Sigma(k_{i} + m_{i})} \frac{(b_{2} \eta_{0})^{\Sigma k_{i}}}{\Pi(k_{i}!)} \frac{(b_{2} \zeta_{0})^{\Sigma m_{i}}}{\Pi(m_{i}!)} \max_{I \subseteq \mathcal{N}} \frac{|\Lambda'|^{N - |I|}}{\rho^{J_{I}}}.$$

$$(2.6)$$

As $|\Lambda'| \leq \frac{1}{\rho^{KL}}$, we have

$$\frac{|\Lambda'|^{N-|I|}}{\rho^{J_I}} \le \frac{1}{\rho^{KL(N-|I|)|J_I}}.$$

If $|I| \leq [.6N]$, then $KL(N-|I|) + J_I \geq (.4)NKL > \frac{NKL}{4} \left(1 + \frac{3.8}{L}\right)$. If |I| > [.6N], then $|I| > (.6)K^2L - 1 \geq (.15)(2(K-1))^2L$ since $L \geq 18$ and $K \geq 500$. By Lemmas 1.3 and 1.4, (with $K_0 = 2(K-1)$) we may assume that

$$J_i \ge \Theta(2(K-1), |I|) \ge |I|^2 \left(1 + \frac{3.8}{L}\right) / 2(2(K-1) + 1).$$

Therefore $KL(N-|I|) + J_I \ge KL(N-|I|) + \frac{|I|^2(1+\frac{3.8}{L})}{2(2K-1)}$. Since $|I| \le N = K^2L$, $K \ge 500$ and $L \ge 20$, it follows that

$$KL(N-|I|) + J_I \ge \frac{N^2 \left(1 + \frac{3.8}{L}\right)}{2(2K-1)} \ge \frac{NKL}{4} \left(1 + \frac{3.8}{L}\right).$$
 (2.7)

Using (2.7), the equality $\sum_{i=0}^{N-1} k_i = \sum_{i=0}^{N-1} m_i = \frac{(K-1)K}{2}KL = \frac{N}{2}(K-1)$, the definition of b, and that $(N!)2^N \leq N^N$ if $N \geq 6$, we obtain for $\Lambda \neq 0$,

$$\begin{split} \log |\Delta| & \leq (M_1 + \rho G_1) \log \alpha_1 + (M_2 + \rho G_2) \log \alpha_2 + (M_3 + \rho G_3) \log \alpha_3 \\ & + N \log N + (K - 1) \frac{N}{2} \log b - N(K - 1) \log 2 \\ & + \left((K - 1)N - \frac{NKL}{4} \left(1 + \frac{3.8}{L} \right) \right) \log \rho + .001. \quad \Box \end{split}$$

2.4. A Lower Bound for $|\Delta|$.

Under the assumption that $\Delta \neq 0$, we use Lemma 1.5 to establish

LEMMA 2.3. With the above assumptions and notation,

$$\log |\Delta| \ge -2\left(\sum_{j=1}^{3} G_j \log a_j\right) + \sum_{j=1}^{3} (M_j + G_j) \log \alpha_j. \tag{2L}$$

Proof: Consider the polynomial

$$P(X,Y,Z) = \sum_{\sigma} \operatorname{sg}(\sigma) \prod_{i=1}^{N} \binom{r_{\sigma(i)}b_2 + s_{\sigma(i)}b_1}{k_i} \binom{t_{\sigma(i)}b_2 + s_{\sigma(i)}b_3}{m_i} \cdot X^{n_{r\sigma}} Y^{n_{s\sigma}} Z^{n_{t\sigma}},$$

where $n_{r\sigma} = \sum_{i=1}^{N} \ell_i r_{\sigma(i)}$, $n_{s\sigma} = \sum_{i=1}^{N} \ell_i s_{\sigma(i)}$, & $n_{t\sigma} = \sum_{i=1}^{N} \ell_i t_{\sigma(i)}$, and σ ranges over the elements of the symmetric group on N letters; as usual, $sg(\sigma)$ denotes the signature of σ . Clearly $\Delta = P(\alpha_1, \alpha_2, \alpha_3)$. By Lemma 1.1,

$$|\deg_X P - M_1| \le G_1,$$

 $|\deg_Y P - M_2| \le G_2, \text{and}$
 $|\deg_Z P - M_3| \le G_3.$

Let $V_j = [M_j + G_j]$ and $U_j = \lceil M_j - G_j \rceil (j = 1, 2, 3)$. Then $\Delta = P(\alpha_1, \alpha_2, \alpha_3) = \alpha_1^{V_1} \alpha_2^{V_2} \alpha_3^{V_3} \tilde{P}\left(\frac{1}{\alpha_1}, \frac{1}{\alpha_1}, \frac{1}{\alpha_3}\right)$, where $\tilde{P}(X, Y, Z) \in \mathbb{Z}[X, Y, Z]$ has

$$\deg_X \tilde{P} \leq V_1 - U_1,$$

 $\deg_Y \tilde{P} \leq V_2 - U_2,$ and
 $\deg_Z \tilde{P} \leq V_3 - U_3.$

By Lemma 1.5, (since $|\alpha_{j_2}| < |\alpha_{j_1}|$),

$$\log \left| \tilde{P}\left(\frac{1}{\alpha_1}, \frac{1}{\alpha_2}, \frac{1}{\alpha_3}\right) \right| \ge -\sum_{j=1}^3 (V_j - U_j) \log a_j.$$

Hence

$$\log |\Delta| \ge -\sum_{j=1}^{3} (V_j - U_j) \log a_j + \sum_{j=1}^{3} V_j \log \alpha_j.$$
 (2.8)

Now

$$2G_j - (V_j - U_j) \ge (M_j + G_j - V_j)$$
 $(j = 1, 2, 3);$

and since $0 \le \log \alpha_i \le \log a_i$, we get (for j = 1, 2, 3)

$$(2G_j - (V_j - U_j))\log a_j \ge (M_j + G_j - V_j)\log \alpha_j.$$

Consequently, (2L) follows at once from (2.8). \square

2.5. Synthesis.

By (2U) and (2L), we deduce that

$$-2\sum_{j=1}^{3} G_{j} \log a_{j} + \sum_{j=1}^{3} (M_{j} + G_{j}) \log \alpha_{j} \leq$$

$$\leq \sum_{j=1}^{3} (M_{j} + \rho G_{j}) \log \alpha_{j} + N \log N + N \log 2$$

$$+ (K - 1) \frac{N}{2} \log b - N(K - 1) \log 2$$

$$+ \left((K - 1)N - \frac{NKL}{4} \left(1 + \frac{3.8}{L} \right) \right) \log \rho + .001.$$

This simplifies to

$$\begin{split} (\rho - 1)(G_1 \log \alpha_1 + G_2 \log \alpha_2 + G_3 \log \alpha_3) + N \log N \\ &+ 2(G_1 \log a_1 + G_2 \log a_2 + G_3 \log a_3) + (K - 1)\frac{N}{2} \log b \\ &\geq N(K - 1) \log 2 + \frac{N}{2} \left(\frac{KL}{2} - (0.1K - 2)\right) \log \rho + .001. \end{split}$$

Since $\log a_j \geq \log \alpha_j > 0 (j = 1, 2, 3)$, substituting a_j for α_j and using the definition of G_j (j = 1, 2, 3), we get a contradiction to the assumption $|\Lambda'| \leq \frac{1}{\rho KL}$ if inequality (2A) holds. This establishes Proposition 2.1. \square

Our next goal is to put conditions on R, S, T, K and L to ensure $N = K^2 L$ distinct triples (r_j, s_j, t_j) can be chosen so that the resulting Δ is non-zero. Equivalently, so that the $N \times RST$ matrix resulting from <u>all</u> triples has full

row rank. By row reduction, as in (2.2) with η_0 and ζ_0 both replaced by 0, this occurs if and only if the matrix with (i,j) entry $(r_j + s_j\beta_j)^{k_i}(t_j + s_j\beta_3)^{m_i}(\alpha_1^{r_j}\alpha_2^{s_j}\alpha_3^{t_j})^{\ell_i}$ has full row rank. That is, if and only if: the only polynomial $\sum_i \lambda_i X^{k_i} Y^{m_i} Z^{\ell_i}$ having all $(r_j + s_j\beta_1, t_j + s_j\beta_3, \alpha_1^{r_j}\alpha_2^{s_j}\alpha_3^{t_j})$ as roots $(0 \le r_j < R; 0 \le s_j < S; 0 \le t_j < T)$ is the zero polynomial. This concerns polynomials with X and Y degree at most K-1 and Z degree at most L-1.

S3. Row Rank.

In this section we prove a result about zeros of polynomials that guarantees that the full row rank is attained (except under propitious circumstances when better results are possible). Here is where we heavily use algebraic groups. Our zero estimate is similar to Philippon's Zero Estimate ([33, Chapter 8]) but requires a close analysis of the intersections of translates of hypersurfaces under the group $\mathbb{Q}^2_+ \times \mathbb{Q}^*$. It allows us to both eliminate the need for Σ_3 and take Σ_1 and Σ_2 to be sets of very different sizes. We will establish (under mild conditions) that either $\{b_1,b_2,b_3\}$ satisfies a linear dependence relation with small integer coefficients, or the only polynomial of prescribed bounded degree having all $(r_j+s_j\beta_j,\,t_j+s_j\beta_3,\,\alpha_1^{r_j}\,\alpha_2^{s_j}\,\alpha_3^{t_j})\,(j\in\{0,\ldots,N-1\})$ as zeros is the zero polynomial, where $\beta_j=b_j/b_2$ (j=1,2,3). Specifically:

We define $\{b_1, b_2, b_3\}$ to be (R, S, T)-linearly dependent over \mathbb{Z} if there exist $d_1, d_2, d_3 \in \mathbb{Z}$ not all 0 such that $d_1b_1 + d_2b_2 + d_3b_3 = 0$ with $|d_2| \le \min\{R, T\}$ and $|d_1|, |d_3| \le S$; and if $d_2 = 0$, then $|d_1| \le T$ and $|d_3| \le R$.

THEOREM 3. Suppose that $K, L, R, S, T, R_1, S_1, T_1, R_2, S_2, T_2$ are positive integers greater than or equal to 3, and that $K \geq 2L$, $R_1 + R_2 < R$, $S_1 + S_2 < S$ and $T_1 + T_2 < T$. Further assume that $T_1 \geq R_1$ without loss of generality. IF

$$4(R_1+1)(S_1+1) \ge T_1+1, \tag{3.1}$$

$$4(R_1+1)(T_1+1) \ge S_1+1, \tag{3.2}$$

$$(R_2+1)(S_2+1)(T_2+1) > 12(K-1)^2(L-1), (3.3)$$

and

$$(R_1+1)(S_1+1)(T_1+1) > 8(2K+L-2)^2. (3.4)$$

<u>THEN</u> either $\{b_1, b_2, b_3\}$ is (R, S, T)-linearly dependent or the only polynomial $P(X, Y, Z) \in \overline{\mathbb{Q}}[X, Y, Z]$ (with $\deg_X P, \deg_Y P \leq K - 1$ and $\deg_Z P \leq L - 1$) having $\{(r + s\beta_1, t + s\beta_3, \alpha_1^r\alpha_2^s\alpha_3^t) : 0 \leq r \leq R - 1, 0 \leq s \leq S - 1, 0 \leq t \leq T - 1\}$ as roots is the zero polynomial. In the latter case,

the $K^2L \times RST$ matrix with (i,j) entry $\binom{r_jb_2+s_jb_3}{k_i}\binom{t_jb_2+s_jb_3}{m_i}\alpha_1^{\ell_ir_j}\alpha_2^{\ell_is_j}\alpha_3^{\ell_it_j}$ has row rank equal to K^2L . Consequently, for an appropriate subset of K^2L columns, the resulting matrix has determinant Δ that is non-zero.

Under condition (2A) of Proposition 2.1, this will yield our lower bound for Λ' .

To prove Theorem 3, we argue by reductio ad absurdum. Let $\Sigma_j = \{(r+s\beta_1,t+s\beta_2,\alpha_1^r\alpha_2^s\alpha_3^t): 0 \leq r \leq R_j, 0 \leq s \leq S_j, 0 \leq t \leq T_j\}$ (j=1,2). Without loss of generality, P(X,Y,Z) can be written as a product of distinct irreducible polynomials P_1,\ldots,P_n (none of which is a scalar multiple of Z). Let $\mathcal{Z}_0 = V(P) = \bigcup \{V(P_i): 1 \leq i \leq n\}$, the set of zeros of P. Let $\mathcal{Z}_1 = \bigcap_{\sigma \in \Sigma_1} (\mathcal{Z}_0 - \sigma) = \bigcap_{\sigma \in \Sigma_1} \bigcup_{i=1}^n (V(P_i) - \sigma)$. Letting $(\Lambda_1,\ldots,\Lambda_n)$ range over all n-tuples of pairwise disjoint subsets of Σ_1 whose union is Σ_1 , we see (by DeMorgan's Laws) that $\mathcal{Z}_1 = \bigcup_{\Lambda_1 \cup \ldots \cup \Lambda_n = \Sigma_1} \bigcap_{i=1}^n \bigcap_{\sigma \in \Lambda_i} (V(P_i) - \sigma)$. Note that, by hypothesis, $\Sigma_2 \subseteq \mathcal{Z}_1$. If $\{b_1,b_2,b_3\}$ is not (R,S,T)-linearly dependent, then the projection of Σ_j onto the first two coordinates is a one-to-one map (j=1,2); i.e., if $\tilde{\Sigma}_j = \{(r+s\beta_1,t+s\beta_2): 0 \leq r \leq R_j, 0 \leq x \leq S_j, 0 \leq t \leq T_j\}$, then $|\tilde{\Sigma}_j| = (R_j+1)(S_j+1)(T_j+1)$ (j=1,2). Throughout we let $D_0 = 2(K-1)$ and $D_1 = L-1$, and assume (without loss of generality) that $R_1 \leq T_1$.

We wish to establish that the non-empty algebraic set \mathcal{Z}_1 has dimension 0. This will follow from a series of lemmas in the next section:

3.1. The dimension of \mathcal{Z}_1 is 0.

If dim $\mathcal{Z}_1 > 0$, then for some partition $\{\Lambda_1, \ldots, \Lambda_n\}$ of Σ_1 , we must have dim $C_i > 0$ for $i \in \{1, \ldots, n\}$, where $C_i = \bigcap_{\sigma \in \Lambda_i} (V(P_i) - \sigma)$.

PROPOSITION 3.1.1. Under the hypotheses of Theorem 3, the number of elements of $\tilde{\Sigma}_1$ lying on a common line is bounded by

$$M = \max\{(R_1 + 1, S_1 + 1, T_1 + 1, 2((R_1 + 1)(S_1 + 1)(T_1 + 1))^{\frac{1}{2}}\}\$$

= $2((R_1 + 1)(S_1 + 1)(T_1 + 1))^{\frac{1}{2}}$.

unless $\{b_1, b_2, b_3\}$ is (R_1, S_1, T_1) -linearly dependent.

Proof: Suppose the number of elements of $\tilde{\Sigma}_1$ lying on a common line ℓ of slope m is greater than M and that $\{b_1, b_2, b_3\}$ is not (R_1, S_1, T_1) -linearly dependent. By the pigeonhole principle, there exist $\sigma_1, \ldots, \sigma_6 \in \tilde{\Sigma}_1$ all

lying on ℓ such that

$$\sigma_{i} = (r_{i} + s_{i}\beta_{1}, t_{i} + s_{i}\beta_{3}),$$
 $\sigma_{1} \neq \sigma_{2},$
 $\sigma_{3} \neq \sigma_{4},$
 $\sigma_{5} \neq \sigma_{6},$
 $r_{1} = r_{2},$
 $s_{3} = s_{4},$ and
 $t_{5} = t_{6}.$

Simple slope calculations now imply

$$\frac{t_2 - t_1 + (s_2 - s_1)\beta_3}{(s_2 - s_1)\beta_1} = m,$$

$$\frac{t_4 - t_3}{r_4 - r_3} = m,$$

$$\frac{(s_6 - s_5)\beta_3}{r_6 - r_5 + (s_6 - s_5)\beta_1} = m.$$

Case A: $m < \infty$. We shall further assume that $\sigma_1, \ldots, \sigma_4$ are chosen such that $|s_2 - s_1|$ is minimal with respect to $r_1 = r_2$ and that $|r_4 - r_3|$ is minimal with respect to $s_3 = s_4$. Since $m = \frac{t_2 - t_1}{(s_2 - s_1)\beta_1} + \frac{\beta_3}{\beta_1}$ is finite, it follows that $|t_2 - t_1|$ is also minimal with respect to $r_1 = r_2$. Similarly, $|t_4 - t_3|$ is minimal with respect to $s_3 = s_4$. We have

$$\frac{t_4 - t_3}{r_4 - r_3} = \frac{t_2 - t_1 + (s_2 - s_1)\beta_3}{(s_2 - s_1)\beta_1}.$$

Clearing denominators and remembering that $\beta_1 = \frac{b_1}{b_2}$ and $\beta_3 = \frac{b_3}{b_2}$, we obtain the equation

$$(t_4-t_3)(s_2-s_1)b_1=(r_4-r_3)(t_2-t_1)b_2+(r_4-r_3)(s_2-s_1)b_3.$$

By the minimality of $|s_2-s_1|$ in the choice of σ_1 and σ_2 , we know that for each r with $0 \le r \le R_1$, there are at most $\frac{\lceil S_1+1 \rceil}{|s_2-s_1|} \le \frac{2(S_1+1)}{|s_2-s_1|}$ different s's such that there exists $t \in \{0,\ldots,T_1\}$ with $(r+s\beta_1,t+s\beta_3) \in \ell$. However, since $m < \infty$, there is at most one such t for every pair, (r,s). Hence, all together there are at most $\frac{2(R_1+1)(S_1+1)}{|s_2-s_1|}$ points of $\tilde{\Sigma}_1$ on ℓ . By our assumption, we have that

$$\frac{2(R_1+1)(S_1+1)}{|S_2-S_1|} > 2((R_1+1)(S_1+1)(T_1+1))^{\frac{1}{2}},$$

and hence $|s_2 - s_1| < ((R_1 + 1)(S_1 + 1)/(T_1 + 1))^{\frac{1}{2}}$. Similarly, $|t_2 - t_1| < ((R_1 + 1)(T_1 + 1)/(S_1 + 1))^{\frac{1}{2}}$.

Exchanging the roles of r and s in the above argument, we also obtain that

$$\frac{2(R_1+1)(S_1+1)}{|r_4-r_3|} > 2((R_1+1)(S_1+1)(T_1+1))^{\frac{1}{2}},$$

whence $|r_4 - r_3| < ((S_1 + 1)(R_1 + 1)/(T_1 + 1))^{\frac{1}{2}}$. Similarly $|t_4 - t_3| < ((S_1 + 1)(T_1 + 1)/(R_1 + 1))^{\frac{1}{2}}$. Combining the above, we obtain

$$|(t_4 - t_3)(s_2 - s_1)| < S_1 + 1,$$

$$|(r_4 - r_3)(s_2 - s_1)| < (R_1 + 1)(S_1 + 1)/(T_1 + 1) \le S_1 + 1,$$

(since $R_1 \leq T_1$) and

$$|(r_4 - r_3)(t_2 - t_1)| < R_1 + 1.$$

Since $m \neq \infty$, we have $r_4 - r_3 \neq 0$. If $t_2 = t_1$, then we have

$$(t_4-t_3)b_1=(r_4-r_3)b_3.$$

We deduce that if $m \neq \infty$ (and hence $s_2 - s_1 \neq 0$), then $\{b_1, b_2, b_3\}$ is (R_1, S_1, T_1) -linearly dependent. This contradiction arose from our assumption that the number of points of $\tilde{\Sigma}_1$ lying on ℓ is greater than M.

Case B: If the slope were infinite, we would then have

$$(r_6 - r_5) + (s_6 - s_5)\beta_1 = 0.$$

Hence

$$(r_6 - r_5)b_2 + (s_6 - s_5)b_1 = 0.$$

Therefore $\{b_1, b_2, b_3\}$ is (R_1, S_1, T_1) -linearly dependent, thus proving Proposition 3.1.1. \square

If P_i has bidegree (1,0), for each $\sigma \in \Lambda_i$, $V(P_i) - \sigma$ is a line. Since $\dim C_i \geq 1$ and $C_i = \bigcap_{\sigma \in \Lambda_i} (V(P_i) - \sigma)$, all $\sigma \in \Lambda_i$ lie on the same translate of the line $V(P_i)$. Hence, by Proposition 3.1.1, $|\Lambda_i| = |\tilde{\Lambda}_i| \leq M$. Let $\kappa = |A|$ where $A = \{i \in \{1, \ldots, n\} : P_i \text{ has bidegree } (1,0)\}$. Then

$$|\Sigma_1| = |\Lambda_1| + \ldots + |\Lambda_n| \le \kappa M + \sum_{\substack{i=1\\i \notin A}}^n |\Lambda_i|. \tag{3.1.1}$$

Since P has bidgree at most (D_0, D_1) , we have $\kappa \leq D_0$. Further, since $|\Sigma_1| > \kappa M$ (by (3.4)), the complement of A is non-empty. We note an essential difference between the elements of A and its complement. Write t_{σ} for translation by $\sigma \in G$; i.e. $t_{\sigma}(x, y, z) = (x + \sigma_1, y + \sigma_2, z\sigma_3)$ where $\sigma = (\sigma_1, \sigma_2, \sigma_3)$.

LEMMA 3.1.2. Let $P_i(X,Y,Z)$ be an irreducible polynomial other than Z, and $\sigma, \sigma' \in \Sigma_1$ with $\sigma \neq \sigma'$. If $V(P_i \circ t_{\sigma}) = V(P_i \circ t_{\sigma'})$, then P_i has bidegree (1,0).

Proof: If $V(P_i \circ t_{\sigma}) = V(P_i \circ t_{\sigma'})$, then $P_i \circ t_{\sigma} = cP_i \circ t_{\sigma'}$ for some $c \in \mathbb{Q}^*$. We first show that $\deg_Z P_i = 0$.

Write

$$P_i(x, y, z) = \sum_{j,k,\ell} c_{jk\ell} X^j Y^k Z^\ell,$$

 $\sigma = (r + s\beta_1, t + s\beta_3, \alpha_1^r \alpha_2^s \alpha_3^t)$ and $\sigma' = (r' + s'\beta_1, t' + s'\beta_3, \alpha_1^{r'} \alpha_2^{s'} \alpha_3^{t'})$. Examining the term with ℓ maximal so that $c_{jk\ell} \neq 0$ for some j, k and j + k is maximal subject to ℓ being maximal (if there is more than one such (j, k), choose any of them), we must have

$$(\alpha_1^r \alpha_2^s \alpha_3^t)^{\ell} = c(\alpha_1^{r'} \alpha_2^{s'} \alpha_3^{t'})^{\ell},$$

and hence $c = (\alpha_1^{r-r'}\alpha_2^{s-s'}\alpha_3^{t-t'})^{\ell}$. Next we examine the coefficients of the highest order term of P_i with Z power equal to 0. That is, we look at the coefficient c_{jk0} with j+k maximal with respect to $c_{jk0} \neq 0$. If no such term exists, then we have that Z divides P_i contrary to our hypothesis. If more than one such term exists, choose any of them. In this case, we obtain that c=1. Hence

$$(\alpha_1^{r-r'}\alpha_2^{s-s'}\alpha_3^{t-t'})^{\ell} = 1.$$

Since $\{\alpha_1, \alpha_2, \alpha_3\}$ is multiplicatively independent, $\ell = 0$. Therefore $\deg_Z P_i = 0$.

We now shew that P_i is indeed linear in X and Y. Since $P_i \circ t_{\sigma} = cP_i \circ t_{\sigma'}$, if $(x_0, y_0, z_0) \in V(P_i)$, then $(x_0, y_0, z_0) + \mathbb{Z}(\sigma - \sigma') \subseteq V(P_i)$. But $\deg_Z P_i = 0$, so $(x_0, y_0) + \mathbb{Z}(\sigma_1 - \sigma'_1, \sigma_2 - \sigma'_2)$ (where $\sigma = (\sigma_1, \sigma_2, \sigma_3)$) is contained in the variety \mathcal{W}_i of $\bar{\mathbb{Q}}^2$ defined by P_i (viewed as an element of $\bar{\mathbb{Q}}[X, Y]$). Since \mathcal{W}_i passes through infinitely many points of the line $(x_0, y_0) + \bar{\mathbb{Q}}(\sigma_1 - \sigma'_1, \sigma_2 - \sigma'_2)$, we obtain by Bézout's Theorem [9, Corollary I.7.8] that \mathcal{W}_i is this line. Hence P_i has bidegree (1, 0) as claimed. \Box

Our next task is to bound $|\Lambda_i|$ if $i \notin A$. So suppose that $i \notin A$ is fixed. Assume that $|\Lambda_i| \geq 2$. We now show that $C_i = \cap_{\sigma \in \Lambda_i} (V(P_i) - \sigma)$ is one-dimensional. Let $\Lambda_i = \{\tau_1, \ldots, \tau_{n_i}\}$ and (for $j = 1, \ldots, n_i$) \mathcal{H}_j denote the hypersurface $V(P_i \circ t_{\tau_j})$. By Lemma 3.1.2 we have that the hypersurfaces \mathcal{H}_{j_1} and \mathcal{H}_{j_2} are not equal whenever $j_1 \neq j_2, j_1, j_2 \in \{1, \ldots, n_i\}$. Therefore, $\dim(\mathcal{H}_{j_1} \cap \mathcal{H}_{j_2}) \leq 1$. Since $\dim C_i > 0$, we must in fact have that $\dim(\mathcal{H}_{j_1} \cap \mathcal{H}_{j_2}) = 1$ (and C_i is a component of the intersection, and so

has dimension 1). Thus dim $\mathcal{Z}_1 \leq 1$. It follows from the generalization of Bézout's theorem ([9, Theorem I.7.7]) that $\mathcal{H}_{j_1} \cap \mathcal{H}_{j_2}$ has at most N_i^2 irreducible components, where $N_i = \deg P_i$. Note that $\sum_{i \notin A} N_i \leq D_0 + D_1 - \kappa$.

We will now establish three lemmas which will allow us to bound $|\Lambda_i|$.

LEMMA 3.1.3. Assume all of the above hypotheses and notation. 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 $\tau_{j_2} - \tau_{j_1} = \tau_{j_4} - \tau_{j_3}$ (with $\tau_{j_1}, \ldots, \tau_{j_4} \in \Lambda_i$), 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 $v \in C_i$. Since $\tau_{j_1}, \ldots, \tau_{j_4} \in \Lambda_i$, we know

$$P_i \circ t_{\tau_{j_3}}(v) = 0, and$$

$$P_i \circ t_{\tau_{j_4}}(v) = 0.$$

From these equations, we deduce

$$P_i \circ t_{\tau_{j_1}}(t_{\tau_{j_3}-\tau_{j_1}}(v)) = P_i(t_{\tau_{j_3}}(v))$$

= 0,

yielding that $t_{\tau_{j_3}-\tau_{j_1}}(v) \in \mathcal{H}_{j_1}$. Similarly

$$\begin{split} P_i \circ t_{\tau_{j_2}}(t_{\tau_{j_3} - \tau_{j_1}}(v)) &= P_i(t_{\tau_{j_2} + \tau_{j_3} - \tau_{j_1}}(v)) \\ &= P_i(t_{\tau_{j_4}}(v)) \\ &= 0. \end{split}$$

and hence $t_{\tau_{j_3}-\tau_{j_1}}(v)\in\mathcal{H}_{j_2}$ also. Therefore, $t_{\tau_{j_3}-\tau_{j_1}}(\mathcal{C}_i)\subseteq\mathcal{H}_{j_1}\cap\mathcal{H}_{j_2}$, implying that $t_{\sigma}(\mathcal{C}_i)$ is a component of $\mathcal{H}_{j_1}\cap\mathcal{H}_{j_2}$. This proves Lemma 3.1.3. \square

LEMMA 3.1.4. With the above assumptions and definitions, if $\sigma, \sigma' \in \Lambda_i$ and $t_{\sigma}(C_i) = t_{\sigma'}(C_i)$, then $\sigma = \sigma'$.

Proof: Let $F = \{g \in G : \mathcal{C}_i + g = \mathcal{C}_i\}$, which is an algebraic subgroup of G by Lemma 1.2(v). Hence $F = \mathcal{U} \times \mathcal{T}_m$ for some vector subspace \mathcal{U} of \mathbb{Q}^2 and $m \geq 0$. If $t_{\sigma}(\mathcal{C}_i) = t_{\sigma'}(\mathcal{C}_i)$, then $\sigma - \sigma' \in F$. If $\sigma \neq \sigma'$, then as $\{\alpha_1, \alpha_2, \alpha_3\}$ is multiplicatively independent, it follows that m = 0. Moreover, since the projection of Λ_i onto the first two coordinates is one-to-one, the projection of $\sigma - \sigma'$ is a non-zero element of U; so $\dim \mathcal{U} \geq 1$. Hence $\dim \mathcal{C}_i \geq 2$, a contradiction. \square

LEMMA 3.1.5. With the above notation and hypotheses, the set Λ_i cannot contain $N_i^2 + 1$ distinct pairs $(\tau_{j_1} - \tau_{j_2})$ such that τ_{j_1}, τ_{j_2} is a non-zero constant independent of j.

Proof: Suppose otherwise. By Lemma 3.1.3, for each such pair, $t_{\tau_{j_1}-\tau_{l_1}}(\mathcal{C}_i)$ is a component of $\mathcal{H}_{j_1} \cap \mathcal{H}_{j_2}$. Since we know that $\mathcal{H}_{j_1} \cap \mathcal{H}_{j_2}$ has at most N_i^2 components, the pigeonhole principle implies either for some $j \neq 1$ we have $t_{\tau_{j_1}-\tau_{l_1}}(\mathcal{C}_i) = \mathcal{C}_i$, or there exist j and j' such that

$$t_{\tau_{j_1}-\tau_{1_1}}(\mathcal{C}_i)=t_{\tau_{j'_1}-\tau_{1_1}}(\mathcal{C}_i).$$

In the former case, we have that $t_{\tau_{j_1}}(\mathcal{C}_i) = t_{\tau_{1_1}}(\mathcal{C}_i)$, and in the latter case, we have $t_{\tau_{j_1}}(\mathcal{C}_i) = t_{\tau_{j'_1}}(\mathcal{C}_i)$. Since $\tau_{j_1} \neq \tau_{j'_1}$ if $j \neq j'$, we get a contradiction to Lemma 3.1.4. Hence Lemma 3.1.5 is true. \square

We now have the tools to bound $|\Lambda_i|$. To do so, we will count the total number of possible differences for the pair (τ_{j_1}, τ_{j_2}) . Then we will count the number of distinct pairs of elements of the set Λ_i . By comparing these and using the pigeonhole principle, we will be able to find a bound.

Recall that $n_i = |\Lambda_i|$. Since $0 \le r \le R_1$, $0 \le s \le S_1$, and $0 \le t \le T_1$, the number of possible non-zero values for $\tau_{j_1} - \tau_{j_2}$ where $\tau_{j_1}, \tau_{j_2} \in \Lambda_i$ is at most

$$(2R_1+1)(2S_1+1)(2T_1+1)-1.$$

On the other hand, the number of distinct ordered pairs of distinct elements of Λ_i is $n_i(n_i-1)$. Thus if

$$n_i(n_i-1) > N_1^2((2R_1+1)(2S_1+1)(2T_1+1)-1),$$

we would obtain a contradiction to Lemma 3.1.5 by the pigeonhole principle. Hence,

$$n_i^2 - n_i - N_i^2((2R_1 + 1)(2S_1 + 1)(2T_1 + 1) - 1) \le 0.$$

Applying the quadratic formula, we have:

$$n_i \le \frac{1}{2} (1 + \sqrt{1 + 4N_i^2((2R_1 + 1)(2S_1 + 1)(2T_1 + 1) - 1)}).$$

Since $1 < 4N_i^2$, this reduces to

$$n_{i} \leq \frac{1}{2} + \frac{1}{2} \sqrt{32N_{i}^{2}(R_{1} + \frac{1}{2})(S_{1} + \frac{1}{2})(T_{1} + \frac{1}{2})}$$

$$= \frac{1}{2} + 2\sqrt{2}N_{i}((R_{1} + \frac{1}{2})(S_{1} + \frac{1}{2})(T_{1} + \frac{1}{2}))^{\frac{1}{2}}.$$

This is the bound we want for n_i . Since $\sum_{i \notin A} N_i \leq D_0 + D_1 - \kappa$ and $n - \kappa \leq \frac{1}{2}D_0 + D_1$ (since there are at most $\frac{1}{2}D_0$ factors with Z-degree 0 not having bidegree (1,0)), we have

$$\sum_{i \notin A} |\Lambda_i| = \sum_{i \notin A} n_i$$

$$\leq \frac{1}{4} D_0 + \frac{1}{2} D_1 + 2\sqrt{2} (D_0 + D_1 - \kappa) ((R_1 + \frac{1}{2})(S_1 + \frac{1}{2})(T_1 + \frac{1}{2}))^{\frac{1}{2}}.$$
(3.1.2)

Hence, by (3.1.1) and (3.1.2),

$$|\Sigma_{1}| \leq \kappa 2((R_{1}+1)(S_{1}+1)(T_{1}+1))^{\frac{1}{2}} + \frac{1}{4}D_{0} + \frac{1}{2}D_{1} + 2\sqrt{2}(D_{0}+D_{1}-\kappa)((R_{1}+\frac{1}{2})(S_{1}+\frac{1}{2})(T_{1}+\frac{1}{2}))^{\frac{1}{2}},$$

$$(3.1.3)$$

and $0 \le \kappa \le D_0$. This right-handside is clearly maximal when $\kappa = 0$. Since $|\Sigma_1| = (R_1+1)(S_1+1)(T_1+1)$ and $(R_1+1)(S_1+1)(T_1+1) > 8(2K+L-2)^2$, inequality (3.1.3) is impossible. Hence dim $\mathcal{Z}_1 = 0$. \square

3.2. Proof of Theorem 3.

We first show that (under the hypotheses of Theorem 3) there exist a vector subspace \mathcal{U} of $\bar{\mathbb{Q}}^2$ of dimension $\delta_0 \geq 0$ and a subgroup \mathcal{T}_m of $\bar{\mathbb{Q}}^*$ of dimension δ_1 with $\delta_0 + \delta_1 \leq 2$ such that

$$\frac{(\delta_0 + \delta_1)!}{\delta_0! \delta_1!} \left| \frac{\Sigma_2 + (\mathcal{U} \times \mathcal{T}_m)}{\mathcal{U} \times \mathcal{T}_m} \right| \le 3(2(K - 1))^{2 - \delta_0} (L - 1)^{1 - \delta_1}. \tag{3.2.1}$$

Proof: Write D_0 for 2(K-1) and D_1 for L-1. Let $\mathcal{H}(E,D_0,D_1)$ be the homogeneous part of p! times the Hilbert-Samuel polynomial of total degree p (= dim \bar{E}). By Lemma 1.2 (i) & (ii), $\mathcal{H}(G,D_0,D_1) = 3D_0^2D_1$ and $((\delta_0 + \delta_1)!/\delta_0!\delta_1!)D_0^{\delta_0}D_1^{\delta_1} \leq \mathcal{H}(\mathcal{U} \times \mathcal{T}_m,D_0,D_1)$. Therefore it suffices to show that

$$\left|\frac{\Sigma_2 + H}{H}\right| \mathcal{H}(H, D_0, D_1) \le \mathcal{H}(G, D_0, D_1)$$

for some $H \neq G$ an algebraic subgroup of G (then $H = \mathcal{U} \times \mathcal{T}_m$). For each $\sigma \in \bar{\mathbb{Q}} \times \bar{\mathbb{Q}} \times \bar{\mathbb{Q}}^*$, let $t_{\sigma}(X,Y,Z) = (X + \pi_1(\sigma), Y + \pi_2(\sigma), Z\pi_3(\sigma))$, where π_1, π_2, π_3 denote the natural projections onto the respective coordinates. We will write $\mathcal{Z} - \sigma$ for $t_{-\sigma}(\mathcal{Z})$ when $\mathcal{Z} \subseteq \bar{\mathbb{Q}} \times \bar{\mathbb{Q}} \times \bar{\mathbb{Q}}^*$.

Let $\mathcal{Z}_0 = V(P)$ denote the set of zeros of P, and $\mathcal{Z}_1 = \bigcap_{\sigma_1 \in \Sigma_1} (\mathcal{Z}_0 - \sigma_1)$, the set of common zeros in G of the polynomials $P \circ t_{\sigma_1}$ ($\sigma_1 \in \Sigma_1$), each of which has bidegree $\leq (D_0, D_1)$. Note that since $\Sigma_1 + \Sigma_2 \subseteq \mathcal{Z}_0$, we

have $\Sigma_2 \subseteq \mathcal{Z}_1$. Let $\mathcal{Z}_2 = \cap_{\sigma_2 \in \Sigma_2} (\mathcal{Z}_1 - \sigma_2) \subseteq \mathcal{Z}_1$. Then $0 \in \mathcal{Z}_2$, and \mathcal{Z}_2 is an algebraic subset. Since dim $\mathcal{Z}_1 = 0$, dim $\mathcal{Z}_2 = \dim \mathcal{Z}_1$. Let \mathcal{V}_0 be a common irreducible component of \mathcal{Z}_1 and \mathcal{Z}_2 of this dimension. So $\mathcal{V}_0 \subseteq \mathcal{Z}_2 = \cap_{\sigma \in \Sigma_2} (\mathcal{Z}_1 - \sigma)$. Thus for all $\tau \in \Sigma_2$, we have $\tau + \mathcal{V}_0 \subseteq \mathcal{Z}_1$. Let $E = \{g \in G : g + \mathcal{V}_0 \subseteq \mathcal{Z}_1\}$; so $\Sigma_2 \subseteq E$. Let $H = \{g \in G : g + \mathcal{V}_0 = \mathcal{V}_0\}$ and $\mathcal{X}_0 = \{g + \mathcal{V}_0 : g \in E\}$. Then \mathcal{V}_0 and each of the elements of \mathcal{X}_0 are algebraic subvarieties of the same dimension as \mathcal{Z}_1 (by Lemma 1.2(iii)). They are also contained in \mathcal{Z}_1 and so \mathcal{X}_0 is finite. Clearly H is a subgroup of G and E is closed under \mathbf{t}_h (translations by h) for all $h \in H$. Hence there is a bijection $E/H \leftrightarrow \mathcal{X}_0$. Thus E is a finite union of translates of H. Now H is an algebraic subset and so an algebraic subgroup of G. Since $\emptyset \neq \mathcal{V}_0 \neq G$, we have $H \neq G$. By Lemma 1.2(v) E is an algebraic subset of G which, like \mathcal{Z}_1 , is defined by polynomials of bidegree $\subseteq (D_0, D_1)$. Since E is a finite union of translates of E, Lemma 1.2(iv) gives

$$\mathcal{H}(E, D_0, D_1) = |E/H|\mathcal{H}(H, D_0, D_1).$$

Since E is defined by polynomials of bidegree $\leq (D_0, D_1)$, we have (by Lemma 1.2(vi)) $\mathcal{H}(E, D_0, D_1) \leq \mathcal{H}(G, D_0, D_1)$. Finally, since $\Sigma_2 \subseteq E$ we have

$$|(\Sigma_2 + H)/H| \le |E/H|.$$

This establishes the claim. \square

Now $H = \mathcal{U} \times \bar{\mathbb{Q}}^*$ (respectively $\mathcal{U} \times \mathcal{T}_m$) = $\{g \in G : \mathcal{V}_0 + g = \mathcal{V}_0\}$ as m = 0 (or $m \neq 0$) for some vector subspace \mathcal{U} of $\bar{\mathbb{Q}}^2$ of dimension δ_0 , where \mathcal{V}_0 is a common irreducible component of \mathcal{Z}_1 and \mathcal{Z}_2 of dimension 0.

If $\mathcal{U} = \{\mathbf{0}\}$ and m = 0, and $\{(x_0, y_0, z_0)\} = \mathcal{V}_0$, then $(x_0, y_0, z) \in \mathcal{V}_0$ for all $z \in \mathbb{Q}^*$. So dim $\mathcal{V}_0 \geq 1$, a contradiction.

If $\mathcal{U} \neq \{\mathbf{0}\}$, let $(\mu_0, \nu_0) \in \mathcal{U} \setminus \{\mathbf{0}\}$ and $\{(x_0, y_0, z_0)\} = \mathcal{V}_0$. Then $((x_0, y_0) + \bar{\mathbb{Q}}(\mu_0, \nu_0), z_0) \subseteq \mathcal{V}_0$. Thus dim $\mathcal{V}_0 > 0$, a contradiction. Hence $H = \{0\} \times \mathcal{T}_m$ with $m \neq 0$.

Now if $(x_0, y_0, z_0) \in \mathcal{V}_0$, then $(x_0, y_0, z_0 e^{2\pi i/m}) \in \mathcal{V}_0$. Consequently, m = 1, and H is the trivial group. Thus (3.2.1) becomes $(R_2 + 1)(S_2 + 1)$ $(T_2 + 1) = |\Sigma_2| \leq 3(2(K - 1))^2(L - 1)$. \square

S4. Numerical Constants.

In this section, we follow standard procedures to obtain numerical constants that satisfy the conditions of both Theorem 3 and Proposition 2.1.

Let c_1, c_2, c_3 & c_4 be real numbers greater than 1; and suppose that $c_1 \geq 2c_2$. Let

$$K = \lceil c_1 B \log a_1 \log a_2 \log a_3 \rceil$$
 and $L = \lceil c_2 B \rceil$.

Let

$$b' = \left(\frac{b_2}{\log a_1} + \frac{b_1}{\log a_2}\right) \left(\frac{b_2}{\log a_3} + \frac{b_3}{\log a_2}\right)$$

and assume that $(B^0 \ge)B \ge \max\{B_0, \log b'\}$. We will assume that $B_0 \ge 10$. Let

$$R = [c_4 B \log a_2 \log a_3]$$

$$S = [c_4 B \log a_3 \log a_1]$$

$$T = [c_4 B \log a_1 \log a_2].$$

Note that $\{b_1, b_2, b_3\}$ is (R, S, T)-linearly dependent over \mathbb{Z} if and only if it is (c_4, B) -linearly dependent over \mathbb{Z} (with respect to (a_1, a_2, a_3)).

Let

$$R_1 = [c_3 B^{2/3} \log a_2 \log a_3],$$
 $S_1 = [c_3 B^{2/3} \log a_3 \log a_1],$ and $T_1 = [c_3 B^{2/3} \log a_1 \log a_2],$

Let
$$R_2 = R - 1 - R_1$$
, $S_2 = S - 1 - S_1$ and $T_2 = T - 1 - T_1$.

PROPOSITION 4.1. With the above definitions, condition (2A) holds as do the hypotheses of Theorem 3 provided that

$$21,000 \le c_1$$

$$3 \le c_2 \le 8$$

$$c_2 < 0.0002c_1$$

$$c_3 = 32.007^{1/3}c_1^{2/3}$$

$$c_4 = (12c_1^2c_2)^{1/3} + \frac{1}{B_0} + \frac{32.007^{1/3}c_1^{2/3}}{B_0^{1/3}},$$

and

$$c_2 \left(1 - \frac{3}{2} \left(\frac{\rho + 1}{\log \rho} \right) \left(12 \frac{c_2}{c_1} \right)^{1/3} \left(1 + \left(\frac{32.007}{12c_2 B_0} \right)^{1/3} \right) \right)$$

$$> \frac{2}{\log \rho} + \frac{3}{2} \left(\frac{\rho + 1}{\log \rho} \right) \left(\frac{c_2}{c_1 B_0} \right) + \frac{1.2}{B^0} - \frac{4 \log 2}{B^0 \log \rho} + .00005$$

where $B_0 \ge 10$ and $e \le \rho \le 9$, and the two terms involving B^0 are omitted if B^0 is not known.

Proof: We first show that $b \leq b'$ (provided that $c_1 \geq e^{3/2}c_4$) and hence $\log b \leq B$.

By definition,

$$b \le c_4^2 B^2 \Big(\prod_{j=1}^3 \log a_j\Big)^2 b' / \Big(\prod_{k=1}^{K-1} k!\Big)^{4/K(K-1)}.$$

Hence it suffices to prove that

$$c_4^2 B^2 \Big(\prod_{j=1}^3 \log a_j\Big)^2 \le \Big(\prod_{k=1}^{K-1} k!\Big)^{4/K(K-1)}.$$

By Lemma 1.6, the right hand side exceeds K^2/e^3 ; so the desired inequality certainly holds if $c_4^2 \le c_1^2/e^3$.

That the hypotheses of Theorem 3 hold (under suitable assumptions on the constants $c_1
ldots c_4$ for these values of $R_1, S_1, T_1, R_2, S_2, T_2, K$, and L-see below) follows by grubby school arithmetic. Specifically, $K \ge 2L$ since $c_1 \ge 2c_2$. Moreover, since $c_3 > 1$ and $\log a_j \ge 1$ (j = 1, 2, 3), we have that conditions (3.1) and (3.2) both hold provided that

$$4B^{4/3} > 1 + B^{2/3}$$
.

Since $B \ge B_0 \ge 10$, this is obviously the case.

Inequality (3.4) certainly holds provided that

$$c_3^3 > 8(2c_1 + c_2)^2 \tag{4.1}$$

Now $c_2/c_1 < .0002$, so we merely require that $c_3 > 2(2.0002)^{2/3}c_1^{2/3}$.

So we take

$$c_3 = (32.007)^{1/3} c_1^{2/3}. (4.2)$$

Note also that $c_3 > 3$, so $R_1, S_1, T_1 \geq 3$.

Next we want $R_2 \geq 3$. For this we need only insist that $R \geq R_1 + 4$. Since $\log a_j \geq 1$ (j = 1, 2, 3) and $B \geq B_0$, it suffices that

$$c_4 \ge \frac{32.007^{1/3}c_1^{2/3}}{B_0^{1/3}} + \frac{5}{B_0}. (4.3)$$

Similarly $S_2 \geq 3$ and $T_2 \geq 3$, assuming (4.3).

Finally, we note that condition (3.3) holds provided that

$$\left(c_4 - \frac{1}{B_0} - \frac{32.007^{1/3} c_1^{2/3}}{B_0^{1/3}}\right)^3 \ge 12c_1^2 c_2.$$
(4.4)

An easy verification shows that

$$c_4 = (12c_1^2c_2)^{1/3} + \frac{1}{B_0} + \frac{32.007^{1/3}c_1^{2/3}}{B_0^{1/3}}$$
(4.5)

satisfies both conditions (4.3) & (4.4), since $B_0 \ge 10$ and $c_1, c_2 \ge 1$.

Moreover, $e^{3/2}c_4 \le c_1$ if (4.5) holds, since $c_2 \le 8$, and $B_0 \ge 10$, and $c_1 \ge 21,000$.

Consequently, with the value of c_4 given by (4.5) (in terms of c_1, c_2, B_0), and the indicated values for R_1, R_2 etc., we are guaranteed full row rank and hence a $K^2L \times K^2L$ submatrix of determinant $\Delta \neq 0$ (Theorem 3). Now to get that $|\Lambda'| > 1/\rho^{KL}$, we need to satisfy inequality (2A) of Section 2.

To satisfy this inequality, if we assume that $K \ge 1,000$ (which occurs if $c_1 B_0 \ge 1,000$ since $\log a_j \ge 1$ (j = 1,2,3)), it suffices that

$$\begin{split} \frac{c_1}{2} \left(c_2 - \frac{1}{B} \right) \log \rho + \frac{2c_1}{B} \left(1 - \frac{1}{c_1 B} \right) \log 2 \\ > \left(\frac{0.1 \log \rho}{B} + 1 \right) c_1 + \frac{3}{4} c_2 c_4 (\rho + 1) \\ + \frac{2}{B^2} \log \left(\left(1 + \frac{1}{c_1 B} \right)^2 c_1^2 c_2 B^3 \right) + \frac{4}{e B^2} \end{split}$$

since $B \ge \log b$ and $\frac{\log t}{t} \le \frac{1}{\epsilon}$ if $t \ge 1$. That is

$$c_{2} > \frac{1.2}{B} + 2\left(\frac{1}{\log \rho} + \frac{3}{4}\frac{c_{2}c_{4}}{c_{1}}\left(\frac{\rho + 1}{\log \rho}\right)\right) + \frac{4\log\left\{\left(1 + \frac{1}{c_{1}B}\right)^{2}c_{1}^{2}c_{2}B^{3}\right\}}{c_{1}B^{2}\log \rho} + \frac{8}{ec_{1}B^{2}\log \rho} - \frac{4}{B}\left(1 - \frac{1}{c_{1}B}\right)\frac{\log 2}{\log \rho}.$$

$$(4.6)$$

We claim that

$$\frac{4 \log 2}{B \log \rho} > \frac{1.2}{B} + \frac{4}{c_1 B^2} \frac{\log 2}{\log \rho} + \frac{8}{e c_1 B^2 \log \rho} + \frac{4 \log \left\{ \left(1 + \frac{1}{c_1 B}\right)^2 c_1^2 c_2 B^3 \right\}}{c_1 B^2 \log \rho}$$

if $B \ge 10$, $c_1 \ge 20,000$, $c_2 \le 8$ and $e \le \rho \le 9$. For the right hand side of the above is at most

$$\frac{1}{B} \left(1.2 + \frac{4 \log 2}{2 \cdot 10^5} + \frac{3}{2 \cdot 10^5} + 4 \left(\frac{10}{2 \cdot 10^5} + \frac{2 \log 20,000}{2 \cdot 10^5} + \frac{\log 8}{2 \cdot 10^5} + \frac{3 \log 10}{2 \cdot 10^5}\right)\right)$$

i.e., at most $\frac{1.21}{B}$. However, $\frac{4 \log 2}{B \log \rho} \ge \frac{4 \log 2}{B \log 9} \ge \frac{1.26}{B}$. This establishes the claim. Hence (4.6) certainly holds provided that

$$c_{2} > 2\left(\frac{1}{\log \rho} + \frac{3}{4} \frac{c_{2}c_{4}}{c_{1}} \left(\frac{\rho + 1}{\log \rho}\right)\right) + \frac{-4\log 2}{B^{0}\log \rho} + \frac{1.2}{B^{0}} + \frac{4\log 2}{c_{1}(B^{0})^{2}\log \rho} + \frac{8}{ec_{1}(B^{0})^{2}\log \rho} + \frac{4\log \left\{\left(1 + \frac{1}{c_{1}B^{0}}\right)^{2} c_{1}^{2}c_{2}(B^{0})^{3}\right\}}{c_{1}(B^{0})^{2}\log \rho}$$

$$(4.7)$$

where $B^0 \geq B$; in the case that no B^0 is given, the three terms with B^0 in them are omitted. Since $c_1 > 2 \times 10^4$ and $B_0 \geq B_0 \geq 10$, the last three terms on the right hand side of (4.7) add up to at most .00005. So substituting for the value of c_4 from (4.5) in (4.7) we see that inequality (4.7) holds if

$$\begin{split} c_2 > & 2 \left(\frac{1}{\log \rho} + \frac{3}{4} \left\{ \frac{12^{1/3} c_2^{4/3}}{c_1^{1/3}} + \frac{c_2}{c_1 B_0} + \frac{32.007^{1/3} c_2}{(c_1 B_0)^{1/3}} \right\} \left(\frac{\rho + 1}{\log \rho} \right) \right) \\ & + \frac{1.2}{B^0} - \frac{4 \log 2}{B^0 \log \rho} + .00005, \end{split}$$

where the two terms involving B^0 are omitted if no B^0 is known. If we let $c_1 = c_2/x$ (with x a positive real number less than 0.0002), then this condition becomes

$$\begin{aligned} c_2 > & 2 \left(\frac{1}{\log \rho} + \frac{3}{4} \left\{ (12x)^{1/3} c_2 + \frac{x}{B_0} + \frac{32.007^{1/3} x^{1/3} c_2^{2/3}}{B_0^{1/3}} \right\} \left(\frac{\rho + 1}{\log \rho} \right) \right) + \\ & + \frac{1.2}{B^0} - \frac{4 \log 2}{B^0 \log \rho} + .00005 \end{aligned}$$

(with the B^0 terms omitted if no B^0 is known). This is certainly true if

$$c_{2} \left(1 - \frac{3}{2} \left(\frac{\rho + 1}{\log \rho} \right) (12x)^{1/3} \left(1 + \left(\frac{32.007}{12c_{2}B_{0}} \right)^{1/3} \right) \right)$$

$$> \frac{2}{\log \rho} + \frac{3}{2} \left(\frac{\rho + 1}{\log \rho} \right) \left(\frac{x}{B_{0}} \right) + \frac{1.2}{B^{0}} - \frac{4 \log 2}{B^{0} \log \rho} + .00005$$

$$(4.8)$$

(with the B^0 terms omitted if B^0 is not known). This establishes Proposition 4.1. \square

Subject to the above constraint (4.8), we wish to minimise the constant $C = c_1 c_2 \log \rho = \frac{c_2^2}{x} \log \rho$ where $e \le \rho \le 9$. Tables (obtained by computer)

are provided in Section 6 for various values of (B_0, B^0) and B_0 . Substituting 5 for ρ yields:

$$c_2\left(1 - 12.803(x^{1/3})\left(1 + \left(\frac{32.007}{12c_2B_0}\right)^{1/3}\right)\right) > 1.243 + \frac{5.593x}{B_0} - \frac{1}{B_0} + .00005.$$

For the case that B_0 is extremely large, we have only the constraint

$$c_2(1 - 12.803x^{1/3}) > 1.243.$$

The minimum for C occurs when x = .000103, $c_2 = 3.109$, $c_1 = 30,182$, and $c_1c_2\log\rho < 1.51 \times 10^5$.

S5. A Lower Bound for $|\Lambda|$.

We have shown under the above constraints that $\Lambda' > 1/\rho KL$. Since

$$KL \le \left(c_1 B\left(\prod_{j=1}^3 \log a_j\right) + 1\right)(c_2 B) \le c_1 c_2 B^2 \left(\prod_{j=1}^3 \log a_j\right) \left(1 + \frac{1}{c_1 B}\right),$$

it follows that

$$\Lambda' > \exp\Big(-\Big(1 + \frac{1}{c_1 B_0}\Big)(c_1 c_2 \log \rho)\Big(\prod_{j=1}^3 \log a_j\Big)B^2\Big).$$

We now deduce that

$$|\Lambda| > \exp\Big(-(c_1c_2\log\rho + \delta)\Big(\prod_{j=1}^3\log a_j\Big)B^2\Big)$$

where δ is small and defined below.

Write $A = B^2 \left(\prod_{j=1}^3 \log a_j \right)$, $W_1 = LR/2b_1$, $W_2 = LS/2b_2$, $W_3 = LT/2b_3$. Recall that

$$\Lambda' = |\Lambda| \max \left\{ \frac{LRe^{LR|\Lambda|/2b_1}}{2b_1} , \frac{LSe^{LS|\Lambda|/2b_2}}{2b_2} , \frac{LTe^{LT|\Lambda|/2b_3}}{2b_3} \right\}$$

and note that

$$R \le \frac{c_4 B\left(\prod_{j=1}^3 \log a_j\right)}{\log a_1}$$

(similarly for S and T replacing $\log a_1$ by $\log a_2$ and $\log a_3$, respectively). If $|\Lambda| > (1 + \log 2)/W_1$, then

$$|\Lambda| > \frac{2b_1}{LR}(1 + \log 2) > \frac{2(1 + \log 2)(b_1 \log a_1)}{c_2 c_4 A} > \frac{1}{c_2 c_4 A}.$$

Hence, to establish that $|\Lambda| \geq \exp(-(c_1c_2\log\rho)A)$, it is enough to prove that

$$(c_1c_2\log\rho)A\geq\log(c_2c_4A).$$

Since $c_1 \ge e^{3/2}c_4 \ge c_4$ and ρ , $c_1c_2A \ge e$, we indeed have

$$(c_1c_2A)\log\rho\geq\log(c_1c_2A)\geq\log(c_2c_4A),$$

as required. Similarly, if $|\Lambda| > (1 + \log 2)/W_j$ (for j = 2 or j = 3), we get that $|\Lambda| > \exp(-(c_1c_2\log\rho)A)$. So assume that $|\Lambda| \le \frac{1+\log 2}{W_j}$ (j = 1, 2, 3). So $W_j|\Lambda| \le 1 + \log 2$ (j = 1, 2, 3). Now

$$\begin{split} \log(W_j e^{|\Lambda|W_j}) &= \log W_j + |\Lambda|W_j \\ &\leq \log W_j + 1 + \log 2 \\ &\leq \log L + \log(\max\{R, S, T\}) + 1. \end{split}$$

But $eLR \leq \frac{ec_2c_4A}{\log a_1}$. So, by the definition of c_4 (see (4.7)), and using $c_1 \geq 100, c_2 \geq 3, B_0 \geq 3$, we get

$$\log(eLR) \le \log(e12^{1/3}c_2^{4/3}c_1^{2/3}A) + \log 1.672$$

$$\le \log A + \left(\frac{4\log c_2 + 2\log c_1}{3}\right) + 2.35.$$

The same upper bound holds for $\log(eLS)$ and $\log(eLT)$. By definition, $-\left(1+\frac{1}{c_1B_0}\right)c_1c_2(\log\rho)A \leq \log|\Lambda'| = \log|\Lambda| + \log(W_je^{W_j|\Lambda|})$ for some $j \in \{1,2,3\}$. Hence

$$\log |\Lambda| \ge -\left(\left(1 + \frac{1}{c_1 B_0}\right) c_1 c_2 \log \rho + \frac{2.35 + \log A}{A} + \frac{4 \log c_2 + 2 \log c_1}{3A}\right) A. \quad (5.1)$$

But $(\log A)/A$ decreases as A increases. Since $A \geq B_0^2$, (5.1) gives

$$\log |\Lambda| \ge -\left(c_1c_2\log \rho + \frac{c_2\log \rho}{B_0} + \frac{2.35 + 2\log B_0}{B_0^2} + \frac{4\log c_2 + 2\log c_1}{3B_0^2}\right)A.$$

If $\delta = \frac{c_2 \log \rho}{B_0} + \frac{2.35 + 2 \log B_0 + (4/3) \log c_2 + (2/3) \log c_1}{B_0^2}$, then

$$\log |\Lambda| \ge -(c_1 c_2 \log \rho + \delta) \Big(\prod_{j=1}^3 \log a_j \Big) B^2.$$

In the limiting case, $\delta = 0$, of course. A table for various values of B_0 (obtained using a computer) is provided in the next section.

S6. Tables.

TABLE 1

B_0	B^0	$oldsymbol{x}$	c_1	c_2	ρ	C4	δ	$\mathcal C$
10	20	4.62987×10^{-5}	78,404	3.63	4.41	9145.22	.703	422,321
20	30	5.35267×10^{-5}	66,322	3.55	4.51	7638.91	.312	354,648
30	40	5.73291×10^{-5}	61,051	3.50	4.56	6973.79	.198	324,219
40	50	6.03653×10^{-5}	57,649	3.48	4.59	6562.91	.145	305,719
50	60	6.24695×10^{-5}	55,387	3.46	4.61	6283.71	.114	292,868
60	70	6.40322×10^{-5}	53,723	3.44	4.63	6075.35	.094	283,228
70	80	6.55995×10^{-5}	52,287	3.43	4.65	5905.11	.080	275,629
80	90	6.64212×10^{-5}	51,339	3.41	4.66	5777.90	.069	269,429
90	100	6.79161×10^{-5}	50,209	3.41	4.68	5654.19	.061	264,232
100	200	6.85304×10^{-5}	49,613	3.40	4.69	5571.79	.055	260,690
200	300	7.42695×10^{-5}	45,106	3.35	4.74	5028.71	.027	235,125
300	400	7.71268×10^{-5}	43,046	3.32	4.77	4777.52	.018	223,279
400	500	7.90912×10^{-5}	41,724	3.30	4.80	4618.75	.014	215,981
500	1000	8.04735×10^{-5}	40,883	3.29	4.80	4515.73	.011	210,987
1000	10^{4}	8.46621×10^{-5}	38,506	3.26	4.83	4233.01	6×10^{-3}	197,690
10^{4}	10^{5}	9.42087×10^{-5}	33,861	3.19	4.90	3681.67	6×10^{-4}	171,664
10^{5}	10^{6}	9.87275×10^{-5}	31,906	3.15	4.93	3444.89	6×10^{-5}	160,338
10^{6}	10^{9}	1.01451×10^{-4}	30,951	3.14	4.94	3336.16	6×10^{-6}	155,242

TABLE 2

B_0	$oldsymbol{x}$	c_1	c_2	ρ	C4	δ	$\mathcal C$
10	4.58044×10^{-5}	79,905	3.66	4.51	9279.51	.715	440,521
20	5.31701×10^{-5}	67,143	3.57	4.58	7712.64	.316	364,752
30	5.71865×10^{-5}	61,553	3.52	4.61	7022.27	.200	331,116
40	5.98627×10^{-5}	58,133	3.48	4.65	6599.59	.146	310,913
50	6.21207×10^{-5}	55,698	3.46	4.67	6307.21	.115	297,005
60	6.40811×10^{-5}	53,838	3.45	4.68	6088.78	.095	286,654
70	6.55650×10^{-5}	52,467	3.44	4.68	5923.35	.080	278,545
80	6.65577×10^{-5}	51,384	3.42	4.70	5785.93	.070	271,958
90	6.75328×10^{-5}	50,494	3.41	4.70	5675.57	.062	266,466
100	6.84311×10^{-5}	49,685	3.40	4.71	5577.18	.055	261,787
200	7.42613×10^{-5}	45,111	3.35	4.76	5029.09	.027	235,788
300	7.70677×10^{-5}	43,079	3.32	4.78	4779.96	.018	223,750
400	7.92264×10^{-5}	41,779	3.31	4.78	4626.95	.014	216,344
500	8.07873×10^{-5}	40,848	3.30	4.79	4517.24	.011	211,166
1000	8.46555×10^{-5}	38,509	3.26	4.83	4233.23	.006	197,705
10^{4}	9.42087×10^{-5}	33,861	3.19	4.90	3681.67	6×10^{-4}	171,664
10^{5}	9.87275×10^{-5}	31,906	3.15	4.93	3444.89	6×10^{-5}	160,338
10^{6}	1.01451×10^{-4}	30,951	3.14	4.94	3336.16	6×10^{-6}	155,242

We are most grateful to our graduate student, Timothy W. O'Neil, for providing us with these tables.

REFERENCES

- [1] A. Baker, The theory of linear forms in logarithms, in Transcendence Theory: Advances and Applications,, Academic Press, London (1977), 1-27.
- [2] A. Baker and G. Wüstholz, Logarithmic forms and group varieties, J. reine angew. Math. 442 (1993), 19-62.
- [3] J. Blass, A. M. W. Glass, D. K. Manski, D. B. Meronk, and R. P. Steiner, Constants for lower bounds for linear forms in the logarithms of algebraic numbers I, II, Acta Arith. 55 (1990), 1-22, corrigendum, ibid 65 (1993).
- [4] D. W. Brownawell and D. W. Masser, Multiplicity estimates for analytic functions II, Duke Math. Journal 47 (1980), 273-295.
- [5] L. Denis, Lemmes des zéros et intersections., Approximations diophantiennes et nombres transcendants Luminy (1990), éd. P. Philippon, de Gruyter (1992), 99– 104.
- [6] Dong Ping Ping, Minorations de combinaisons linéaires de logarithmes de nombres algébriques p-adiques, C. R. Acad. Sci. Paris, Sér. I 315 (1992), 103-106.
- [7] A. O. Gel'fond, Transcendental and algebraic numbers, (Russian). English trans.: Dover, New York (1960).
- [8] A. M. W. Glass, D. B. Meronk, T. Okada, and R. Steiner, A small contribution to Catalan's equation, J. Number Theory 47 (1994), 131-137.
- [9] R. Hartshorne, Algebraic Geometry, Graduate Texts in Math. 52, Springer Verlag, Heidelberg, 1977.
- [10] E. Kunz, Introduction to Commutative Algebra and Algebraic Geometry (German), English trans.: Birkhaüser, Boston (1985).
- [11] M. Laurent, Sur quelques résultats récents de transcendance, Astérisque 198-200 (1991), 209-230.
- [12] M. Laurent, Hauteurs de matrices d'interpolation, Approximations diophantiennes et nombres transcendants, Luminy (1990), éd. P. Philippon, de Gruyter (1992), 215-238.
- [13] M. Laurent, Linear forms in two logarithms and interpolation determinants, Acta Arith. LXVI (1994), 181-199, or Appendix to [33].
- [14] M. Laurent, M. Mignotte, and Y. V. Nesterenko, Formes linéaires en deux logarithmes et determinants d'interpolation, J. Number Theory 55 (1995), 285-321.
- [15] D. W. Masser, On polynomials and exponential polynomials in several variables, Inv. Math. 63 (1981), 81-95.
- [16] D. W. Masser and G. Wüstholz, Zero estimates on group varieties I, Inv. Math. 64 (1981), 489-516.
- [17] D. W. Masser and G. Wüstholz, Zero estimates on group varieties II, Inv. Math. 80 (1985), 233-267.
- [18] D. W. Masser and G. Wüstholz, Fields of large transcendence degree, Inv. Math. 72 (1983), 407-464.

- [19] M. Mignotte and M. Waldschmidt, Linear forms in two logarithms and Schneider's method III, Ann. Fac. Sci. Toulouse 97 (1989), 43-75.
- [20] Y. V. Nesterenko, Estimates for the orders of zeros of functions of a certain class and their applications in the theory of transcendental numbers, Math. USSR Izv. 11 (1977), 239-270.
- [21] P. Philippon, Lemmes de zéros dans les groupes algébriques commutatifs, Bull. Soc. Math. France 114 (1986), 355-383, et 115 (1987), 397-398.
- [22] P. Philippon and M. Waldschmidt, Lower bounds for linear forms in logarithms, Chapter 18 of New Advances in Transcendence Theory, Proc. Conf. Durham (1986), ed. A. Baker, Cambridge Univ. Press, Cambridge (1988), 280-312.
- [23] P. Philippon and M. Waldschmidt, Formes linéaires de logarithmes elliptiques et mesures de transcendance, Théorie des nombres, Proc. Conf. Québec City 1987, de Gruyter, Berlin, (1989), 798-805.
- [24] A. J. van der Poorten, Linear forms in logarithms in the p-adic case, Transcendence Theory: Advances and Applications, Academic Press, London (1977), 29-57.
- [25] E. Reyssat, Approximation algébrique de nombres liés aux fonctions elliptiques et exponentielle, Bull. Soc. Math. France 108 (1980), 47-79.
- [26] T. Shorey and R. Tijdeman, Exponential Diophantine Equations, Cambridge Tracts in Mathematics, No. 87, Cambridge Univ. Press, Cambridge (1986).
- [27] D. Sinnou, Minorations de formes linéaires de logarithmes elliptiques., Publ. Math. de l'Univ. Pierre et Marie Curie, No. 106, Problèmes diophantiennes 1991-1992, exposé 3.
- [28] N. Tzanakis and B. M. M. de Weger, On the practical solution of the Thue equation, J. Number Theory 31 (1989), 99-132.
- [29] M. Waldschmidt, A lower bound for linear forms in logarithms, Acta Arith. 37 (1980), 257-283.
- [30] M. Waldschmidt, Nouvelles méthodes pour minorer des combinaisons linéaires de logarithmes de nombres algébriques, Sém. Th. Nombres Bordeaux 3 (1991), 129– 185.
- [31] M. Waldschmidt, Nouvelles méthodes pour minorer des combinaisons linéaires de logarithmes de nombres algébriques II, Problèmes Diophantiens 1989-1990, Publ. Univ. Pierre et Marie Curie (Paris VI) 93 (1991), 1-36.
- [32] M. Waldschmidt, Minorations de combinaisons linéaires de logarithmes de nombres algébriques, Canadian J. Math 45 (1993), 176-224.
- [33] M. Waldschmidt, Linear independence of logarithms of algebraic numbers, Matscience Lecture Notes, Madras (1992).
- [34] G. Wüstholz, Recent progress in transcendence theory, Springer Lecture Notes in Math., Springer Verlag, Heidelberg, 1068 (1984), 280-296.
- [35] G. Wüstholz, A new approach to Baker's theorem on linear forms in logarithms I, Lecture Notes in Math., Springer Verlag, Heidelberg 1290 (1987), 189-202.
- [36] G. Wüstholz, A new approach to Baker's theorem on linear forms in logarithms II, Lecture Notes in Math., Springer Verlag, Heidelberg 1290 (1987), 203-211.

- [37] G. Wüstholz, A new approach to Baker's theorem on linear forms in logarithms, III, Chapter 25 of New Advances in Transcendence Theory, Proc. Conf. Durham (1986), ed. A. Baker, Cambridge Univ. Press, Cambridge (1988), 399-410.
- [38] Kunrui Yu., Linear forms in p-adic logarithms I., Acta Arith. 53 (1989), 107-186.
- [39] Kunrui Yu, Linear forms in p-adic logarithms II, Compositio Math. 74 (1990), 15-113.

Bowling Green State University Ohio 43403, USA e-mail: cbennet@bgnet.bgsu.edu