A sharpening of the bounds for linear forms in logarithms III

by

A. Baker (Cambridge)

In memory of Professors
Yu. V. Linnik and L.J. Mordell

1. Introduction. Let $a_1, \ldots, a_n$ be non-zero algebraic numbers with
degrees at most $d$ and suppose that the height of $a_i$ is at most $A_j$ ($\geq 4$).
Further let $b_1, \ldots, b_n$ be rational integers with absolute values at most
$B$ ($\geq 4$), and let

$$A = b_1 \log a_1 + \ldots + b_n \log a_n,$$

where the logarithms are assumed to have their principal values. We
prove:

**Theorem.** If $A \neq 0$ then $|A| > B^{-C|\log \Omega|}$, where

$$\Omega = \log A_1 \ldots \log A_n,$$

and $C$ is an effectively computable number depending only on $n$ and $d$.

The theorem improves upon the recent work of Stark [7] which
itself refined several earlier results in this field. It does not, however,
include the theorems of the first two memoirs of this series [3], [4], nor
indeed those of [5] or [7] wherein, in particular, the linear form $A$ pos-
sesses algebraic and not merely rational integer coefficients; and it would
be of much interest to eliminate $\log \Omega$ and to generalize $A$ so as to incor-
porate these results.

The estimate of [7] was recently utilized by Stark [8] to strengthen
the bound for the size of the solutions of the Diophantine equation $y^8 = x^8 + k$ obtained in [2], and moreover a special version was employed
by Shorey [6] to sharpen certain theorems concerning the distribution
of the primes; it seems likely that these results will admit still further
improvement in the light of the work here(1).

(1) Added in proof. The work of this series has recently been applied by
R. Tijdeman to show that the famous conjecture of Catalan is, in principle, decidable.
2. Main theory. We signify by \(a_1, \ldots, a_n\), where \(n \geq 2\), algebraic numbers as in §1, and we denote by \(K\) the field which they generate over the rationals; further we denote by \(a_1, a_2, \ldots\) numbers greater than 1 that can be specified in terms of \(n\) and \(d\) only. We suppose that there exist rational integers \(b_1, \ldots, b_n\), with \(b_a \neq 0\), having absolute values at most \(B\), such that \(|A| < B^{c+\text{const}}\), where \(O = O(n, d)\) is assumed sufficiently large. We proceed to prove that then, for any \(c_1\), there exists \(c_2\) and a prime \(p\) with \(c_1 < p < c_2\) such that \(K[a_1p^{-1/2}, \ldots, a_np^{-1/2}]\) is not an extension of \(K\) of degree \(p^n\); we shall show in §4 that this suffices to establish the theorem.

The notation of [3] will be adopted without change, except that we now define \(L_j = [B^{-1+\text{const}}} \log \log \log A_j \quad (0 \leq j \leq n)\), where \(A_0 = \Omega\).

It is then readily verified that Lemmas 5, 6 and 7 of [3] are valid with \(L_j\) replaced by \(\log A_j\) and \(L = L_0 \log \Omega\); also one easily checks that Lemma 8 of [3] holds with the range of \(m_0, \ldots, m_{n-1}\) extended to cover all non-negative integers with

\[
m_0 + \cdots + m_{n-1} < c_1^{-2} k \log \log \Omega
\]

for some \(c_1\) as above. We now take \(g\) to be a prime \(p\) between \(B^{1/2}\) and \(2B^{1/2}\) exclusive and we assume that \(K[a_1p^{-1/2}, \ldots, a_np^{-1/2}]\) is an extension of \(K\) of degree \(p^n\). Then, for any integers \(\lambda_1, \ldots, \lambda_n\) between 0 and \(p-1\) inclusive,

(2) [of [3]] holds with \(L\) replaced by \(l/p\) and with the \(p(\lambda_1, \ldots, \lambda_n)\) other than those such that \(\lambda_j = \lambda_j (\mod p)\) for all \(j\), equated to 0. This gives

\[
\sum_{\lambda_1=0}^{L_1-1} \cdots \sum_{\lambda_n=0}^{L_n-1} p(\lambda_1, \lambda_2, \ldots, \lambda_n) A(l/p) a_1^{\lambda_1} \cdots a_n^{\lambda_n} = 0
\]

for all \(l\) with \(1 \leq l \leq kp, (l, p) = 1\), where

\[
\Lambda_j = L_j - L_0, \quad \lambda_j = [L_j - \lambda_j] / p \quad (1 \leq j \leq n), \quad \mu_j = \lambda_j + p\lambda_j,
\]

and \(A\) is defined like \(\Lambda\) but with \(\lambda_j\) replaced by \(\mu_j\). In fact (2) holds with \(A'\) replaced by \(A\); for clearly \(A(b_0\mu_0 - b_1\mu_1)\) is a polynomial in \(\gamma_0\), \(\gamma_1, \ldots, \gamma_n\) with coefficients independent of the \(\lambda\)'s and with degree \(m_0\), whence arguing by induction with respect to \(m_0 + \cdots + m_{n-1}\) as in the proof of Lemma 7, we infer that (2) remains valid if the product over \(r\) in \(A'\) is replaced by \(\gamma_0^{\lambda_0} \cdots \gamma_n^{\lambda_n}\), and the required result then follows on taking linear combinations. Thus we have shown that from the validity of (2) of [3] for \(1 \leq l \leq k\) and \(m_0 + \cdots + m_{n-1} \leq k \log \log \Omega\) we obtain

\[
\sum_{\lambda_1=0}^{L_1-1} \cdots \sum_{\lambda_n=0}^{L_n-1} p'(\lambda_1, \ldots, \lambda_n) A(l/p) a_1^{\lambda_1} \cdots a_n^{\lambda_n} = 0
\]

for all \(l\) with \(1 \leq l \leq kp, (l, p) = 1\), and all \(m_0, \ldots, m_{n-1}\) satisfying (1), where the \(p'(\lambda_1, \ldots, \lambda_n)\) are integers given by some subset of the \(p(\lambda_1, \ldots, \ldots, \lambda_n)\), which, for a suitable choice of \(\lambda_1, \ldots, \lambda_n\), are not all 0.

We shall demonstrate in the next section that the argument can be repeated and one obtains, for each positive integer \(J\), an equation as above with \(L_J \leq L_{[p^{-1}\log \log A]} (1 \leq j \leq n)\) and with \(l/p\) replaced by \(l/p^J\), valid for all \(l\) with \(1 \leq l \leq kp, (l, p) = 1\), and all \(m_0, \ldots, m_{n-1}\) satisfying (1), with \(c_1\) replaced by \(p^{-J}\). The process is continued until \(L_J = 0 (1 \leq j \leq n)\), which occurs for some \(J\) such that \(p^J \leq k \log \log \Omega\). This completes the argument thus far. We shall now establish the assertion in the beginning.

3. Inductive argument. We require the proposition that for each integer \(J = 0, 1, \ldots, p^J \leq k \log \log \Omega\) there exist integers \(m_0, \ldots, m_{n-1}\) satisfying (1), not all 0, with absolute values at most \(O^{c\log \log \log \log \Omega}\), such that

\[
\sum_{l=0}^{L_1-1} \cdots \sum_{l=0}^{L_n-1} p^{(J)}(\lambda_1, \ldots, \lambda_n) A(l/p^J) a_1^{\lambda_1} \cdots a_n^{\lambda_n} = 0
\]

for all integers \(l\) with \(1 \leq l \leq kp, (l, p) = 1\), and all non-negative integers \(m_0, \ldots, m_{n-1}\), with

\[
m_0 + \cdots + m_{n-1} \leq p^{-J} k \log \log \Omega,
\]

where \(L_j^J = L_j, L_0^J = L_0\) and \(L_j^J = L_j / p^J (1 \leq j \leq n)\) for all \(J\).

We assert that for \(J = 0\) by Lemma 1 of [3]. We assume the result for \(J = K\) and proceed to prove the validity for \(J = K + 1\). For any non-negative integers \(m_0, \ldots, m_{n-1}\), satisfying (4) with \(J = K\) we write

\[
f(x) = \sum_{\lambda_1=0}^{L_1^K} \cdots \sum_{\lambda_n=0}^{L_n^K} p^{(K)}(\lambda_1, \ldots, \lambda_n) A(x/p^K) a_1^{\lambda_1} \cdots a_n^{\lambda_n}.
\]

It is then readily verified that

\[
|f(x)| \leq O^{c\log \log \log \log \log \log \Omega} \cdot \|e^{K\log K}\|
\]

and furthermore that for any integer \(l\) with \(h < l/p < kh^2\), either (3) holds with \(J = K\) or

\[
|f(l)| \geq p^{-4KH} q^{-hK} \cdot \|e^{K\log K}\| \cdot \|e^{K\log K}\|,
\]

these estimates follow in fact as in the proof of Lemma 6 of [3], on noting that the left-hand side of (3), multiplied by

\[
p^{4K} e^{K} a_1^{(K)} \cdots a_n^{(K)} (l/p)^{K} m_0\]

is an algebraic integer, and we have \(m_0 p^K \leq k \log \log \Omega\). One deduces next, as in Lemma 7 of [3], that for some \(\epsilon (0 < \epsilon < 1)\) depending only on \(n\) and \(d\), and for any integer \(J\) with \(0 < \epsilon < J' < 2n/\epsilon\), holds with \(J = K\).
for all integers \( l \) with \( 1 \leq l \leq hp^K k^{2p} \) and all non-negative integers \( m_0, \ldots, m_{n-1} \) satisfying (4) with \( k \) replaced by \( k/2^p \); the argument follows closely its earlier counterpart, \( k \) and \( \log A \) being replaced by \( hp^K \) and \( \log D \) respectively, and, since \( \log D \) does not exceed \( k \log D \), one obtains the same estimates as in [3] for the numbers on the right of (12) and (13) with, say, \( K' \) in place of \( K \). Similarly one sees that the analogue of Lemma 8 of [3] holds, that is, (3) is valid with \( k \) replaced by \( k/2^p \) for all \( l \) with \( 1 \leq l \leq kp^K \), \( (l, p) = 1 \), and all \( m_0, \ldots, m_{n-1} \) satisfying (4) with \( J = K + 1 \). Finally one argues as in \( \S \) 2 above, and this yields the required result.

4. Proof of the theorem. We adopt the notation of \( \S \) 2 and record first two preliminary lemmas; here \( A \) denotes the maximum of \( A_1, \ldots, A_n \) and \( D = d^n \).

**Lemma 1.** If \( A \neq 0 \) then
\[
\log |A| > -4nDB\log(dA).
\]

**Lemma 2.** If \( A = 0 \) but \( b_1, \ldots, b_n \) are not all 0 then in fact \( A = 0 \) for some \( b_1, \ldots, b_n \), not all 0, with absolute values at most
\[
(4^nD^2\log A)^{2(n+1)}.
\]

The first result is Lemma 6 of [1] and the second is a consequence of the main deduction of that paper; indeed it is clear that the conclusion of the last paragraph of \( \S \) 2 of [1] holds when \( A = 0 \), and the required result follows on applying this with \( n' = n, \delta = 1 \) and \( H = B^{-1} = A^{1/\delta} \), where \( B \) the maximum of the absolute values of \( b_1, \ldots, b_n \), is chosen minimally.

We shall suppose, as we may without loss of generality, that \( A_1 \leq A_2 \leq \ldots \leq A_n = A \) and that \( a_i = -1 \). We can clearly suppose further that \( A > C', B > C' \) for some suitably large \( C' = C'(n, \delta) \), for otherwise the theorem follows at once either from the result of [3] or from Lemma 1. We note also that if \( A \neq 0 \), then, by Lemma 1,
\[
\log |A| > -c\log A,
\]
where \( c = 8nD \), and thus, if \( \log A < C/\log d \), we have \( \log A > (C/c) \log d \), whence
\[
\log A_j < B^{\log d} \quad (1 \leq j \leq n-1).
\]

We now apply the result of \( \S \) 2 with \( c_i = (4d)^n \); if \( p \) is the prime indicated there, then, for some \( m \) with \( 0 \leq m < n \), \( a_{m+1} \) does not generate an extension of \( K \) in \( F(a_{m+1}) \) of degree \( p \). Hence, by Lemma 3 of [3],
\[
a_{m+1} = a_{m+1}^1 \ldots a_{m+1}^\alpha
\]
for some \( \gamma \) in \( K \) and some integers \( r_1, \ldots, r_m \) with \( 0 \leq r_j < p \). We shall suppose that the height \( A' = A_{m+1} \) of \( a_{m+1} \) satisfies
\[
\log A' < \alpha(\log d)^p,
\]
and we verify first that this involves no loss of generality. In fact, if \( m \leq n-2 \), (7) is a weaker version of (6); thus we assume that \( m = n-1 \), whence \( A' = A \). Clearly each conjugate of
\[
y = a_{m+1}^{r_1} \ldots a_{m+1}^{r_m}
\]
has absolute value at most \( (dA')^{2p}(dA)^n \), and thus, by Lemma 4 of [3], the height of \( y \) is at most \( (2dA)^{2n} \). This would be less than \( A^{1/\delta} \) if (7) did not hold, for then (5) would give \( A_{m+1} < A \). But from (6) we see that
\[
\log a_m = r_1 \log a_1 + \ldots + r_n \log a_n + p \log y
\]
for some value of \( \log y \), and thus
\[
A = b_1 \log a_1 + \ldots + b_n \log a_n + b_p \log y
\]
where
\[
b_j = b_j + b_p r_j \quad (1 \leq j \leq m), \quad b_p = b_n p.
\]
The integers \( b_j \) plainly have absolute values at most \( 2pB \) and hence, on modifying \( b_j \) if necessary so as to make \( \log y \) principal-valued, we see that the theorem would follow by induction on \( A \). It suffices therefore to assume that (7) is valid.

We now construct, as far as possible, a sequence \( \gamma_1 = \gamma, \gamma_2, \gamma_3, \ldots \) of elements of \( K \) such that \( \gamma_j = a_{m+1}^{r_1} \ldots a_{m+1}^{r_j} (1 \leq j \leq 2, \ldots) \), where the \( r_j \) are integers with \( 0 \leq r_j < p \). Clearly we have
\[
a_{m+1} = a_{m+1}^{r_1} \ldots a_{m+1}^{r_j}
\]
where the \( s_k \) are integers with \( 0 \leq s_k < p' \), and from this we deduce as above that the height of \( \gamma_j \) is at most \( (2dA')^{n+1} \). Let \( H \) be the bound specified in Lemma 2 with the latter number in place of \( A \) and with \( n+1 \) in place of \( n \). We distinguish two cases according as the sequence terminates for some \( l \) with \( p' \leq H \) or it does not. In the latter case, let \( l \) be the least integer with \( p' > H \). From (8), taking logarithms, and Lemma 2, we see that there exist integers \( b'_1, b'_2, \ldots, b'_{m+1} \), not all 0, with absolute values at most \( H \), such that
\[
b'_1 \log a_1 + \ldots + b'_{m+1} \log a_{m+1} + b' \log \gamma_1 = 0,
\]
and, on utilizing (8) again and eliminating \( \gamma_1 \), we obtain
\[
b'_1 \log a_1 + \ldots + b'_{m+1} \log a_{m+1} = 0
\]
for some integer $b_j'$, where
\[ b_j' = p b_j - b_j v_j \quad (1 < j \leq m) \], \quad b_{m+1}' = p b_{m+1} + b'. \]

Now the $b_j'$ ($j > 1$) are integers with absolute values at most $2pH^2$; thus all $b_j'$ have absolute values at most $2npH^2$ and, by (7), this is less than $B$ if $C$ is sufficiently large. From (9), we can plainly express $b_{m+1}' A$ as a linear form in the log $a_j$ with $j \neq m+1$ and with integer coefficients having absolute values at most $2B^2$. Hence, if $b_{m+1}' = 0$, the theorem follows by induction on $n$. If $b_{m+1}' = 0$ then, since $p^j > H$, we have $b' = 0$ and so $b_j' \neq 0$ for some $j \leq m$; in this case the elimination of log $a_j$ furnishes the desired conclusion.

It remains to consider the possibility that the sequence terminates for some $l$ with $p^l \leq H$. From (8) we see that $A$ can be expressed as a linear form in the log $a_j$ with $a_{m+1}$ replaced by $y_j$ and with integer coefficients having absolute values at most $2npH^2$; furthermore, from (7), this is less than $B^2$ if $C$ is sufficiently large. Furthermore, since by supposition the sequence terminates, we deduce from Lemma 3 of [5] that $y_j^{(p)}$ generates an extension of $K(a_1^{(p)}, \ldots, a_n^{(p)})$ of degree $p$. Recalling that $y_j$ has height $A''$, say, where log $A''$ log $A'$ is bounded in terms of $n$ and $d$ only, it follows that the hypothesis of §2 hold with $y_j$ substituted for $a_{m+1}$ and with a reduced value of $C$. After at most $n$ such substitutions this contradicts the result of §3 (since the choice of $p$ where depends only on $n$ and $d$) and the contradiction proves the theorem.

References


Received on 23. 8. 1973 (449)