Symmetric improvements of Liouville's inequality: A survey

Jan-Hendrik Evertse *

Abstract. Let K_1, K_2 be algebraic number fields of degrees $r \geq 3$, $s \geq 3$, respectively such that K_1K_2 has degree rs. Denote the conjugates of $\alpha \in K_1$ by $\alpha^{(1)}, \ldots, \alpha^{(r)}$ and those of $\beta \in K_2$ by $\beta^{(1)}, \ldots, \beta^{(s)}$. Let $\mathcal{E}$ be a subset of $\{(i,j) : i = 1, \ldots, r,\ j = 1, \ldots, s\}$. According to Liouville's inequality we have $\prod_{(i,j)\in\mathcal{E}} |\alpha^{(i)} - \beta^{(j)}| \geq 2^{-rs} M(\alpha)^{-s} M(\beta)^{-r}$ for α, β with $\mathbf{Q}(\alpha) = K_1$, $\mathbf{Q}(\beta) = K_2$, where $M(\cdot)$ denotes the Mahler measure of an algebraic number. We are interested in the problem whether there exists a symmetric improvement of this inequality, i.e., whether we can replace both exponents r, s at the right-hand side by smaller values. In this paper we give an overview of some (ineffective) results related to this problem.

1991 Mathematics Subject Classification: 11J68.

1. Introduction

If $f(X) = a(X - \alpha^{(1)}) \cdots (X - \alpha^{(r)})$ is the minimal polynomial of an algebraic number α (i.e., with coefficients in $\mathbf{Z}$ having gcd 1) then the Mahler measure of α is defined by

$$M(\alpha) := |a| \prod_{i=1}^{r} \max(1, |\alpha^{(i)}|) \ .$$

The generalisation of Liouville's inequality to number fields states that if K is an algebraic number field and α has degree r over K, then

$$|\alpha - \beta| \geq c(\alpha, K) \cdot M(\beta)^{-r} \quad \text{for } \beta \in K,$$

where $c(\alpha, K)$ is an effective constant depending only on K and α. ¿From a generalisation of Dirichlet's theorem to number fields it follows that the exponent r cannot be replaced by a number ≤ 2 (cf. [10], p. 253, Thm. 2A) if $\alpha \in \mathbf{R}$ and $K \subset \mathbf{R}$. On the other hand, a generalisation by LeVeque [8] (Chap. 4) of Roth's

*The author has done part of the research for this paper while he was visiting the Institute for Advanced Study in Princeton during the fall of 1997. The author is very grateful to the IAS for its hospitality.

theorem [9] states that for every algebraic number α and every $\delta > 0$ there are only finitely many $\beta \in K$ with

$$|\alpha - \beta| < M(\beta)^{-2-\delta}\,.$$

We now consider symmetric analogues of these results. Let K_1, K_2 be number fields satisfying

$$[K_1K_2 : K_2] = r\,, \qquad [K_1K_2 : K_1] = s\,, \tag{1.1}$$

where K_1K_2 denotes the composite of K_1, K_2. Then the symmetric version of Liouville's inequality states that

$$|\alpha - \beta| \geq 2^{-[K_1K_2:\mathbf{Q}]} M(\alpha)^{-s} M(\beta)^{-r} \quad \text{for } \alpha, \beta \text{ with } \mathbf{Q}(\alpha) = K_1, \mathbf{Q}(\beta) = K_2. \tag{1.2}$$

In 1982, Schmidt [11] conjectured the following symmetric version of Roth's theorem: for every $\delta > 0$ there are only finitely many pairs α, β with

$$|\alpha - \beta| < \big(\max(M(\alpha), M(\beta))\big)^{-2-\delta}\,, \quad \mathbf{Q}(\alpha) = K_1,\ \mathbf{Q}(\beta) = K_2,\ \alpha \neq \beta. \tag{1.3}$$

This conjecture is as yet unproved. Some evidence for this conjecture is given by a result of Bombieri and van der Poorten [1], which implies that there are positive numbers $c_1(r, s, \delta)$, $c_2(r, s, \delta)$, increasing to infinity as $\delta \downarrow 0$, $r \to \infty$ or $s \to \infty$, such that (1.3) has only finitely many solutions with

$$M(\beta) > M(\alpha)^{c_1(r,s,\delta)} \quad \text{or} \quad M(\alpha) > M(\beta)^{c_2(r,s,\delta)}\,. \tag{1.4}$$

Bombieri and van der Poorten proved their result by means of a suitable adaptation of Roth's argument. A similar result may be deduced by Vojta's method [12] which uses Schmidt's Subspace theorem.

Since we were not able to prove Schmidt's conjecture, we tried to prove weaker so-called symmetric improvements of Liouville's inequality (1.2). These are finiteness results for inequalities of the type

$$|\alpha - \beta| \leq \big(\Psi(M(\alpha), M(\beta))\big)^{-1} \quad \text{in } \alpha, \beta \text{ with } \mathbf{Q}(\alpha) = K_1, \mathbf{Q}(\beta) = K_2,$$

where Ψ is a function with

$$\lim_{\max(x,y)\to\infty} \frac{\Psi(x, y)}{x^s y^r} = 0\,. \tag{1.5}$$

Here we do not wish to impose restrictions on $M(\alpha)$ and $M(\beta)$ such as (1.4). Note that Schmidt's conjecture stated above yields a symmetric improvement of Liouville's inequality only if $r \geq 3$ and $s \geq 3$. In [5] we proved the following much weaker symmetric improvement. Assume K_1, K_2 are linearly disjoint, i.e.,

$$[K_1K_2 : \mathbf{Q}] = [K_1 : \mathbf{Q}][K_2 : \mathbf{Q}]\,. \tag{1.6}$$

Further assume

$$[K_1 : \mathbf{Q}] = [K_1K_2 : K_2] = r \geq 3, \quad [K_2 : \mathbf{Q}] = [K_1K_2 : K_1] = s \geq 3. \tag{1.7}$$

Theorem 1. *The inequality*

$$|\alpha - \beta| \leq \left(M(\alpha)^{-s} M(\beta)^{-r}\right)^{1-\frac{1}{1436}} \quad \text{in } \alpha, \beta \text{ with } \mathbf{Q}(\alpha) = K_1, \mathbf{Q}(\beta) = K_2$$

has only finitely many solutions.

It is reasonable to assume that $r \geq 3$, $s \geq 3$ since otherwise not even Schmidt's conjecture would give a symmetric improvement of Liouville's inequality. Condition (1.6) is unnatural but it is necessary in the proof.

We consider a more general situation. We continue to assume (1.6), (1.7). Let $\alpha \mapsto \alpha^{(i)}$ $(i = 1, \dots, r)$ denote the isomorphic embeddings of K_1 into $\mathbf{C}$ and $\beta \mapsto \beta^{(j)}$ $(j = 1, \dots, s)$ the isomorphic embeddings of K_2 into $\mathbf{C}$. Let

$$\mathcal{E} \subseteq \{(i, j) : i = 1, \dots, r,\ j = 1, \dots, s\}$$

be any non-empty subset. A generalisation of Liouville's inequality (1.2) states that

$$\prod_{(i,j)\in\mathcal{E}} |\alpha^{(i)} - \beta^{(j)}| \geq 2^{-rs} M(\alpha)^{-s} M(\beta)^{-r} \qquad \text{for } \alpha, \beta \text{ with } \mathbf{Q}(\alpha) = K_1,\ \mathbf{Q}(\beta) = K_2\,. \tag{1.8}$$

Again we are interested in symmetric improvements of this inequality, i.e., finiteness results for inequalities of the type

$$\prod_{(i,j)\in\mathcal{E}} |\alpha^{(i)} - \beta^{(j)}| \leq \left(\Psi(M(\alpha), M(\beta))\right)^{-1} \qquad \text{in } \alpha, \beta \text{ with } \mathbf{Q}(\alpha) = K_1,\ \mathbf{Q}(\beta) = K_2\,, \tag{1.9}$$

where Ψ is a function with (1.5).

In view of Schmidt's conjecture one might expect that for "small" sets $\mathcal{E}$, inequality (1.9) has only finitely solutions if $\Psi(x, y) = \max(x, y)^{2+\delta}$, $\delta > 0$, that the function Ψ has to be chosen larger if $\mathcal{E}$ is larger and that finally no symmetric improvement of (1.8) exists if $\mathcal{E}$ is too large. At the moment we are not able to pose a precise conjecture about the best possible symmetric improvement, i.e., the smallest function Ψ for a given set $\mathcal{E}$. Below we have stated some theorems giving far from optimal symmetric improvements of (1.8). These results deal with inequalities

$$\prod_{(i,j)\in\mathcal{E}} |\alpha^{(i)} - \beta^{(j)}| \leq \left(M(\alpha)^{-s} M(\beta)^{-r}\right)^{1-c} \qquad \text{in } \alpha, \beta \text{ with } \mathbf{Q}(\alpha) = K_1,\ \mathbf{Q}(\beta) = K_2 \tag{1.10}$$

with positive, but very small values of c.

We first recall a result from [5]. A pair (i, j) with $1 \leq i \leq r$, $1 \leq j \leq s$ is called real if both maps $\alpha \mapsto \alpha^{(i)}$, $\beta \mapsto \beta^{(j)}$, defined on K_1, K_2, respectively, have their images contained in $\mathbf{R}$. The pair (i, j) is called complex if at least one of these maps does not have its image contained in $\mathbf{R}$. For each complex pair (i, j) there is a pair (i', j') such that $\alpha^{(i')}$, $\beta^{(j')}$ are the complex conjugates of $\alpha^{(i)}, \beta^{(j)}$, respectively for all $\alpha \in K_1$, $\beta \in K_2$. We showed that if $\mathcal{E}$ has the property that whenever a complex pair (i,j) belongs to $\mathcal{E}$ then also $(i',j') \in \mathcal{E}$, and if $\mathcal{E}$ has cardinality $|\mathcal{E}| < \frac{1}{3}rs = \frac{1}{3}[K_1K_2 : \mathbf{Q}]$, then (1.10) has only finitely many solutions for $c = \frac{1}{718} \cdot \frac{rs-3|\mathcal{E}|}{rs+3|\mathcal{E}|}$. On the other hand we showed that if $\mathcal{E}$ is the full set $\{(i,j) : i = 1,\dots,r,\ j = 1,\dots,s\}$ then for every $c > 0$ (1.10) has infinitely many solutions. In fact, we constructed infinitely many solutions by picking arbitrary α_0, β_0 with $\mathbf{Q}(\alpha_0) = K_1$, $\mathbf{Q}(\beta_0) = K_2$ and then showing that there are infinitely many $a \in \mathbf{Z}$ such that $\alpha := \alpha_0 + a$, $\beta := \beta_0 + a$ is a solution of (1.10). So roughly speaking, we showed that there is a symmetric improvement of (1.8) if $\mathcal{E}$ is "small" and that there is no such symmetric improvement if $\mathcal{E}$ consists of all pairs (i,j).

We recently succeeded in giving a precise description of the collection of sets $\mathcal{E}$ for which (1.8) has a symmetric improvement. We view the set $\{(i,j) : i = 1,\dots,r,\ j = 1,\dots,s\}$ as an $r\times s$-matrix of which i indexes the rows and j the columns. A real row is a set $\{(i,1),\dots,(i,s)\}$ such that $\alpha \mapsto \alpha^{(i)}$ maps K_1 into $\mathbf{R}$. A real column is a set $\{(1,j),\dots,(r,j)\}$ such that $\beta \mapsto \beta^{(j)}$ maps K_2 into $\mathbf{R}$. Let $\mathcal{E}^c$ denote the complement of $\mathcal{E}$ in $\{(i,j) : i = 1,\dots,r,\ j = 1,\dots,s\}$.

Theorem 2. *Assume that K_1, K_2 satisfy (1.6), (1.7). Further, assume that $\mathcal{E}^c \neq \emptyset$, that $\mathcal{E}^c$ is not contained in a real row and that $\mathcal{E}^c$ is not contained in a real column. Then for*

$$c = \frac{1}{718(r+s)^2} \tag{1.11}$$

inequality (1.10) has only finitely many solutions.

If $\mathcal{E}^c$ does not satisfy the conditions of Theorem 2 then basically there is no symmetric improvement of Liouville's inequality:

Theorem 3. *Assume that K_1, K_2 satisfy (1.6), (1.7). Further, assume that $\mathcal{E}^c = \emptyset$ or that $\mathcal{E}^c$ is contained in a real row or that $\mathcal{E}^c$ is contained in a real column. Then for every $c > 0$, inequality (1.10) has infinitely many solutions.*
More precisely, if for instance $\mathcal{E}^c \neq \emptyset$ and $\mathcal{E}^c$ is contained in a real row, then for every $c > 0$, (1.10) has infinitely many solutions with

$$\frac{r-2}{s} - c < \frac{\log M(\alpha)}{\log M(\beta)} < \frac{r-2}{s} + c\,. \tag{1.12}$$

In Section 2 we will sketch some of the ideas behind the proofs of Theorems 2 and 3. The complete proofs of p-adic generalisations of Theorems 2 and 3 are given in [6]. We would like to mention here that both the proofs of Theorems 2 and 3 use Schmidt's Subspace theorem. Hence Theorem 2 is ineffective. A basic flaw of our methods of proof is that we have to assume (1.6), (1.7). One would expect that these conditions can be relaxed to $[K_1K_2 : K_2] = r \geq 3$, $[K_1K_2 : K_1] = s \geq 3$, say. The value $1/718(r+s)^2$ for c in Theorem 2 arises from the proof and has no special meaning. Very likely, the dependence on r and s is not best possible.

Theorem 3 states that (1.10) has infinitely many solutions with $\frac{\log M(\alpha)}{\log M(\beta)}$ lying in a very specific interval. The next result, which is just a straightforward consequence of a theorem of Corvaja ([2], p. 13, Thm. 2) implies that (1.10), and in fact some much stronger inequality, has only finitely many solutions if we require $\log M(\alpha)/\log M(\beta)$ to be very large or very small. This result may be viewed as an explicit version of Vojta's "Roth's theorem with moving targets." [12]

Theorem 4. *Let K_1, K_2 be algebraic number fields of degrees $r \geq 1, s \geq 1$, respectively and let $\mathcal{E}$ be any non-empty subset of $\{(i,j) : i = 1, \ldots, r,\ j = 1, \ldots, s\}$. Further, let*

$$c(r,s,\delta) = s \cdot \exp(10^4 \delta^{-2} \log 6r \log(4\delta^{-1} \log 6r))\,. \tag{1.13}$$

Then for every $\delta > 0$, the inequality

$$\prod_{(i,j)\in\mathcal{E}} |\alpha^{(i)} - \beta^{(j)}| \leq M(\beta)^{-2-\delta}$$

has only finitely many solutions with

$$\mathbf{Q}(\alpha) = K_1,\ \mathbf{Q}(\beta) = K_2,\ M(\beta) > M(\alpha)^{c(r,s,\delta)}\,.$$

In Section 3 we deduce Theorem 4 from Corvaja's result.

2. Sketches of the proofs of Theorems 2 and 3

The Mahler measure of $F(X) = a(X - \alpha^{(1)}) \cdots (X - \alpha^{(r)}) \in \mathbf{Z}[X]$ is defined by $M(F) = |a| \prod_{i=1}^{r} \max(1, |\alpha^{(i)}|)$. For $F \in \mathbf{Z}[X]$ of degree r and $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})$ we define the polynomial $F_U(X) = (cX + d)^r F(\frac{aX+b}{cX+d})$. The *resultant* of $F(X) = a(X - \alpha^{(1)}) \cdots (X - \alpha^{(r)})$ and $G(X) = b(X - \beta^{(1)}) \cdots (X - \beta^{(s)})$ is defined by

$$R(F,G) = a^s b^r \prod_{i=1}^{r} \prod_{j=1}^{s} (\alpha^{(i)} - \beta^{(j)})\,.$$

$R(F,G)$ is a rational integer which is non-zero if and only if F and G have no common factor. Further we have:

$$|R(F,G)| \leq 2^{rs} M(F)^s M(G)^r\,; \tag{2.1}$$

$$R(F_U, G_U) = R(F,G) \quad \text{for } U \in SL_2(\mathbf{Z}). \tag{2.2}$$

Now let K_1, K_2 be algebraic number fields with (1.6), (1.7). Let α, β be numbers with $\mathbf{Q}(\alpha) = K_1$ and $\mathbf{Q}(\beta) = K_2$. Further, let $F(X) = a(X - \alpha^{(1)}) \cdots (X - \alpha^{(r)})$, $G(X) = b(X - \beta^{(1)}) \cdots (X - \beta^{(s)})$ be the minimal polynomials of F, G, respectively. From (1.6) it follows that α, β are non-conjugate, hence F and G have no common factor. Let $\mathcal{E}$ be a non-empty subset of $\{(i,j) : i = 1, \ldots, r,\ j = 1, \ldots, s\}$. We have

$$\begin{aligned}\prod_{(i,j)\in\mathcal{E}} |\alpha^{(i)} - \beta^{(j)}| &\geq \prod_{(i,j)\in\mathcal{E}} \frac{|\alpha^{(i)} - \beta^{(j)}|}{\max(1, |\alpha^{(i)}|)\max(1, |\beta^{(j)}|)} \\ &\geq 2^{-rs} \prod_{i=1}^{r}\prod_{j=1}^{s} \frac{|\alpha^{(i)} - \beta^{(j)}|}{\max(1, |\alpha^{(i)}|)\max(1, |\beta^{(j)}|)} \\ &= 2^{-rs}|R(F,G)| \cdot M(F)^{-s}M(G)^{-r}\end{aligned} \tag{2.3}$$

on multiplying both numerator and denominator with $a^s b^r$. By inserting the trivial lower bound $|R(F,G)| \geq 1$, following from the fact that $R(F,G)$ is a non-zero integer, we get Liouville's inequality (1.8). In the proof of Theorem 2 we used the following non-trivial lower bound for $|R(F,G)|$ which has been proved in [5]. In fact, the proof of this lower bound uses various other results, proved in [4], [7]. For a sketchy overview of the proof we refer to [3]. The foundation is Schmidt's Subspace theorem.

Theorem 5. *Let $F, G \in \mathbf{Z}[X]$ be polynomials of degrees $r \geq 3$, $s \geq 3$, respectively such that FG has splitting field L and such that FG has no multiple zeros. Then there is a matrix $U \in SL_2(\mathbf{Z})$ such that*

$$|R(F,G)| \geq C(r,s,L)\big(M(F_U)^s M(G_U)^r\big)^{\frac{1}{718}} \tag{2.4}$$

where $C(r,s,L)$ is an ineffective positive number depending only on r, s, L.

The matrix U in the right-hand side of (2.4) is necessary because of (2.2).

Let again K_1, K_2 be number fields with (1.6), (1.7), $\mathcal{E}$ a subset of $\{(i,j) : i = 1,\dots,r,\ j = 1,\dots,s\}$, α, β numbers with $\mathbf{Q}(\alpha) = K_1$, $\mathbf{Q}(\beta) = K_2$ and F, G their respective minimal polynomials. Theorem 2 follows from Theorem 5 and the elementary Lemma 6 below which has been proved in [6]. Below, constants implied by $\ll$, $\gg$ depend on K_1, K_2 only.

Lemma 6. *Suppose that $\mathcal{E}^c \neq \emptyset$, that $\mathcal{E}^c$ is not contained in a real row and that $\mathcal{E}^c$ is not contained in a real column. Then for every $U \in SL_2(\mathbf{Z})$ there is a pair $(i_0, j_0) \in \mathcal{E}^c$ with*

$$\frac{|\alpha^{(i_0)} - \beta^{(j_0)}|}{\max(1, |\alpha^{(i_0)}|)\max(1, |\beta^{(j_0)}|)} \ll \frac{M(F_U)^{r+s}M(G_U)^{r+s}}{M(F)^{1/r}M(G)^{1/s}}\,. \tag{2.5}$$

Now Theorem 2 is deduced as follows. Put $f_{ij} := \frac{|\alpha^{(i)}-\beta^{(j)}|}{\max(1,|\alpha^{(i)}|)\max(1,|\beta^{(j)}|)}$. Let $0 < \theta < 1$. Let U be the matrix from Theorem 5 and, assuming $\mathcal{E}$ sastisfies the conditions of Theorem 2, let $(i_0, j_0) \in \mathcal{E}^c$ be the pair from Lemma 6. Then from

$f_{ij} \ll 1$, (2.4), (2.5), $M(F) = M(\alpha)$, $M(G) = M(\beta)$ it follows

$$\begin{aligned}
\prod_{(i,j)\in\mathcal{E}} |\alpha^{(i)} - \beta^{(j)}| &\gg \prod_{(i,j)\in\mathcal{E}} f_{ij} \\
&\gg \left(\prod_{i=1}^{r}\prod_{j=1}^{s} f_{ij}\right) f_{i_0,j_0}^{-\theta} = \frac{|R(F,G)|}{M(F)^s M(G)^r} \cdot f_{i_0,j_0}^{-\theta} \\
&\gg \left(\frac{\left(M(F_U)^s M(G_U)^r\right)^{\frac{1}{718}}}{M(F)^s M(G)^r}\right) \cdot \left(\frac{M(F)^{1/r} M(G)^{1/s}}{M(F_U)^{r+s} M(G_U)^{r+s}}\right)^{\theta} \\
&\gg \left(M(\alpha)^{-s} M(\beta)^{-r}\right)^{1-\frac{1}{718(r+s)^2}}
\end{aligned}$$

taking $\theta = \frac{\min(r,s)}{718(r+s)}$ so that the exponents on $M(F_U)$, $M(G_U)$ become non-negative. This implies Theorem 2. □

We now sketch the proof of Theorem 3. In what follows, we take $c > 0$ and we choose $\delta > 0$ sufficiently small in terms of c. Suppose for instance that $\mathcal{E}^c \neq \emptyset$ and that $\mathcal{E}^c$ is contained in the real row $\{(1,1), \ldots, (1,s)\}$ where $\alpha \mapsto \alpha^{(1)}$ is a real embedding of K_1. Pick any α_0, β_0 with $\mathbf{Q}(\alpha_0) = K_1$, $\mathbf{Q}(\beta_0) = K_2$. Constants implied by $\ll$, $\gg$ depend only on K_1, K_2, α_0, β_0 and c.

We start with the observation that for every $Q \gg 1$ there is a non-zero vector $(x, y) \in \mathbf{Z}^2$ satisfying the inequalities

$$\begin{aligned}
&|x + \alpha_0^{(1)} y| \ll Q^{-1}, \ \ |x + \alpha_0^{(i)} y| \ll Q \text{ for } i = 2, \ldots, r, \\
&|x + \beta_0^{(j)} y| \ll Q \text{ for } j = 1, \ldots, s.
\end{aligned}$$

Indeed, using $\alpha_0^{(1)} \in \mathbf{R}$ (which is essential) one shows that these inequalities define a symmetric convex body in $\mathbf{R}^2$ of volume $\gg\ll 1$ and then the existence of a non-zero integral solution follows from Minkowski's theorem. More precisely, using the (two-dimensional) Subspace theorem and Minkowski's theorem on successive minima one shows that for every $Q \gg 1$ the system of inequalities

$$\left.\begin{aligned}
&Q^{-1-\delta} \le |x + \alpha_0^{(1)} y| \le Q^{-1+\delta}, \ \ Q^{1-\delta} \le |x + \alpha_0^{(i)} y| \le Q^{1+\delta} \text{ for } i = 2, \ldots, r, \\
&Q^{1-\delta} \le |x + \beta_0^{(j)} y| \le Q^{1+\delta} \text{ for } j = 1, \ldots, s
\end{aligned}\right\} \tag{2.6}$$

has two linearly independent solutions in $\mathbf{Z}^2$, (a, b) and (c, d), say, which moreover satisfy

$$|ad - bc| \ll 1. \tag{2.7}$$

For further details we refer to [6].

Choose $Q \gg 1$ and corresponding linearly independent vectors (a, b), (c, d) satisfying (2.6) and (2.7) and put $\alpha := (a + b\alpha_0)/(c + d\alpha_0)$, $\beta := (a + b\beta_0)/(c + d\beta_0)$. By (2.7) we have $M(\alpha) \gg\ll \prod_{i=1}^{r} \max(|a + b\alpha_0^{(i)}|, |c + d\alpha_0^{(i)}|)$ and together with (2.6) this yields

$$Q^{r-2-r\delta} \ll M(\alpha) \ll Q^{r-2+r\delta} \ . \tag{2.8}$$

In a very similar way one shows

$$Q^{s-s\delta} \ll M(\beta) \ll Q^{s+s\delta}. \tag{2.9}$$

Provided δ is sufficiently small this implies

$$\frac{r-2-r\delta}{s+s\delta} \ll \frac{\log M(\alpha)}{\log M(\beta)} \ll \frac{r-2+r\delta}{s-s\delta}\,. \tag{2.10}$$

Since (a,b), (c,d) satisfy (2.6) and (2.7) we have for each pair (i,j),

$$\begin{aligned} |\alpha^{(i)}-\beta^{(j)}| &= \left| \frac{a+b\alpha_0^{(i)}}{c+d\alpha_0^{(i)}} - \frac{a+b\beta_0^{(j)}}{c+d\beta_0^{(j)}} \right| = \frac{|ad-bc|\cdot|\alpha_0^{(i)}-\beta_0^{(j)}|}{|c+d\alpha_0^{(i)}|\cdot|c+d\beta_0^{(j)}|} \\ &\ll \begin{cases} Q^{2\delta} & \text{if } i=1\,, \\ Q^{-2+2\delta} & \text{if } i\neq 1\,. \end{cases} \end{aligned}$$

Now using that $\mathcal{E}$ contains all pairs (i,j) with $i=2,\dots,r$, $j=1,\dots,s$ (which follows from our assumption $\mathcal{E}^c \subset \{(1,1),\dots,(1,s)\}$) and (2.8), (2.9) we get

$$\prod_{(i,j)\in\mathcal{E}} |\alpha^{(i)}-\beta^{(j)}| \ll Q^{-(r-2)s-sr+2rs\delta} \ll \big(M(\alpha)^{-s}M(\beta)^{-r}\big)^{1-c}$$

assuming δ is sufficiently small. Now making δ even smaller if necessary and then letting $Q\to\infty$ we get in view of (2.10) infinitely many solutions (α,β) of (1.10) with (1.12). This proves Theorem 3. Note that we started with an arbitrary pair (α_0,β_0) and then showed that the orbit $(\frac{a+b\alpha_0}{c+d\alpha_0},\frac{a+b\alpha_0}{c+d\alpha_0})$ $(a,b,c,d\in\mathbf{Z},\ ad-bc\neq 0)$ contains infinitely many solutions. Thus, there are infinitely many orbits, each having infinitely many solutions. $\square$

3. Proof of Theorem 4.

Let K be an algebraic number field and M_K its set of places. For every place $v\in M_K$, choose a normalised absolute value $\|\cdot\|_v$ such that if v is archimedean, then the restriction of $\|\cdot\|_v$ to $\mathbf{Q}$ is $|\cdot|^{[K_v:\mathbf{R}]/[K:\mathbf{Q}]}$ and if v lies above the prime number p then the restriction of $\|\cdot\|_v$ to $\mathbf{Q}$ is $|\cdot|_p^{[K_v:\mathbf{Q}_p]/[K:\mathbf{Q}]}$. We define the absolute height of an algebraic number α by $H(\alpha)=M(\alpha)^{1/\deg\alpha}$. We need the following result of Corvaja:

Theorem 7. *Let $n\geq 1$ and $N\geq 36^2\log 6n$ be integers. Let $S_1,\dots,S_n$ be pairwise disjoint finite sets of places on K and $S=S_1\cup\dots\cup S_n$. Further, let μ_v $(v\in S)$ be non-negative reals. For tuples of algebraic numbers $(\beta,\alpha_1,\dots,\alpha_n)$ put*

$$A(\beta,\alpha_1,\dots,\alpha_n) := H(\beta)\cdot\Big(4\cdot\prod_{h=1}^{n} H(\alpha_h)^{3/n}\Big)^{2N!}\,.$$

Suppose there are N tuples $(\beta_k, \alpha_{1k}, \dots, \alpha_{n,k}) \in K^{n+1}$ $(k = 1, \dots, N)$ satisfying

$$0 < ||\alpha_{hk} - \beta_k||_v \leq A(\beta_k, \alpha_{1k}, \dots, \alpha_{nk})^{-\mu_v} \quad \text{for } k = 1, \dots, N,\ v \in S_h,\ h = 1, \dots, n, \tag{3.1}$$

$$\alpha_{h_1,k} \neq \alpha_{h_2,k} \quad \text{for } 1 \leq h_1 < h_2 \leq n,\ k = 1, \dots, N, \tag{3.2}$$

$$\frac{\log A(\beta_k, \alpha_{1k}, \dots, \alpha_{nk})}{\log A(\beta_{k+1}, \alpha_{1,k+1}, \dots, \alpha_{n,k+1})} < \frac{1}{48nN^2N!} \quad \text{for } k = 1, \dots, N-1. \tag{3.3}$$

Then

$$\sum_{v \in S} \mu_v < \frac{9\sqrt{\log 6n}}{\sqrt{N}}. \tag{3.4}$$

Proof. This is almost Thm. 2 of Corvaja [2], p. 13. Corvaja has the technical condition $n \geq 3$. If $n < 3$, Corvaja's condition can be satisfied by adding two new groups of non-archimedean places S_{n+1}, S_{n+2} such that $||\beta_k||_v = 1$ for $k = 1, \dots, N$, $v \in S_{n+1} \cup S_{n+2}$ and taking $\alpha_h \in \{-1, 0, 1\}$, $\mu_v = 0$ for $v \in S_h$, $h = n+1, n+2$. Thus, in Corvaja's Thm. 2 the number n must be replaced everywhere by $n+2$ and we have taken care of that by enlarging some of Corvaja's constants. Further, Corvaja assumes $\mu_v \leq 1$ for $v \in S$. If this is not satisfied one may replace K by a sufficiently large finite extension K' and the set of places S_h by the set S'_h consisting of the continuations to K' of the places in S_h. Put $S' = S'_1 \cup \dots \cup S'_n$ and $\mu_{v'} := \mu_v \cdot \frac{[K'_{v'}:K_v]}{[K':K]}$ for $v' \in S'$ lying above $v \in S$. Then (3.1)–(3.4) imply the same conditions with K, S_h, v, μ_v replaced by $K', S'_h, v', \mu_{v'}$, respectively. and by taking K' appropriately we can achieve $\mu_{v'} \leq 1$ for $v' \in S'$. Finally, in Corvaja's Thm. 2 there is a system of inequalities (1.1) which is similar to our system (3.1) except that it has at the right-hand side $<$-signs instead of $\leq$-signs. An inspection of Corvaja's proof (cf. pp. 35–40 of [2]) learns that Corvaja's Thm. 2 remains correct if these $<$-signs are replaced by $\leq$-signs.

In his original proof, Roth [9] constructed an auxiliary polynomial in N variables having large index at points $(\alpha_h, \dots, \alpha_h)$ $(h = 1, \dots, n)$ with equal coordinates. Following Bombieri and van der Poorten [1], Corvaja constructed instead a polynomial in N variables having large index at points $(\alpha_{h1}, \dots, \alpha_{hN})$ with distinct coordinates. We mention that Roth and Bombieri and van der Poorten used Siegel's lemma to construct the auxiliary polynomial, whereas Corvaja used interpolation determinants as introduced by Laurent in transcendence theory. □

The deduction of Theorem 4 from Theorem 7 is pretty much routine but we do not wish to leave the technical details to the reader. Assume Theorem 4 is false. Then there are algebraic number fields K_1, K_2 of degrees $r \geq 1$, $s \geq 1$, respectively, a number δ with $0 < \delta < 1$ and some set $\mathcal{E} \subset \{(i,j) : i = 1, \dots, r,\ j = 1, \dots, s\}$ for which there are infinitely many pairs (α, β) satisfying

$$\prod_{(i,j) \in \mathcal{E}} |\alpha^{(i)} - \beta^{(j)}| \leq M(\beta)^{-2-\delta},\ \mathbf{Q}(\alpha) = K_1,\ \mathbf{Q}(\beta) = K_2,\ M(\beta) \geq M(\alpha)^{c(r,s,\delta)}.$$

Then clearly, there are infinitely many pairs (α,β) with

$$\begin{aligned}\prod_{i=1}^{r}\prod_{j=1}^{s}\min\bigl(1,|\alpha^{(i)}-\beta^{(j)}|\bigr)\le M(\beta)^{-2-\delta}\,,\\ \mathbf{Q}(\alpha)=K_1,\ \mathbf{Q}(\beta)=K_2,\quad M(\beta)\ge M(\alpha)^{c(r,s,\delta)}\,.\end{aligned}\tag{3.5}$$

Let (α,β) be a solution of (3.5). For each $j=1,\ldots,s$, choose $i_j\in\{1,\ldots,r\}$ such that

$$|\alpha^{(i_j)}-\beta^{(j)}|\le|\alpha^{(i)}-\beta^{(j)}|\quad\text{for } i=1,\ldots,r.\tag{3.6}$$

By the triangle inequality, we have $|\alpha^{(i)}-\alpha^{(i_j)}|\le|\alpha^{(i_j)}-\beta^{(j)}|+|\alpha^{(i_j)}-\beta^{(j)}|\le 2|\alpha^{(i)}-\beta^{(j)}|$, so $|\alpha^{(i)}-\beta^{(j)}|\ge\frac12|\alpha^{(i_j)}-\alpha^{(i)}|$. Letting $F(X)=a\cdot\prod_{i=1}^r(X-\alpha^{(i)})$ denote the minimal polynomial of α, its discriminant, which is given by $D(F)=a^{2r-2}\prod_{1\le k<l\le r}(\alpha^{(k)}-\alpha^{(l)})^2$, is a non-zero rational integer. Hence

$$\begin{aligned}\prod_{j=1}^{s}\prod_{i\ne i_j}\min(1,|\alpha^{(i)}-\beta^{(j)}|)&\ge\prod_{j=1}^{s}\prod_{i\ne i_j}\frac{|\alpha^{(i)}-\alpha^{(i_j)}|}{2\max(1,|\alpha^{(i)}|)\max(1,|\alpha^{(i_j)}|)}\\ &\ge\prod_{1\le k<l\le r}\frac{|\alpha^{(k)}-\alpha^{(l)}|}{2\max(1,|\alpha^{(k)}|)\max(1,|\alpha^{(l)}|)}=2^{-\frac{r(r-1)}{2}}\frac{|D(F)|^{1/2}}{M(\alpha)^{r-1}}\\ &\ge 2^{-\frac{r(r-1)}{2}}M(\alpha)^{1-r}\,.\end{aligned}$$

Together with (3.5) this implies

$$\prod_{j=1}^{s}\min(1,|\alpha^{(i_j)}-\beta^{(j)}|)\le 2^{\frac{r(r-1)}{2}}M(\alpha)^{r-1}M(\beta)^{-2-\delta}\,.\tag{3.7}$$

Choose a normal, totally complex extension K of $\mathbf{Q}$ containing K_1K_2. Suppose $[K:\mathbf{Q}]=d$ and let $\sigma_1,\ldots,\sigma_d$ be the isomorphic embeddings of K into $\mathbf{C}$. Then d is even and we may assume without loss of generality that $\sigma_{k+d/2}=\overline{\sigma_k}$ is the complex conjugate of σ_k for $k=1,\ldots,d/2$. Thus, the normalised absolute values on K corresponding to the archimedean places are $||\cdot||_{v_k}=|\sigma_k(\cdot)|^{2/d}$ $(k=1,\ldots,d/2)$. Denote the set of archimedean places $\{v_1,\ldots,v_{d/2}\}$ by S. Put $i_k:=i_j$ if σ_k is a continuation to K of the embedding $\beta\mapsto\beta^{(j)}$ of K_2. (3.6) implies $|\alpha^{(i_k)}-\sigma_k(\beta)|\le|\alpha^{(i)}-\sigma_k(\beta)|$ for $i=1,\ldots,r$, $k=1,\ldots,d$. Hence for $k=1,\ldots,d/2$ we have

$$|\alpha^{(i_{k+d/2})}-\sigma_{k+d/2}(\beta)|=\min_{i=1,\ldots,r}|\overline{\alpha^{(i)}}-\overline{\sigma_k(\beta)}|=|\alpha^{(i_k)}-\sigma_k(\beta)|\,.$$

Now, noting that each map $\beta \mapsto \beta^{(j)}$ can be extended to precisely $[K : K_2] = d/s$ isomorphisms σ_k, we can rewrite (3.7) as

$$\prod_{k=1}^{d/2} \min(1, |\alpha^{(i_k)} - \sigma_k(\beta)|^2) = \prod_{k=1}^{d} \min(1, |\alpha^{(i_k)} - \sigma_k(\beta)|) \\ \leq \left(2^{\frac{r(r-1)}{2}} M(\alpha)^{r-1} M(\beta)^{-2-\delta}\right)^{d/s}$$

and since α has degree $[K_1 : \mathbf{Q}] = r$ and β has degree $[K_2 : \mathbf{Q}] = s$, this can be translated into

$$\prod_{v \in S} \min(1, ||\alpha^{(i_v)} - \beta||_v) \leq 2^{\frac{r(r-1)}{2s}} H(\alpha)^{\frac{r(r-1)}{s}} H(\beta)^{-2-\delta} \tag{3.8}$$

with $\alpha^{(i_v)} := \sigma_k^{-1}(\alpha^{(i_k)})$ if $v = v_k$.

Denote by A the left-hand side of (3.8). Choose $\theta > 0$ sufficiently small. There is a finite set $V \subset [0,1]^{d/2}$ such that for every $(x_v : v \in S) \in [0,1]^{d/2}$ there is a point $(\lambda_v : v \in S) \in V$ with $\lambda_v \leq x_v \leq \lambda_v + \theta$ for $v \in S$. In particular, there is a $(\lambda_v : v \in S) \in V$ with

$$A^{\lambda_v + \theta} \leq \min(1, ||\alpha^{(i_v)} - \beta||_v) \leq A^{\lambda_v} \quad \text{for } v \in S.$$

Clearly,

$$\sum_{v \in S} \lambda_v \geq 1 - s\theta \tag{3.9}$$

and, in view of (3.8),

$$\min(1, ||\alpha^{(i_v)} - \beta||_v) \leq \left(2^{\frac{r(r-1)}{2s}} H(\alpha)^{\frac{r(r-1)}{s}} H(\beta)^{-2-\delta}\right)^{\lambda_v} \quad \text{for } v \in S.$$

Let S' be the set of v with $\lambda_v > 0$ and partition S' into subsets $S_1, \ldots, S_n$ such that v_1, v_2 belong to the same subset if and only if $i_{v_1} = i_{v_2}$. Note that $n \leq r$. Put $i_h := i_v$ for $v \in S_h$. Then finally the latter system of inequalities can be rewritten as

$$||\alpha^{(i_h)} - \beta||_v \leq \left(2^{\frac{r(r-1)}{2s}} H(\alpha)^{\frac{r(r-1)}{s}} H(\beta)^{-2-\delta}\right)^{\lambda_v} \quad \text{for } v \in S_h,\ h = 1, \ldots, n. \tag{3.10}$$

We now pick indices i_v $(v \in S)$ and a tuple $(\lambda_v : v \in S)$ from the finite set V such that (3.5) has infinitely many solutions (α, β) with (3.10). Choose the integer

$$N := [1300\delta^{-2} \log 6r]\,. \tag{3.11}$$

Thus, the condition $N > 36^2 \log 6n$ of Theorem 7 is satisfied. Further we have $A(\beta, \alpha^{(i_1)}, \ldots, \alpha^{(i_n)}) = H(\beta) \cdot (4H(\alpha)^3)^{2N!}$. ¿From the assumptions $M(\beta) \geq M(\alpha)^{c(r,s,\delta)}$, $0 < \delta < 1$ it follows that $H(\beta)^{\delta/3} \geq H(\alpha)^{(2+\frac{1}{2}\delta)6N! + \frac{r(r-1)}{s}}$ and so for $M(\beta)$ sufficiently large we have

$$2^{\frac{r(r-1)}{2s}} H(\alpha)^{\frac{r(r-1)}{s}} H(\beta)^{-2-\delta} \leq A(\beta, \alpha^{(i_1)}, \ldots, \alpha^{(i_n)})^{-2-\delta/2}\,.$$

Further, since $M(\beta) > M(\alpha)$, the number β is not equal to any conjugate of α. By inserting these facts into (3.10), we infer that the system of inequalities

$$0 < ||\alpha^{(i_h)} - \beta||_v \leq A(\beta, \alpha^{(i_1)}, \ldots, \alpha^{(i_n)})^{-\lambda_v(2+\delta/2)} \quad (v \in S_h,\ h = 1, \ldots, n) \tag{3.12}$$

has infinitely many solutions (α, β) with $\mathbf{Q}(\alpha) = K_1$, $\mathbf{Q}(\beta) = K_2$.

We can now apply Theorem 7. From the infinitely many solutions of (3.12) we select N, $(\alpha_1, \beta_1), \ldots, (\alpha_N, \beta_N)$, say, such that $(\beta_k, \alpha_{1k}, \ldots, \alpha_{nk})$ with $\alpha_{hk} = \alpha_k^{(i_h)}$ satisfy (3.3). Thus we have obtained N tuples in K^{n+1} satisfying (3.2), (3.3) and (3.1) with S' replacing S and with $\mu_v = \lambda_v(2+\delta/2)$ for $v \in S'$. From (3.9), (3.11) it follows that for θ sufficiently small,

$$\sum_{v \in S'} \mu_v = \sum_{v \in S'} \lambda_v(2+\delta/2) \geq (1 - s\theta)(2+\delta/2) > 2 + \frac{9\sqrt{\log 6n}}{\sqrt{N}}\,.$$

But this contradicts the conclusion (3.4) of Theorem 7. As we arrived at this contradiction starting with the assumption that Theorem 4 is false, this completes the proof of Theorem 4. $\square$

References

[1] Bombieri, E., Poorten, A.J. van der, Some quantitative results related to Roth's theorem. J. Austral. Math. Soc. (Ser. A) 45 (1988), 233–248.

[2] Corvaja, P., Approximation diophantienne sur la droite, Ph-D dissertation, Paris, 1995.

[3] Evertse, J.-H., Estimates for discriminants and resultants of binary forms. In: Advances in Number Theory, Proc. 3rd conf. CNTA, Kingston 1991 (ed. by F.Q. Gouvêa, N. Yui), 367–380. Clarendon Press, Oxford, 1993.

[4] — Estimates for reduced binary forms. J. reine angew. Math. 434 (1993), 159–190.

[5] — Lower bounds for resultants II. In: Number Theory, Proc. conf. Eger 1996 (ed. by K. Győry, A. Pethő, V. Sós), 181–198. Walter de Gruyter, Berlin, etc. 1998.

[6] — Symmetric improvements of Liouville's inequality. Report no. MI 07–99, Univ. Leiden, 1999. Submitted for publication.

[7] Evertse, J.-H., Győry, K., Lower bounds for resultants I. Compositio Math. 88 (1993), 1–23.

[8] LeVeque, W.J., Topics in Number Theory, vol. II. Addison-Wesley, Reading. Mass. USA 1956.

[9] Roth, K.F., Rational approximation to algebraic numbers. Mathematika 2 (1955), 1–20.

[10] Schmidt, W.M., Diophantine Approximation. Lecture Notes Math. 785. Springer Verlag, Berlin etc. 1980.

[11] — Open problems in Diophantine approximation. In: Approximations Diophantiennes et Nombres Transcendants, Proc. conf. Luminy 1982 (ed. by D. Bertrand, M. Waldschmidt), Progr. Math. 31, 271–287. Birkhäuser, Boston etc. 1983.

[12] Vojta, P., Roth's Theorem with Moving Targets. Intern. Math. Res. Notices 3 (1996), 109–114.

Adress of the author:

Jan-Hendrik Evertse
Universiteit Leiden
Mathematisch Instituut
Postbus 9512
2300 RA Leiden
The Netherlands

E-mail: evertse@wi.leidenuniv.nl