On the multiples of a badly approximable vector

Yann BUGEAUD

Abstract. Let d be a positive integer and α a real algebraic number of degree $d+1$. Set $\underline{\alpha} := (\alpha, \alpha^2, \ldots, \alpha^d)$. It is well-known that the quantity

$$c(\underline{\alpha}) := \liminf_{q \to +\infty} q^{1/d} \cdot \|q\underline{\alpha}\|$$

is positive, where $\|\cdot\|$ denotes the distance to the nearest integer. Furthermore, the inequalities

$$c(\underline{\alpha}) n^{-1/d} \le c(n\underline{\alpha}) \le nc(\underline{\alpha})$$

hold for any integer $n \ge 1$. Our main result asserts that there exists a real number C, depending only on α, such that

$$c(n\underline{\alpha}) \le Cn^{-1/d},$$

for any integer $n \ge 1$.

1. Introduction and results

Let $\|\cdot\|$ denote the distance to the nearest integer. The set ***Bad*** of badly approximable real numbers, defined by

$$\boldsymbol{Bad} = \{\alpha \in \mathbf{R} : \inf_{q \ge 1} q \cdot \|q\alpha\| > 0\},$$

is the set of real numbers whose sequence of partial quotients is infinite and bounded. The Lagrange constant $c(\alpha)$ of an irrational real number α is the quantity

$$c(\alpha) := \liminf_{q \to +\infty} q \cdot \|q\alpha\|.$$

Clearly, a real number α lies in ***Bad*** if, and only if, its Lagrange constant $c(\alpha)$ is positive. A classical theorem of Hurwitz (see e.g. [11, 2]) asserts that $c(\alpha) \le 1/\sqrt{5}$ for every real number α.

2000 *Mathematics Subject Classification :* 11J13. Key words: Lagrange constant, badly approximable vector, simultaneous approximation.

For any positive integer n and any badly approximable real number α, the equalities

$$\left|n\alpha - \frac{np}{q}\right| = n\left|\alpha - \frac{p}{q}\right|$$

and

$$\left|\alpha - \frac{p}{nq}\right| = \frac{1}{n}\left|n\alpha - \frac{np}{nq}\right|$$

imply that the Lagrange constants of α and $n\alpha$ are related by the inequalities

$$\frac{c(\alpha)}{n} \le c(n\alpha) \le nc(\alpha). \tag{1.1}$$

The first general result on the behaviour of the sequence $(c(n\alpha))_{n\ge1}$ is Theorem 1.11 of Einsiedler, Fishman, and Shapira [4], reproduced below.

Theorem EFS. *Every badly approximable real number α satisfies*

$$\inf_{n\ge1} c(n\alpha) = 0. \tag{1.2}$$

At present, we still do not know whether, for every α in $\boldsymbol{Bad}$, the infimum over all positive integers n in (1.2) can be replaced by the limit as n tends to infinity. In this direction, it has been proved in [1] that a much stronger result than (1.2), namely that $\sup_{n\ge1} nc(n\alpha)$ is finite, holds for certain classes of badly approximable real numbers α, whose sequence of partial quotients enjoys specific combinatorial properties. Among other results, the following statement is established in [1].

Theorem BBEK. *Let $(a_k)_{k\ge1}$ be a sequence of positive integers. If there exists an integer $m \ge 0$ and an increasing sequence $(n_j)_{j\ge1}$ of positive integers such that $n_{j+1} > n_j$ and*

$$a_{m+1}\dots a_{m+n_j} = a_{m+n_{j+1}-n_j+1}\dots a_{m+n_{j+1}}, \quad \text{for } j \ge 1,$$

then the real number $\alpha := [0; a_1, a_2, \dots]$ satisfies

$$\sup_{n\ge1} nc(n\alpha) < +\infty. \tag{1.3}$$

In view of the left-hand side inequality of (1.1), the conclusion of Theorem BBEK is nearly best possible. Furthermore, Theorem BBEK applies to every ultimately periodic sequence $(a_k)_{k\ge1}$, hence it shows that (1.3) holds for every real quadratic number α.

The aim of the present note is to investigate a multidimensional extension of the latter result.

Let d be a positive integer. By Dirichlet's theorem, for any d-dimensional real vector $\underline{\alpha} = (\alpha_1, \dots, \alpha_d)$, there are arbitrarily large positive integers q with

$$\|q\underline{\alpha}\| \le q^{-1/d}, \tag{1.4}$$

where we have set $\|q\underline{\alpha}\| := \max_{1\le i\le d}\|q\alpha_i\|$. The set $\boldsymbol{Bad}_d$ of badly approximable d-dimensional real vectors is the set

$$\boldsymbol{Bad}_d = \{\underline{\alpha} = (\alpha_1, \ldots, \alpha_d) \in \mathbf{R}^d : \inf_{q\ge 1} q^{1/d} \cdot \max_{1\le i\le d} \|q\alpha_i\| > 0\}$$

of real vectors such that (1.4) is best possible up to a numerical constant. The set $\boldsymbol{Bad}_d$ has zero Lebesgue measure and full Hausdorff dimension (that is, its Hausdorff dimension is equal to d). If α is a real algebraic number of degree $d+1$, then the vector $\underline{\alpha} := (\alpha, \alpha^2, \ldots, \alpha^d)$ is in $\boldsymbol{Bad}_d$; see e.g. [10]. The definition of the Lagrange constant can be extended in a natural way to real vectors.

Definition 1.1. *Let d be a positive integer. The Lagrange constant $c(\underline{\alpha})$ of a d-dimensional real vector $\underline{\alpha}$ is the quantity*

$$c(\underline{\alpha}) := \liminf_{q\to+\infty} q^{1/d} \cdot \|q\underline{\alpha}\|.$$

Again, noticing that

$$q^{1/d}|q(n\alpha) - np| = nq^{1/d}|q\alpha - p|$$

and

$$(nq)^{1/d}|(nq)\alpha - p| = n^{1/d}q^{1/d}|q(n\alpha) - p|,$$

for all positive integers p, n, q and all real numbers α, we deduce that

$$\frac{c(\underline{\alpha})}{n^{1/d}} \le c(n\underline{\alpha}) \le nc(\underline{\alpha}) \tag{1.5}$$

holds for any integer $n \ge 1$ and any $\underline{\alpha}$ in $\boldsymbol{Bad}_d$.

Our main result asserts that, for every positive integer d, there are elements of $\boldsymbol{Bad}_d$ for which the left-hand side inequality of (1.5) is sharp.

Theorem 1.2. *Let $d \ge 2$ be an integer. Let K be a real algebraic number field of degree $d+1$. Let $\alpha_1, \ldots, \alpha_d$ be in K such that $1, \alpha_1, \ldots, \alpha_d$ are linearly independent over the rationals. Then, there exists a real number C such that*

$$c(n(\alpha_1, \ldots, \alpha_d)) \le \frac{C}{n^{1/d}},$$

for any positive integer n.

The method of the proof of Theorem 1.2 works also for $d = 1$ and allows us to give an alternative proof that

$$\sup_{n\ge 1} nc(n\alpha) < +\infty$$

holds for every real quadratic number α. Unlike in [1], our argument is not based on the continued fraction expansion of α. In addition, the proof in [1] gives that

$$\liminf_{q \to +\infty} q \cdot (\log q) \cdot \|q\alpha\| \cdot |q|_p < +\infty \tag{1.6}$$

holds for every real quadratic number α and every prime number p, a result first established by de Mathan and Teulié [9] using p-adic analysis (see also [6] for a third proof). Here, $|\cdot|_p$ is the p-adic absolute value normalized in such a way that $|p|_p = p^{-1}$. Our method allows us to extend (1.6) as follows.

Theorem 1.3. *Let $d \geq 2$ be an integer. Let K be a real algebraic number field of degree $d+1$. Let $\alpha_1, \ldots, \alpha_d$ be in K such that $1, \alpha_1, \ldots, \alpha_d$ are linearly independent over the rationals. Let p be a prime number. Then,*

$$\liminf_{q \to +\infty} q^{1/d} \cdot (\log q) \cdot \max\{\|q\alpha_1\|, \ldots, \|q\alpha_d\|\} \cdot |q|_p < +\infty. \tag{1.7}$$

A weaker result than Theorem 1.3, namely with the factor $(\log q)$ in (1.7) replaced by $(\log q)^{1/d}$, is a particular case of Théorème 3.1 of [9].

The proof of Theorem 1.2 follows very closely a method developed by Peck [10] to improve and extend a result of Cassels and Swinnerton-Dyer [3] on the Littlewood conjecture in simultaneous Diophantine approximation.

Our paper is organized as follows. A special case of Theorem 1.2 is discussed in Section 2. Theorems 1.2 and 1.3 are then established in Section 3, while some open questions are addressed in the last section.

2. A special case of Theorem 1.2

We start with an auxiliary lemma used in the last part of the proofs.

Lemma 2.1. *Let $(u_n)_{n\geq 1}$ be a recurrence sequence of order d of rational integers. Then, for every prime number p and every positive integer k, the period length of the sequence $(u_n)_{n\geq 1}$ modulo p^k is at most equal to $(p^d - 1)p^{k-1}$. Furthermore, for any integer $\ell \geq 2$, the period length of $(u_n)_{n\geq 1}$ modulo ℓ is at most equal to ℓ^d.*

Proof. For the first statement, see Everest et al. [5] on page 47. If $\ell = p_1^{a_1} \cdots p_m^{a_m}$ for distinct prime numbers $p_1, \ldots, p_m$, then the period length of $(u_n)_{n\geq 1}$ modulo ℓ is at most equal to the product $p_1^{d+a_1-1} \cdots p_m^{d+a_m-1}$, which is bounded from above by ℓ^d. □

We display the following special case of Theorem 1.2.

Theorem 2.2. *Let K be a real cubic number field with two complex (non-real) conjugate embeddings. Let α_1, α_2 be in K such that $1, \alpha_1, \alpha_2$ are linearly independent over the rationals. Then, there exists a real number C such that*

$$c(n(\alpha_1, \alpha_2)) \leq \frac{C}{n^{1/2}},$$

for any positive integer n.

The proof of Theorem 2.2 is much simpler than that of Theorem 1.2 since the unit rank of the number field K is equal to 1. Furthermore, it can be adapted *mutatis mutandis* to the case where K is a real quadratic number field and α is an irrational number in K to show that $\sup_{n\geq 1} nc(n\alpha)$ is finite, a result already proved in [1].

Proof. Set $\alpha_0 = 1$. Let $\mathcal{M}$ be the $\mathbf{Z}$-module generated by $1, \alpha_1$ and α_2. Let $\mathcal{O}$ denote the set of algebraic integers ρ in K such that $\rho\alpha$ is in $\mathcal{M}$ whenever α is in $\mathcal{M}$. Clearly, the set $\mathcal{O}$ is a ring included in $\mathcal{M}$. It is an order in the field K. Let $\varepsilon > 1$ be a unit in $\mathcal{O}$.

The elements δ of K such that the trace of $\alpha\delta$ is a rational integer for every α in $\mathcal{M}$ form a $\mathbf{Z}$-module D. A basis $\delta_0, \delta_1, \delta_2$ of D is obtained by solving the equations

$$\mathrm{Trace}(\alpha_i\delta_j) = 0 \text{ if } i \neq j, \text{ and } \mathrm{Trace}(\alpha_i\delta_j) = 1 \text{ if } i = j.$$

Let t be a positive integer. By our choice of ε, if α is in $\mathcal{M}$, then $\varepsilon^t\alpha$ is also in $\mathcal{M}$ and the trace of $\alpha\varepsilon^t\delta_2$ is a rational integer. Consequently, $\varepsilon^t\delta_2$ lies in D. Write

$$\varepsilon^t\delta_2 = q_{0,t}\delta_0 + q_{1,t}\delta_1 + q_{2,t}\delta_2, \tag{2.1}$$

where $q_{0,t}, q_{1,t}$ and $q_{2,t}$ are rational integers. Observe that

$$q_{k,t} = \mathrm{Trace}(\varepsilon^t\delta_2\alpha_k) = \varepsilon^t\delta_2\alpha_k + \sigma(\varepsilon^t\delta_2\alpha_k) + \overline{\sigma(\varepsilon^t\delta_2\alpha_k)}, \text{ for } k = 0, 1, 2,$$

where σ denotes a complex non-real embedding of K and $\overline{\cdot}$ denotes the complex conjugation. Since ε is a unit, we have $\varepsilon^t|\sigma(\varepsilon^t)|^2 = 1$, thus

$$|\sigma(\varepsilon^t)| = \varepsilon^{-t/2}.$$

Consequently, there are positive constants C_1, C_2, depending only on α_1 and α_2, such that

$$\begin{aligned} |q_{k,t} - q_{0,t}\alpha_k| &= |(\sigma(\alpha_k) - \alpha_k)\sigma(\varepsilon^t\delta_2) + \overline{(\sigma(\alpha_k) - \alpha_k)\sigma(\varepsilon^t\delta_2)}| \\ &\leq C_1\varepsilon^{-t/2}, \end{aligned}$$

for $k = 1, 2$, while

$$|q_{0,t} - \varepsilon^t\delta_2| = |\sigma(\varepsilon^t\delta_2) + \overline{\sigma(\varepsilon^t\delta_2)}| \leq C_2\varepsilon^{-t/2}. \tag{2.2}$$

These inequalities show that there exists a positive constant C_3, depending only on α_1 and α_2, such that

$$|q_{0,t}|^{1/2} \cdot \max\{\|q_{0,t}\alpha_1\|, \|q_{0,t}\alpha_2\|\} \leq C_3, \quad t \geq 0. \tag{2.3}$$

Let $X^3 + a_2X^2 + a_1X + a_0$ denote the minimal defining polynomial of ε, where $a_0 = \pm 1$. In view of (2.1) and setting $q_{0,0} = 0$, the sequence $(q_{0,t})_{t\geq 0}$ satisfies

$$q_{0,t+3} + a_2 q_{0,t+2} + a_1 q_{0,t+1} + a_0 q_{0,t} = 0,$$

for every integer $t \geq 0$. By Lemma 2.1, for every integer $\ell \geq 2$, the sequence $(q_{0,t})_{t\geq 0}$ is periodic modulo ℓ with period length at most equal to ℓ^3. Since $q_{0,0} = 0$, this means that there exists $h \geq 1$ such that ℓ divides $q_{0,ht}$ for every $t \geq 1$. Consequently, we deduce from (2.3) that, upon writing $q'_{0,ht} = q_{0,ht}/\ell$, we have

$$|q'_{0,ht}|^{1/2} \cdot \max\{\|q'_{0,ht}(\ell\alpha_1)\|, \|q'_{0,ht}(\ell\alpha_2)\|\} \leq \frac{C_3}{\ell^{1/2}},$$

for every positive integer t. Since, by (2.2), the integer $q_{0,ht}$ is nonzero for t large enough, we conclude that $c(\ell\alpha_1, \ell\alpha_2) \leq C_3\ell^{-1/2}$ and the proof of Theorem 2.2 is complete. □

Let α_1, α_2 be real numbers in a same cubic field K, such that $1, \alpha_1, \alpha_2$ are linearly independent over the rationals and K has two complex non-real embeddings. The above proof shows how to associate with the pair (α_1, α_2) a linearly recurrent sequence $(q_n)_{n\geq 0}$, an integer n_0 and a positive real number C such that $q_0 = 0$ and

$$\max\{\|q_n\alpha_1\|, \|q_n\alpha_2\|\} \leq C q_n^{-1/2}, \quad n \geq n_0.$$

For an explicit example, let us consider simultaneous rational approximation to $\sqrt[3]{2}$ and $\sqrt[3]{4}$. Then, the proof of Theorem 2.2 shows that there exists $C > 0$ such that the sequence $(q_n)_{n\geq 0}$ starting with

$$0, 1, 4, 15, 58, 223, 858, 3301, 12700, \ldots$$

and defined by the recurrent relation

$$q_{n+3} = 3q_{n+2} + 3q_{n+1} + q_n, \;\; n \geq 0,$$

satisfies

$$\max\{\|q_n\sqrt[3]{2}\|, \|q_n\sqrt[3]{4}\|\} \leq C q_n^{-1/2}, \quad n \geq 1.$$

3. Proofs of Theorems 1.2 and 1.3

We proceed with the proof of Theorem 1.2. As already written, it follows very closely the argument of Peck [10], with some suitable modifications near to the end.

Assume that K has $r+1$ real embeddings and $2s$ complex non-real embeddings numbered in such a way that $K = K^{(0)}$, $K^{(1)}, \ldots, K^{(r)}$ are real and $K^{(r+1)}, \ldots, K^{(r+2s)}$ are complex non-real, with $K^{(r+s+j)} = \overline{K^{(r+j)}}$ for $j = 1, \ldots, s$. Note that $d = r + 2s$. In view of Theorem 2.2, which adresses the case $(r, s) = (0, 1)$, we assume that $r + s \geq 2$.

Let $\mathcal{M}$ denote the $\mathbf{Z}$-module generated by $1, \alpha_1, \ldots, \alpha_d$. Let $\mathcal{O}$ denote the set of algebraic integers ρ in K such that $\rho\alpha$ is in $\mathcal{M}$ whenever α is in M. Clearly, the set $\mathcal{O}$ is a ring included in $\mathcal{M}$. It is an order in the field K. By Dirichlet's Unit Theorem (see, e.g., Theorem 2.8.1 of [7]), there exists an independent family $\varepsilon_1, \ldots, \varepsilon_{r+s}$ of algebraic units in $\mathcal{O}$. In particular, $\varepsilon_k \alpha_i$ is in $\mathcal{M}$ for $k = 1, \ldots, r+s$ and $i = 1, \ldots, d$.

Write
$$C_4 = \max\{2, \max_{1 \leq j,k \leq r+s} |\log|\varepsilon_k^{(j)}||\}.$$

The key ingredient of the proof consists in finding so-called *dominant units*, that is, units $\zeta > 1$, such that every conjugate of ζ, distinct from ζ, has nearly the same modulus $\zeta^{-1/d}$. Note that, for any real number $T \geq dC_4$, there exist rational integers $g_1, \ldots, g_{r+s}$, not all 0, such that

$$-\frac{T}{d} - \frac{C_4}{2} \leq \sum_{k=1}^{r+s} g_k |\log \varepsilon_k^{(j)}| < -\frac{T}{d} + \frac{C_4}{2}, \quad j = 1, \ldots, r+s,$$

which, by the fact that the norm of each unit ε_k is ± 1, also gives that

$$T - \frac{dC_4}{2} \leq \sum_{k=1}^{r+s} g_k |\log \varepsilon_k| < T + \frac{dC_4}{2}.$$

Setting then
$$\zeta := |\varepsilon_1^{g_1} \cdots \varepsilon_{r+s}^{g_{r+s}}|$$
and $C_5 = \mathrm{e}^{C_4}$, we get

$$|\log|\zeta^{1/d}\zeta^{(j)}|| < C_4 \quad \text{and} \quad |\zeta^{(j)}| < C_5 \zeta^{-1/d}, \quad j = 1, \ldots, r+s. \tag{3.1}$$

A unit $\zeta > 1$ satisfying (3.1) is called a dominant unit. The above argument shows that every interval $[T, C_5^d T)$, with $T \geq dC_4$, contains (at least) one dominant unit.

Our aim is to find a dominant unit satisfying a sharper estimate than (3.1).

Let M be a large positive integer. Since each interval of the form $[dC_4C_5^{2jd}, dC_4C_5^{(2j+1)d})$, where j is a non-negative integer, contains a dominant unit, there exist $M+1$ dominant units $\theta_1 < \theta_2 < \ldots < \theta_{M+1}$ in the interval $[dC_4, dC_4 \mathrm{e}^{(2M+1)dC_4})$ which satisfy $\theta_{j+1}/\theta_j \geq C_5^d$, for $j = 1, \ldots, M$. Recalling that $d = r+2s$, it follows from the *Schubfachprinzip* of Dirichlet that there exist two dominant units θ and η such that

$$dC_4 \leq \theta < \eta < dC_4 \mathrm{e}^{(2M+1)dC_4},$$

$$|\log|\eta^{1/d}\eta^{(j)}| - \log|\theta^{1/d}\theta^{(j)}|| < 2C_4 M^{-1/(d-1)}, \quad j = 2, \ldots, r+s.$$

and

$$|\arg \eta^{(j)} - \arg \theta^{(j)}| \leq 2\pi M^{-1/(d-1)}, \quad j = r+1, \ldots, r+s.$$

Setting $N = \mathrm{e}^{2MdC_4} = C_5^{2Md}$, we conclude that the unit $\varepsilon := \eta/\theta$ satisfies $C_5^d \leq \varepsilon < C_5^d N$,

$$|\log|\varepsilon^{1/d}\varepsilon^{(j)}|| < 2(2C_4^d d/\log N)^{1/(d-1)}, \quad j = 2, \ldots, r+s.$$

and

$$|\arg \varepsilon^{(j)}| \leq 2\pi(2C_4 d/\log N)^{1/(d-1)}, \quad j = r+1, \ldots, r+s.$$

Since

$$\sum_{j=1}^{r} \log|\varepsilon^{1/d}\varepsilon^{(j)}| + 2\sum_{j=r+1}^{r+s} \log|\varepsilon^{1/d}\varepsilon^{(j)}| = 0,$$

we deduce that

$$|\log|\varepsilon^{1/d}\varepsilon^{(1)}|| < 2(d-1)(2C_4^d d/\log N)^{1/(d-1)}.$$

It follows that, for $j = 1, \ldots, r+s$, we can write

$$\varepsilon^{(j)} = |\varepsilon^{(j)}|\mathrm{e}^{\mathrm{i}\arg \varepsilon^{(j)}} = \pm \varepsilon^{-1/d}(1+\nu_j),$$

where the complex number ν_j satisfies

$$|\nu_j| < 4(d-1)(2C_4^d d/\log N)^{1/(d-1)},$$

if N is large enough. In particular, for every positive integer t less than $(\log N)^{1/(d-1)}$ times a small positive constant depending only on d, we get

$$|(1+\nu_j)^t| \leq 3, \quad \text{for } j = 1, \ldots, r+s.$$

Let T be a positive integer. The above argument shows that for N sufficiently large in terms of T one can construct a unit ε such that

$$|(\varepsilon^{(j)})^t| \leq 3\varepsilon^{-t/d}, \quad \text{for } 0 \leq t \leq T \text{ and } 1 \leq j \leq r+s. \tag{3.2}$$

Set $\alpha_0 = 1$. Recall that $\mathcal{M}$ denotes the $\mathbf{Z}$-module generated by $1, \alpha_1, \ldots, \alpha_d$. The elements δ of K such that the trace of $\alpha\delta$ is a rational integer for every α in $\mathcal{M}$ form a $\mathbf{Z}$-module D. A basis $\delta_0, \delta_1, \ldots, \delta_d$ of D is obtained by solving the equations

$$\begin{aligned} \operatorname{Trace}(\alpha_i\delta_j) &= 0, \quad \text{if } 0 \leq i \neq j \leq d, \\ \operatorname{Trace}(\alpha_i\delta_j) &= 1, \quad \text{if } i = j = 0, \ldots, d. \end{aligned}$$

Let t be an integer. Our choice of $\varepsilon_1, \ldots, \varepsilon_{r+s}$ shows that ε^t lies in the order $\mathcal{O}$. Consequently, if α is in $\mathcal{M}$, then $\varepsilon^t\alpha$ is also in $\mathcal{M}$ and the trace of $\alpha\varepsilon^t\delta_d$ is a rational integer. Consequently, $\varepsilon^t\delta_d$ lies in D. Write

$$\varepsilon^t\delta_d = q_{0,t}\delta_0 + q_{1,t}\delta_1 + \cdots + q_{d,t}\delta_d, \tag{3.3}$$

where $q_{0,t}, \ldots, q_{d,t}$ are rational integers. Observe that

$$q_{k,t} = \operatorname{Trace}(\varepsilon^t\delta_d\alpha_k) = \varepsilon^t\delta_d\alpha_k + \sum_{j=1}^{d} \alpha_k^{(j)}\delta_d^{(j)}(\varepsilon^{(j)})^t, \;\; \text{for } k = 1, \ldots, d, \tag{3.4}$$

and, recalling that $\alpha_0 = 1$,

$$q_{0,t} = \operatorname{Trace}(\varepsilon^t\delta_d) = \varepsilon^t\delta_d + \sum_{j=1}^{d} \delta_d^{(j)}(\varepsilon^{(j)})^t. \tag{3.5}$$

Consequently, by (3.2), (3.4), (3.5), for $k = 1, \ldots, d$ and $0 \leq t \leq T$, we have

$$\begin{aligned} |q_{k,t} - q_{0,t}\alpha_k| &= \Big|\sum_{j=1}^{d} (\alpha_k^{(j)} - \alpha_k)\delta_d^{(j)}(\varepsilon^{(j)})^t\Big| \\ &\leq 3\Big(\sum_{j=1}^{d} |(\alpha_k^{(j)} - \alpha_k)\delta_d^{(j)}|\Big)\varepsilon^{-t/d}. \end{aligned} \tag{3.6}$$

Since, likewise, we have

$$|q_{0,t} - \varepsilon^t\delta_d| = \Big|\sum_{j=1}^{d} \delta_d^{(j)}(\varepsilon^{(j)})^t\Big| \leq 3\Big(\sum_{j=1}^{d} |\delta_d^{(j)}|\Big)\varepsilon^{-t/d}, \tag{3.7}$$

it follows from (3.6) and (3.7) that there exists a positive constant C_6, depending only on $\alpha_1, \ldots, \alpha_d$, such that

$$|q_{0,t}|^{1/d} \cdot \max\{\|q_{0,t}\alpha_1\|, \ldots, \|q_{0,t}\alpha_d\|\} \leq C_6, \quad 0 \leq t \leq T. \tag{3.8}$$

Let f denote the degree of ε and

$$X^{f+1} + a_f X^f + \ldots + a_1 X + a_0$$

denote its minimal defining polynomial, where $a_0 = \pm 1$. In view of (3.3), the integers $q_{0,0}, \ldots, q_{0,T}$ satisfy

$$q_{0,t+f+1} + a_d q_{0,t+f} + \ldots + a_1 q_{0,t+1} + a_0 q_{0,t} = 0,$$

for $t = 0, \ldots, T - f - 1$. Let $\ell \geq 2$ be an integer. By Lemma 2.1, the sequence $(q_{0,t})_{0 \leq t \leq T}$ is periodic modulo ℓ with period length at most equal to ℓ^{f+1}. Since $q_{0,0} = 0$ and $f \leq d$, it implies that there exists $h \geq 1$ such that $1 \leq h \leq \ell^{d+1}$ and ℓ divides $q_{0,ht}$, for every $t \geq 1$ with $ht \leq T - d - 1$.

Consequently, by (3.8), the integer $|q_{0,ht}|/\ell$ satisfies the inequality

$$q^{1/d} \cdot \max\{\|q(\ell\alpha_1)\|, \ldots, \|q(\ell\alpha_d)\|\} \leq \frac{C_6}{\ell^{1/d}},$$

for every integer t with $1 \leq t \leq (T - d - 1)/h$. By (3.7) and the fact that ε^t tends to infinity as t tends to infinity (recall that $\varepsilon \geq C_5^d$), the integer $q_{0,ht}$ is nonzero for every integer t greater than some integer t_0, depending only on $\alpha_1, \ldots, \alpha_d$. Since N and T can be chosen arbitrarily large, this shows that the Lagrange constant of the d-tuple $(\ell\alpha_1, \ldots, \ell\alpha_d)$ is at most equal to $C_6 \ell^{-1/d}$. The proof of Theorem 1.2 is complete.

Let p be a prime number and m be a positive integer. For the proof of Theorem 1.3, we follow exactly the same lines as for the proof of Theorem 1.2 and take for ℓ the integer p^m. By Lemma 2.1 and the fact that $q_{0,0} = 0$, there exists an integer h such that $1 \leq h \leq p^{m+d}$ and p^m divides $q_{0,h}$. We take for h the largest integer with these properties and we observe that $h \geq p^{m+d}/2$. Since, by (3.7), the integer $q_{0,t}$ is nonzero for every integer t greater than some integer t_0, depending only on $\alpha_1, \ldots, \alpha_d$, we deduce that $q_{0,h}$ is nonzero if m is large enough.

Furthermore, we deduce from (3.7) that there exists a real number $C_7 > 1$ such that $|q_{0,t}| \leq C_7^t$ for $t = 0, \ldots, T$. Combined with (3.8), this gives

$$|q_{0,h}|^{1/d} \cdot (\log |q_{0,h}|) \cdot \max\{\|q_{0,h}\alpha_1\|, \ldots, \|q_{0,h}\alpha_d\|\} \cdot |q_{0,h}|_p \leq p^d C_6 (\log C_7),$$

since $\log |q_{0,h}| < p^{m+d} \log C_7$. The same argument can be applied with the proof of Theorem 2.2. This completes the proof of Theorem 1.3.

4. Open questions

We formulate the open problem mentioned after the statement of Theorem EFS.

Problem 4.1. *Prove or disprove that every badly approximable real number α satisfy*

$$\lim_{n\to+\infty} c(n\alpha) = 0. \tag{4.1}$$

As noted in [1], a proof of (4.1) would imply the proof of the mixed Littlewood conjecture [9].

Theorem EFS suggests the following problem.

Problem 4.2. *To find suitable assumptions on the infinite set $\mathcal{N}$ of positive integers under which every badly approximable real number α satisfies*

$$\inf_{n\in\mathcal{N}} c(n\alpha) = 0.$$

We may also consider the following extension of (4.1). Let $\Gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be an integral matrix with non-zero discriminant $\det\Gamma = ad-bc$ and put

$$\Gamma\alpha = \frac{a\alpha+b}{c\alpha+d}.$$

It is proved in [8] that

$$\frac{c(\alpha)}{|\det\Gamma|} \le c(\Gamma\alpha) \le |\det\Gamma|\, c(\alpha).$$

Problem 4.3. *To find explicit examples of irrational real numbers α such that the quantity*

$$|\det(\Gamma)|\, c(\Gamma\cdot\alpha)$$

is bounded independently of the regular 2×2 integer matrix Γ.

In [1], we have considered the family of matrices $\begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix}$, $n\ge 1$.

We end this section with a metrical question.

Problem 4.4. *Let d be a positive integer. To determine the Hausdorff dimension of the set of vectors $\underline{\alpha}$ such that*

$$\sup_{n\ge 1} n^{1/d}\, c(n\underline{\alpha}) < +\infty.$$

and the Hausdorff dimension of the set of vectors $\underline{\alpha}$ such that

$$\sup_{n\ge 1} n^{1/d}\, c(n\underline{\alpha}) = +\infty.$$

Acknowledgements. I am thankful to the referee for a very careful reading.

References

[1] D. Badziahin, Y. Bugeaud, M. Einsiedler and D. Kleinbock, *On the complexity of a putative counterexample to the p-adic Littlewood conjecture*. Preprint.

[2] Y. Bugeaud, Approximation by algebraic numbers. Cambridge Tracts in Mathematics 160, Cambridge, 2004.

[3] J. W. S. Cassels and H. P. F. Swinnerton-Dyer, *On the product of three homogeneous linear forms and indefinite ternary quadratic forms*, Philos. Trans. Roy. Soc. London, Ser. A, 248 (1955), 73–96.

[4] M. Einsiedler, L. Fishman, and U. Shapira, *Diophantine approximation on fractals*, Geom. Funct. Anal. 21 (2011), 14–35.

[5] G. Everest, A. van der Poorten, I. Shparlinski, and T. Ward, Recurrence sequences. Mathematical Surveys and Monographs, 104. American Mathematical Society, Providence, RI, 2003.

[6] A. Haynes and S. Munday, *Diophantine approximation and coloring*, Amer. Math. Monthly. To appear.

[7] H. Koch, Number theory. Algebraic numbers and functions. Translated from the 1997 German original by David Kramer. Graduate Studies in Mathematics, 24. American Mathematical Society, Providence, RI, 2000.

[8] J. C. Lagarias and J. O. Shallit, *Linear fractional transformations of continued fractions with bounded partial quotients*, J. Théor. Nombres Bordeaux 9 (1997), 267–279; Correction: J. Théor. Nombres Bordeaux 15 (2003), 741–743.

[9] B. de Mathan et O. Teulié, *Problèmes diophantiens simultanés*, Monatsh. Math. 143 (2004), 229–245.

[10] L. G. Peck, *Simultaneous rational approximations to algebraic numbers*, Bull. Amer. Math. Soc. 67 (1961), 197–201.

[11] O. Perron, Die Lehre von den Ketterbrüchen. Teubner, Leipzig, 1929.

Yann Bugeaud
Université de Strasbourg
Mathématiques
7, rue René Descartes
67084 STRASBOURG Cedex (France)

`bugeaud@math.unistra.fr`