GEOMETRY OF NUMBERS D

Tapani Matala-aho, Aalto University, 2023

Upper bound for a linear form

Theorem 1

Let

$$\alpha_1, ..., \alpha_m \in \mathbb{R}, \qquad h_1, ..., h_m \in \mathbb{Z}^+$$

be given. Then there exist $p, q_1, ..., q_m \in \mathbb{Z}$ *with a* $q_k \neq 0$*, satisfying*

$$|q_i| \leq h_i, \quad i = 1, ..., m,$$

and

$$|p + q_1\alpha_1 + ... + q_m\alpha_m| < \frac{1}{h_1 \cdots h_m}.$$

Upper bound for a linear form

Proof. Write

$$L_0\overline{x} := x_0 + \alpha_1 x_1 + \ldots + \alpha_m x_m,$$

$$L_k\overline{x} := x_k, \quad k = 1, \ldots, m$$

and put

$$|L_0\overline{x}| < \frac{1}{h} := \frac{1}{h_1 \cdots h_m}, \tag{1}$$

$$|L_k\overline{x}| \leq h_k + 1/2, \quad k = 1, \ldots, m. \tag{2}$$

Upper bound for a linear form

Then $(L_0, L_1, ..., L_m) : \mathbb{Z}^{m+1} \to \mathbb{R}^{m+1}$ defines a full lattice

$$\Lambda := \mathbb{Z}\bar{\ell}_0 + \mathbb{Z}\bar{\ell}_1 + ... + \mathbb{Z}\bar{\ell}_m =$$

$$\mathbb{Z}(1,0,...,0)^t + \mathbb{Z}(\alpha_1,1,0,...,0)^t + ... + \mathbb{Z}(\alpha_m,0,...,1)^t \subseteq \mathbb{R}^{m+1},$$

where we should find a non-zero vector

$$(p + q_1\alpha_1 + ... + q_m\alpha_m, q_1, \ldots, q_m)^t =$$

$$p(1,0,...,0)^t + q_1(\alpha_1,1,0,...,0)^t + ... + q_m(\alpha_m,0,...,1)^t.$$

Upper bound for a linear form

Lattice determinant:

$$\det\Lambda = \left|\det(\overline{\ell}_0\ \overline{\ell}_1 \ldots \overline{\ell}_m)\right| = \begin{vmatrix} 1 & \alpha_1 & \alpha_2 & \ldots & \alpha_m \\ 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ . & . & . & \ldots & . \\ 0 & 0 & 0 & \ldots & 1 \end{vmatrix} = 1. \qquad (3)$$

Upper bound for a linear form

Now the conditions (1) and (2) determine a convex set

$$\mathcal{C} := \{(y_0, ..., y_m)^t \,|\; |y_0| < 1/h,\; |y_k| \leq h_k + 1/2\} \subseteq \mathbb{R}^{m+1}$$

with volume

$$\operatorname{vol}\mathcal{C} = \frac{2^{m+1}(h_1 + 1/2)\cdots(h_m + 1/2)}{h_1 \cdots h_m} > 2^{m+1} \det \Lambda.$$

By the first Minkowski's convex body there exists a non-zero vector

$$\overline{0} \neq \overline{y} = (p + q_1\alpha_1 + ... + q_m\alpha_m, q_1, ..., q_m)^t \in \mathcal{C} \cap \Lambda. \tag{4}$$

Upper bound for a linear form

such that

$$|q_i| \leq h_i, \quad \forall i = 1, ..., m,$$

and

$$|p + q_1\alpha_1 + ... + q_m\alpha_m| < \frac{1}{h_1 \cdots h_m}, \tag{5}$$

where by (4) we have

$$(p, q_1, ..., q_m)^t \in \mathbb{Z}^{m+1} \setminus \{\bar{0}\}.$$

Finally, if all $q_1 = ... = q_m = 0$ in (5), then also $p = 0$. A contradiction. □

Primitive vector

An integer vector

$$(r_0, r_1, \ldots, r_m)^t \in \mathbb{Z}^{m+1}$$

is *primitive*, if the greatest common divisor satisfies

$$\gcd(r_0, r_1, \ldots, r_m) = 1.$$

Let

$$\gcd(p, q_1, \ldots, q_m) = d \in \mathbb{Z}_{\geq 2}$$

Primitive vector

and suppose the integer vector

$$(p, q_1, ..., q_m)^t = d(s, r_1, ..., r_m)^t, \quad (s, r_1, ..., r_m)^t \in \mathbb{Z}^{m+1},$$

satisfies the estimate

$$|p + q_1\alpha_1 + ... + q_m\alpha_m| < \frac{1}{h}.$$

Then

$$|s + r_1\alpha_1 + ... + r_m\alpha_m| < \frac{1}{dh} < \frac{1}{h}.$$

Primitive vector

Thus we have also a primitive solution

$$(s, r_1, ..., r_m)^t \in \mathbb{Z}^{m+1}$$

for equation

$$|p + q_1\alpha_1 + ... + q_m\alpha_m| < \frac{1}{h}.$$

Primitive vector

Theorem 2

Let $\alpha_1, ..., \alpha_m \in \mathbb{R}$ *and* $h_1, ..., h_m \in \mathbb{Z}^+$ *be given. Then there exist a primitive vector*

$$(p, q_1, ..., q_m)^t \in \mathbb{Z}^{m+1} \setminus \{\overline{0}\}$$

with a $q_k \neq 0$, *satisfying*

$$|q_i| \leq h_i, \quad \forall i = 1, ..., m,$$

and

$$|p + q_1\alpha_1 + ... + q_m\alpha_m| < \frac{1}{h_1 \cdots h_m}.$$

Dirichlet's theorem

Theorem 2 with $m = 1$:

Corollary 3

Let $\alpha \in \mathbb{R}, h \in \mathbb{Z}^+$ be given. Then there exist $p, q \in \mathbb{Z}$, such that

$$1 \leq q \leq h, \quad p \perp q,$$

and

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{qh}.$$

$sa + tb = 1$

Theorem 2 with $m = 1$:

Corollary 4

Let $a \in \mathbb{Z}$, $b \in \mathbb{Z}^+$, $a \perp b$, $b \geq a + 1$ *be given. Then there exist* $s, t \in \mathbb{Z}$ *such that*

$$1 \leq |s| \leq b - 1, \quad s \perp t,$$

and

$$sa + tb = 1. \tag{6}$$

$sa + tb = 1$

Proof. Denote

$$\alpha := \frac{a}{b}, \quad b = h + 1, \; h \geq 1. \tag{7}$$

By Theorem 2 there exist $p, q \in \mathbb{Z}$ such that

$$|p + q\alpha| < \frac{1}{h}, \qquad p \perp q, \quad 1 \leq q \leq h. \tag{8}$$

It follows

$$|pb + qa| < \frac{h+1}{h} \leq 2. \tag{9}$$

Hence

$$|pb + qa| \leq 1. \tag{10}$$

$sa + tb = 1$

If $pb + qa = 0$, then $b|q$. But $b = h + 1$ and $q \leq h$. A contradiction. Thus

$$|pb + qa| = 1, \tag{11}$$

Which means that there exist $s, t \in \mathbb{Z}$ such that

$$1 \leq |s| \leq b - 1, \quad s \perp t,$$

and

$$sa + tb = 1. \quad \square \tag{12}$$

Infiniteness of primitive solutions

Theorem 5

Let $1, \alpha_1, ..., \alpha_m \in \mathbb{R}$ *be linearly independent over* $\mathbb{Q}$. *Then there exist infinitely many primitive vectors*

$$\overline{v}_k = (p_k, q_{1,k}, ..., q_{m,k})^t \in \mathbb{Z}^{m+1} \setminus \{\overline{0}\} \tag{13}$$

satisfying

$$|p_k + q_{1,k}\alpha_1 + ... + q_{m,k}\alpha_m| < \frac{1}{h_{1,k} \cdots h_{m,k}} := \frac{1}{h_k}, \tag{14}$$

with $h_{i,k} := \max\{1, |q_{i,k}|\}$, *for i=1,...,m.*

Infiniteness of primitive solutions

Proof. Suppose on the contrary, that there exist only finitely many primitive solutions for (14). Then by the linear independence and assumption (13) there exists a minimum

$$\min |p_k + q_{1,k}\alpha_1 + \dots + q_{m,k}\alpha_m| := \frac{1}{R} > 0. \tag{15}$$

Choose then

$$\hat{h}_i \in \mathbb{Z}^+, \quad \hat{h} := \hat{h}_1 \cdots \hat{h}_m, \quad \frac{1}{\hat{h}} \leq \frac{1}{R}.$$

Infiniteness of primitive solutions

Now by Theorem 2 there exists a primitive solution

$$(\hat{p}, \hat{q}_1, ..., \hat{q}_m)^t \in \mathbb{Z}^{m+1} \setminus \{\bar{0}\}$$

with

$$\max\{1, |\hat{q}_i|\} \leq \hat{h}_i, \quad \forall i = 1, ..., m,$$

satisfying

$$|\hat{p} + \hat{q}_1\alpha_1 + ... + \hat{q}_m\alpha_m| < \frac{1}{\hat{h}} \leq \frac{1}{R}.$$

which contradicts (15). □

Lower bounds

Theorem 6

Let $1, \alpha_1, ..., \alpha_m \in \mathbb{R}$ *be linearly independent over* $\mathbb{Q}$*. If there exist positive constants* $c, \omega \in \mathbb{R}^+$ *such that*

$$|\beta_0 + \beta_1\alpha_1 + ... + \beta_m\alpha_m| \geq \frac{c}{(h_1 \cdots h_m)^\omega} \tag{16}$$

holds for all

$$(\beta_0, \beta_1, ..., \beta_m) \in \mathbb{Z}^{m+1} \setminus \{\overline{0}\}, \quad h_k = \max\{1, |\beta_k|\},$$

then

$$\omega \geq 1. \tag{17}$$

Lower bounds

Assume on the contrary that

$$\omega < 1.$$

By Theorem 5 there exists an infinity of primitive vectors satisfying

$$|p_k + q_{1,k}\alpha_1 + \ldots + q_{m,k}\alpha_m| < \frac{1}{h_{1,k} \cdots h_{m,k}}$$

and by (16) we have

$$\frac{c}{(h_{1,k} \cdots h_{m,k})^{\omega}} \leq |p_k + q_{1,k}\alpha_1 + \ldots + q_{m,k}\alpha_m| < \frac{1}{h_{1,k} \cdots h_{m,k}}. \qquad (18)$$

Choose now $h_{1,k}, \ldots, h_{m,k}$ such that

$$(h_{1,k} \cdots h_{m,k})^{1-\omega} \geq \frac{1}{c}.$$

A contradiction with (18).

Lower bounds

Usually, in the existing literature, the above results are only given in terms of

$$H_k := \max_{i=1,\dots,m} |q_{i,k}|.$$

Theorem 7

Let $1, \alpha_1, \dots, \alpha_m \in \mathbb{R}$ be linearly independent over $\mathbb{Q}$. Then there exist infinitely many primitive vectors $\overline{v}_k = (p_k, q_{1,k}, \dots, q_{m,k})^t \in \mathbb{Z}^{m+1} \setminus \{\overline{0}\}$ satisfying

$$|p_k + q_{1,k}\alpha_1 + \dots + q_{m,k}\alpha_m| < \frac{1}{H_k^m}. \tag{19}$$

Lower bounds

One may wonder, if the exponent in (19) could be improved? Theorem 8 shows that the upper bound in (19) is best possible up to a constant factor for an arbitrary m-tuple $(\alpha_1, ..., \alpha_m)$ of real numbers.

Lower bounds

Theorem 8

Let $\alpha = \alpha_0$ *be an algebraic integer of degree* $\deg_{\mathbb{Q}} \alpha = m + 1$ *and* $\alpha_i = \sigma_i(\alpha)$, $i = 0, 1, ..., m$, *where* σ_i *are the field monomorphisms of the field* $\mathbb{Q}(\alpha)$. *Then*

$$|p + q_1\alpha + ... + q_m\alpha^m| > \frac{1}{H^m (3m)^m A^{m^2}}, \quad A = \max_{i=0,1,...,m}\{1, |\alpha_i|\}, \quad (20)$$

for all

$$(p, q_1, ..., q_m)^t \in \mathbb{Z}^{m+1}, \quad 1 \leq H = \max_{i=1,...,m} |q_i|.$$

Lower bounds

We divide the proof in two cases. If $|p + q_1\alpha + \ldots + q_m\alpha^m| \geq 1$, we are done. From now on we suppose $|p + q_1\alpha + \ldots + q_m\alpha^m| < 1$. Immediately

$$|p| < 1 + |q_1\alpha + \ldots + q_m\alpha^m| \leq 1 + mH \max\{1, |\alpha|\}^m$$

implying

$$\begin{aligned} |p + q_1\alpha_i + \ldots + q_m\alpha_i^m| &< |p| + |q_1\alpha_i + \ldots + q_m\alpha_i^m| \\ &\leq 1 + mH \max\{1, |\alpha|\}^m + mH \max\{1, |\alpha_i|\}^m \\ &\leq 3mH \left(\max_{i=0,1,\ldots,m} \{1, |\alpha_i|\} \right)^m \\ &= 3mHA^m \end{aligned}$$

Lower bounds

Because $\alpha = \alpha_0$ is an algebraic integer of degree $\deg_{\mathbb{Q}} \alpha = m + 1$, then

$$\Theta := p + q_1\alpha + ... + q_m\alpha^m \in \mathbb{Z}[\alpha] \setminus \{0\}$$

is a non-zero algebraic integer and its field norm is an integer. Hence

$$\begin{aligned} 1 \le |N(\Theta)| &= |\Theta_0\Theta_1 \cdots \Theta_m| \\ &\le |\Theta| \prod_{i=1}^{m} |p + q_1\alpha_i + ... + q_m\alpha_i^m| \\ &\le |\Theta| \, (3mH)^m A^{m^2}. \qquad \square \end{aligned}$$

Lower bounds

Theorem 9

Let $1, \alpha_1, ..., \alpha_m \in \mathbb{R}$ *be linearly independent over* $\mathbb{Q}$*. If there exist positive constants* $c, \omega \in \mathbb{R}^+$ *such that*

$$|p_k + q_{1,k}\alpha_1 + ... + q_{m,k}\alpha_m| > \frac{c}{H_k^{\omega}}$$

for all

$$\overline{v}_k = (p_k, q_{1,k}, ..., q_{m,k})^t \in \mathbb{Z}^{m+1}, \quad 1 \le H_k = \max|q_{i,k}|,$$

then

$$\omega \ge m.$$

Lower contra upper

$$\frac{1}{H^{m+\frac{m\log(3m)+m^2\log A}{\log H}}} \underset{\forall}{<} \left|p+q_1\alpha+\ldots+q_m\alpha^m\right| \underset{\#=\infty}{<} \frac{1}{H^m}. \tag{21}$$

$$\frac{1}{H^{m+\frac{m^2\log m}{\log\log H}}} \underset{\forall}{<} \left|p+q_1 e+q_2 e^2+\cdots+q_m e^m\right| \underset{\#=\infty}{<} \frac{1}{H^m}. \tag{22}$$

a.a.

Theorem 10

For almost all $\alpha_1, \dots, \alpha_m \in \mathbb{R}$ wrt Lebesgue measure, there exist infinitely many primitive vectors $\overline{v}_k = (p_k, q_{1,k}, \dots, q_{m,k})^t \in \mathbb{Z}^{m+1} \setminus \{\overline{0}\}$, with $H_k := \max |q_{i,k}|,\ i = 1, \dots, m$, satisfying

$$|p_k + q_{1,k}\alpha_1 + \dots + q_{m,k}\alpha_m| < \frac{1}{H_k^m \log H_k}. \tag{23}$$

Further (23) is the best bound for a.a.

By (20) we know that (23) is not valid for all m-tuples $(\alpha_1, \dots, \alpha_m)$ of real numbers.

Simultaneous approximations

Theorem 11

Let $\alpha_1, ..., \alpha_m, f_1, ..., f_m \in \mathbb{R},\ h \in \mathbb{Z}_{\geq 1},$ *be given and suppose*

$$f_1 + ... + f_m = 1. \tag{24}$$

Then there exist a primitive vector $(q, p_1, ..., p_m)^t \in \mathbb{Z}^{m+1} \setminus \{\bar{0}\}$ *such that* $1 \leq q \leq h$ *and*

$$|q\alpha_i + p_i| < \frac{1}{h^{f_i}} \quad \forall\ i = 1, ..., m. \tag{25}$$

Simultaneous approximations

Write

$$L_0\overline{x} := x_0,$$

$$L_i\overline{x} := x_0\alpha_i + x_i, \quad i = 1, ..., m$$

and put

$$|L_0\overline{x}| \leq h + 1/2, \tag{26}$$

$$|L_i\overline{x}| < \frac{1}{h^{f_i}}, \quad i = 1, ..., m. \tag{27}$$

Simultaneous approximations

Then $(L_0, L_1, ..., L_m) : \mathbb{Z}^{m+1} \rightarrow \mathbb{R}^{m+1}$ defines a full lattice

$$\Lambda := \mathbb{Z}\bar{\ell}_0 + \mathbb{Z}\bar{\ell}_1 + ... + \mathbb{Z}\bar{\ell}_m =$$

$$\mathbb{Z}(1, \alpha_1, ..., \alpha_m)^t + \mathbb{Z}(0, 1, 0, ..., 0)^t + ... + \mathbb{Z}(0, ..., 0, 1)^t \subseteq \mathbb{R}^{m+1},$$

where we should find a non-zero vector

$$(q, q\alpha_1 + p_1, \ldots, q\alpha_m + p_m)^t =$$

$$q(1, \alpha_1, ..., \alpha_m)^t + p_1(0, 1, 0, ..., 0)^t + ... + p_m(0, \ldots, 0, 1)^t$$

satisfying (25).

Simultaneous approximations

Lattice determinant:

$$\det \Lambda = \left|\det(\overline{\ell}_0\ \overline{\ell}_1 \dots \overline{\ell}_m)\right| = \begin{vmatrix} 1 & 0 & 0 & \dots & 0 \\ \alpha_1 & 1 & 0 & \dots & 0 \\ \alpha_2 & 0 & 1 & \dots & 0 \\ . & . & . & \dots & . \\ \alpha_m & 0 & 0 & \dots & 1 \end{vmatrix} = 1. \tag{28}$$

Note, that the matrices (3) and (28) are transposes to each other.

Simultaneous approximations

Therefore we define a set

$$\mathcal{C} = \{(x_0, x_1, ..., x_m)^t \in \mathbb{R}^{m+1} \big| \ |x_0| \le h+1/2, \ |x_0\alpha_i + x_i| < \frac{1}{h^{f_i}}, \ i = 1, ..., m\}.$$

The set $\mathcal{C}$ is a central symmetric convex body and its volume satisfies

$$\operatorname{vol} \mathcal{C} = (2h+1)\frac{2}{h^{f_1}} \cdots \frac{2}{h^{f_m}} > 2^{m+1} \det \Lambda.$$

Simultaneous approximations

The first Minkowski's convex body theorem gives a vector

$$\overline{0} \neq q(1, \alpha_1, ..., \alpha_m)^t + p_1(0, 1, 0, ..., 0)^t + ... + p_m(0, \ldots, 0, 1)^t \in \mathcal{C} \cap \Lambda.$$

Hence we have a $(m+1)$-tuple

$$(q, p_1, ..., p_m) \in \mathbb{Z}^{m+1} \setminus \{\overline{0}\}$$

satisfying the inequalities (25). □

Infiniteness of primitive solutions

Theorem 12

Let $f_1, \ldots, f_m \in \mathbb{R}^+$ satisfy $f_1 + \ldots + f_m = 1$, and let at least one of the numbers $\alpha_1, \ldots, \alpha_m \in \mathbb{R}$ be irrational. Then there exist infinitely many primitive vectors

$$\overline{v}_k = (q_k, p_{1,k}, \ldots, p_{m,k})^t \in \mathbb{Z}^{m+1} \setminus \{\overline{0}\}, \quad q_k \in \mathbb{Z}^+,$$

satisfying

$$|q_k \alpha_i + p_{i,k}| < \frac{1}{q_k^{f_i}}, \quad \forall\ i = 1, \ldots, m. \tag{29}$$

Infiniteness of primitive solutions

Proof. Let α_2 be irrational. If there were only finitely many primitive solutions for (29), then there exists a minimum

$$\min_k |q_k\alpha_2 + p_{2,k}| := \frac{1}{R} > 0. \tag{30}$$

Choose then

$$\hat{h} \in \mathbb{Z}^+, \quad \frac{1}{\hat{h}^{f_2}} \leq \frac{1}{R}.$$

Now by Theorem 11 there exist $\hat{q}, \hat{p}_2 \in \mathbb{Z}$ such that

$$|\hat{q}\alpha_2 + \hat{p}_2| < \frac{1}{\hat{h}^{f_2}} \leq \frac{1}{R}. \tag{31}$$

which contradicts (30). □

Dirichlet's theorem on simultaneous approximations

Theorem 13

Let $\alpha_1, \ldots, \alpha_m \in \mathbb{R}$ *be given. Then there exist a primitive vector* $(q, p_1, \ldots, p_m)^t \in \mathbb{Z}^{m+1} \setminus \{\overline{0}\}$ *such that* $q \in \mathbb{Z}^+$ *and*

$$\left|\alpha_i + \frac{p_i}{q}\right| < \frac{1}{q^{1+1/m}}, \quad \forall\ i = 1, \ldots, m. \tag{32}$$

Dirichlet's theorem on simultaneous approximations

Theorem 14

Let at least one of the numbers $\alpha_1, ..., \alpha_m \in \mathbb{R}$ be irrational. Then there exist infinitely many primitive vectors

$$\overline{v}_k = (q_k, p_{1,k}, ..., p_{m,k})^t \in \mathbb{Z}^{m+1} \setminus \{\overline{0}\}, \quad q_k \in \mathbb{Z}^+,$$

satisfying

$$\left|\alpha_i + \frac{p_{i,k}}{q_k}\right| < \frac{1}{q_k^{1+1/m}}, \quad \forall\ i = 1, ..., m. \tag{33}$$

Nearest integer

We will use the notation $\|\alpha\|_m = \|\alpha\|$ for the distance of a real number α to the nearest integer

$$\|\alpha\|_m = \min_{k \in \mathbb{Z}} |\alpha - k|.$$

Note, that

$$\|\alpha\|_m \leq |\alpha - k|,$$

for all $k \in \mathbb{Z}$.

Simultaneous linear forms/Infinity of primitive solutions

Let at least one of the numbers $\alpha_1, ..., \alpha_m \in \mathbb{R}$ be irrational. Then there exist infinitely many primitive vectors

$$(q, p_1, ..., p_m)^t \in \mathbb{Z}^{m+1} \setminus \{\bar{0}\}, \quad q \in \mathbb{Z}^+,$$

satisfying

$$|q\alpha_i + p_i| < \frac{1}{q^{1/m}}, \quad \forall\ i = 1, ..., m, \tag{34}$$

or

$$q^{1/m}\|q\alpha_i\| < 1, \quad \forall\ i = 1, ..., m. \tag{35}$$

Case $m = 2$

Set $m = 2$ and let at least one of the numbers $\alpha, \beta \in \mathbb{R}$ be irrational. Then there exist infinitely many solutions $q \in \mathbb{Z}^+$ to

$$\begin{aligned} q^{1/2}\|q\alpha\| &< 1; \\ q^{1/2}\|q\beta\| &< 1. \end{aligned} \tag{36}$$

Hence also for

$$q\,\|q\alpha\|\,\|q\beta\| < 1 \tag{37}$$

without any assumption on the pair (α, β).

Littlewood conjecture

Define a Littlewood quantity

$$\ell(\alpha, \beta) = \inf_{q \in \mathbb{Z}_{\geq 1}} \{q \, \|q\alpha\| \, \|q\beta\|\}.$$

LITTLEWOOD CONJECTURE:

Let $(\alpha, \beta) \in \mathbb{R}^2$, then

$$\ell(\alpha, \beta) = 0. \tag{38}$$

Badly approximable

It can be proved, that there exist badly approximable m-tuples $(\alpha_1, ..., \alpha_m)$, meaning the existence of such a constant $0 < \gamma < 1$ that

$$\max_{i=1,...,m} |q\alpha_i + p_i| > \frac{\gamma}{q^{1/m}} \tag{39}$$

for all

$$(q, p_1, ..., p_m)^t \in \mathbb{Z}^{m+1} \setminus \{\overline{0}\}, \quad q \in \mathbb{Z}^+.$$

BAD

The set of badly approximable numbers

$$Bad := \{\alpha \in \mathbb{R} \,\big|\, \exists\, \mu(\alpha) \in \mathbb{R}^+ : \; q\,\|q\alpha\| \geq \mu(\alpha) \quad \forall q \in \mathbb{Z}_{\geq 1}\}. \tag{40}$$

Thus, if $\alpha \in$ Bad, then there exists a positive constant $\mu = \mu(\alpha)$ such that

$$q\,\|q\alpha\| \geq \mu \quad \Rightarrow \quad \left|\alpha - \frac{p}{q}\right| \geq \frac{\mu}{q^2} \tag{41}$$

for all rationals $p/q \in \mathbb{Q}$.