数理解析研究所講究録 1384 巻 2004 年 57-63

ON SHARP DIOPHANTINE INEQUALITIES HAVING ONLY FINITELY MANY SOLUTIONS

EDWARD B. BURGER

1. CLASSICAL RESULTS: THE LAGRANGE SPECTRUM

Here we begin with a brief overview of some classical diophantine approximation results in order to place our work in context. We begin with the well-known result of Dirichlet from 1842 ([5], or see [2]).

Theorem 1. *For $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, there are infinitely many solutions $q \in \mathbb{Z}^+$ to*

$$q\|\alpha q\| \leq 1 , \tag{1.1}$$

where $\|x\|$ denotes the distance to the nearest integer function, $\|x\| = \min\{|x-n| : n \in \mathbb{Z}\}$.

We remark that if p is the nearest integer to αq, then $q\|\alpha q\| = q|\alpha q - p| = q^2\left|\alpha - \frac{p}{q}\right|$, and thus (1.1) is equivalent to the inequality

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^2} .$$

A Fundamental Question. Find the *largest* constant μ such that for any $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, there are infinitely many solutions $q \in \mathbb{Z}^+$ to

$$q\|\alpha q\| \leq \frac{1}{\mu} .$$

In 1879 Markoff [8] (see also [7]) showed that the largest such constant is $\mu = \sqrt{5}$, which we will denote as μ_1, and this constant is best possible for $\alpha = \alpha_1 = \frac{-1+\sqrt{5}}{2}$.

In fact more is true. We recall that $\alpha \sim \beta$ if α is a *linear fractional transformation* of β, that is, if there exist integers A, B, C, D satisfying $AD - BC = \pm 1$ for which

$$\alpha = \frac{A\beta + B}{C\beta + D} ,$$

This article is based on a plenary lecture delivered at The Conference on Analytic Number Theory and Surrounding Areas held at the Research Institute of Mathematical Sciences, Kyoto University, on September 30, 2003. The author wishes to thank the organizers for their warm hospitality.

or equivalently, if we denote the simple continued fraction expansions of α and β as $\alpha = [a_0, a_1, \ldots]$ and $\beta = [b_0, b_1, \ldots]$, then $\alpha \sim \beta$ if there exist indices M and N such that $a_{M+\ell} = b_{N+\ell}$ for all $\ell = 0, 1, 2, \ldots$. Then Markoff proved that μ_1 is best possible for all $\alpha \sim \alpha_1 = \frac{-1+\sqrt{5}}{2}$.

For $\alpha \not\sim \alpha_1$, Markoff showed that the next best constant is $\mu_2 = \sqrt{8}$ and cannot be improved for any $\alpha \sim \alpha_2 = -1 + \sqrt{2}$. In order to establish the general case, we consider *primitive* solutions $(r < s < m)$ to $x^2 + y^2 + z^2 = 3xyz$, that is, relatively prime integer solutions. The *Markoff numbers* are defined to be $m_1 < m_2 < m_3 < \cdots$. We remark that the sequence begins 1,2,5,13,29,... . Markoff proved that if μ_r denotes the rth best possible constant, then

$$\mu_r = \frac{\sqrt{9m_r^2 - 4}}{m_r} \ ,$$

and it cannot be improved for $\alpha \sim \alpha_{m_r} \in \mathbb{Q}\left(\sqrt{9m_r^2 - 4}\right)$, where the quadratic irrational α_{m_r} has a continued fraction expansion of the form

$$\alpha_{m_r} = \left[0, \overline{2, W_r, 1, 1, 2}\right] \ ,$$

where the "word" W_r consists of only 1's and 2's, all the runs are of even length (thus W_r itself is even in length), and W_r is a *palindrome*, that is, $\overrightarrow{W_r} = \overleftarrow{W_r}$ (see [4]).

The numbers $\mu_1, \mu_2, \mu_3, \ldots$ are the smallest values of the *Lagrange spectrum* and thus we immediately have the following important consequence.

Corollary 2. *The first accumulation point of the Lagrange spectrum is* 3.

2. A Question of Davenport

In 1947, H. Davenport posed the following problem: Given a positive integer n, what is the best constant $c_1(n)$ such that for any $\alpha \in \mathbb{R} \setminus \mathbb{Q}$,

$$q\|\alpha q\| \leq \frac{1}{c_1(n)}$$

has at least n solutions $q \in \mathbb{Z}^+$.

Previous Results. In 1948, Prasad [9] answered Davenport's question and showed that $c_1(n) = \frac{1+\sqrt{5}}{2} + \frac{p_{2n-1}}{q_{2n-1}}$, where p_ℓ/q_ℓ is the ℓth convergent of α_{m_1}, and $c_1(n)$ is best possible for $\alpha = \alpha_{m_1} = \frac{-1+\sqrt{5}}{2}$.

In 1961, Eggan [6] proved that for $\alpha \neq \alpha_{m_1}$, the constant can be improved to equal $c_2(n) = 1 + \sqrt{2} + \frac{p_{2n-1}}{q_{2n-1}}$, where p_ℓ/q_ℓ is the ℓth convergent of α_{m_2}. Moreover $c_2(n)$ is best possible for $\alpha = \alpha_{m_2} = -1 + \sqrt{2}$.

In 1971, Prasad and Prasad [10] showed that for $\alpha \neq \alpha_{m_1}, \alpha_{m_2}$, $c_3(n) = \frac{11+\sqrt{221}}{10} + \frac{p_{4n-1}}{q_{4n-1}}$, where p_ℓ/q_ℓ is the ℓth convergent of α_{m_3}, and established that $c_3(n)$ is best possible for $\alpha = \alpha_{m_3} = \frac{-11+\sqrt{221}}{10}$.

Open questions.

- What is $c_r(1)$ for an arbitrary r? Such a sequence would produce the analogue of the Lagrange spectrum where only one solution (rather than infinitely many) is desired.
- What is $\lim_{r\to\infty} c_r(1)$? If the limit exists, then it would produce the first accumulation point of the "one-solution" spectrum.
- Given an arbitrary r and n, what is $c_r(n)$?

3. Recent results

We begin by defining the linear recurrence sequence $\mathcal{Z}_r(n)$ by $\mathcal{Z}_r(0) = 0, \mathcal{Z}_r(1) = 1$, and for $n > 1$,

$$\mathcal{Z}_r(n) = 3m_r\mathcal{Z}_r(n-1) - \mathcal{Z}_r(n-2) .$$

Given this recurrence sequence, we can now offer answers to the open questions from the close of the previous section. This result was recently found by the author together with Folsom, Pekker, Roengpitya, and Snyder [2].

Theorem 3. *For any positive integers n and r,*

$$c_r(n) = \frac{\sqrt{9m_r^2-4}}{2m_r} + \frac{3}{2} - \frac{\mathcal{Z}_r(n-1)}{m_r\mathcal{Z}_r(n)} .$$

That is, for an irrational number α not equivalent to α_{m_s} for any s, $s < r$, the inequality

$$q\,\|\alpha q\| \le \frac{1}{c_r(n)}$$

has at least n positive integer solutions q. Moreover, the constant $c_r(n)$ is best possible for $\alpha = \alpha_{m_r}$.

Remark. As it is easy to verify that

$$\lim_{n\to\infty} \frac{\mathcal{Z}_r(n-1)}{\mathcal{Z}_r(n)} = \frac{3m_r - \sqrt{9m_r^2-4}}{2} ,$$

we see that

$$\lim_{n\to\infty} c_r(n) = \frac{\sqrt{9m_r^2-4}}{m_r} = \mu_r .$$

Corollary 4. *Given the notation of the previous theorem, $c_r(1) = \frac{3+\mu_r}{2}$ and thus*

$$\lim_{r\to\infty} c_r(n) = 3 .$$

Thus these observations show that the values $c_r(n)$ produce a *quantitative refinement* of the Lagrange spectrum. We remark that we also have the following technical result that provides a generalization in a form in sympathy with the previously known cases.

Theorem 5. *Let $r > 0$ be an integer. If $r = 1$ or 2, then let $L = 2$. For $r \ge 3$, let L equal the smallest period length of the continued fraction for α_{m_r}. Then $c_r(n) = -\overline{\alpha_{m_r}} + \frac{p_{nL-1}}{q_{nL-1}}$, where $\overline{\alpha}$ denotes the conjugate of α and p_ℓ/q_ℓ is the ℓth convergent of α_{m_r}.*

4. A sketch of the proof of Theorem 4

Given an irrational α, we consider three cases: (i) $\alpha = \alpha_{m_r}$; (ii) $\alpha \sim \alpha_m$, for $m \geq m_r$; (iii) $\alpha \not\sim \alpha_m$, for any m.

(i) Suppose that $\alpha = \alpha_{m_r}$. It follows from various properties of the recurrence sequence $\mathcal{Z}_r(n)$ that

$$\frac{p_{L-1}}{q_{L-1}}, \quad \frac{p_{2L-1}}{q_{2L-1}}, \ldots, \frac{p_{nL-1}}{q_{nL-1}}$$

all satisfy the inequality

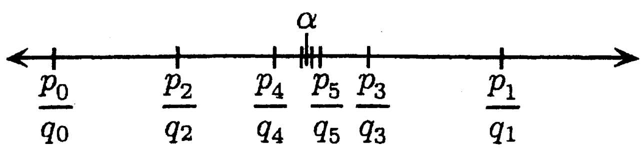
$$\left|\alpha_{m_r} - \frac{p}{q}\right| \leq \frac{1}{c_r(n)q^2}, \tag{4.1}$$

with *equality* holding for $\frac{p}{q} = \frac{p_{nL-1}}{q_{nL-1}}$.

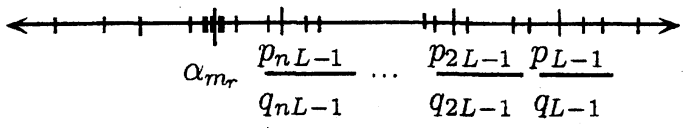
We now show that no other rational solutions to (4.1). First we note that for all indices r and n, $c_r(n) \geq 2$. Thus for any rational number $\frac{p}{q} \neq \frac{p_\ell}{q_\ell}$ for any ℓ, it follows by a classical result of Legendre that

$$\frac{1}{c_r(n)q^2} \leq \frac{1}{2q^2} < \left|\alpha_{m_r} - \frac{p}{q}\right| .$$

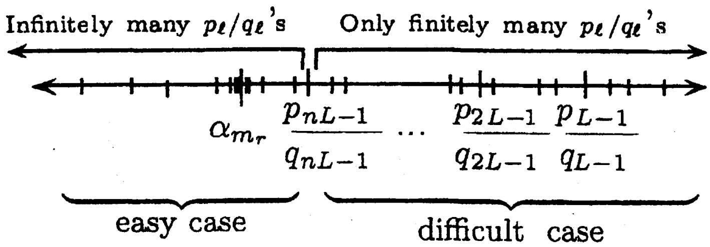
Hence we need only consider best approximates, p_ℓ/q_ℓ. Given that the p_ℓ/q_ℓ's straddle α as shown below



together with the fact that L is *even*, we see that



and hence we have two cases to consider:



The easy case. Suppose that $\frac{p}{q} < \frac{p_{nL-1}}{q_{nL-1}}$. Then we have that

$$\overline{\alpha_{m_r}} < 0 \leq \frac{p}{q} < \frac{p_{nL-1}}{q_{nL-1}},$$

and hence

$$\left|\overline{\alpha_{m_r}} - \frac{p}{q}\right| < \left|\overline{\alpha_{m_r}} - \frac{p_{nL-1}}{q_{nL-1}}\right| = c_r(n) \ .$$

If we write

$$f_{m_r}(x,y) = m_r\,(x - \alpha_{m_r} y)\,(x - \overline{\alpha_{m_r}}\ y) \in \mathbb{Z}[x,y]$$

for the m_rth *Markoff form*, then by a well-known result (see [4]) we have

$$\min_{\substack{(x,y)\in\mathbb{Z}^2\\(x,y)\neq(0,0)}} \left\{\left|f_{m_r}(x,y)\right|\right\} = m_r \ .$$

Putting these observations together with Theorem 5 reveals that

$$\begin{aligned}\frac{m_r}{q^2} \le \frac{|f_{m_r}(p,q)|}{q^2} &= m_r\left|\alpha_{m_r} - \frac{p}{q}\right|\left|\overline{\alpha_{m_r}} - \frac{p}{q}\right|\\ &< m_r\left|\alpha_{m_r} - \frac{p}{q}\right| c_r(n) \ ,\end{aligned}$$

which establishes the easy case.

The difficult case. Suppose that $\frac{p}{q} > \frac{p_{nL-1}}{q_{nL-1}}$. Thus we must have $\frac{p}{q} = \frac{p_{\ell L-k}}{q_{\ell L-k}}$, for some *odd* integer k satisfying $3 \le k \le L-1$. The proof of this case immediately follows from the next theorem which appears to be of some independent interest.

Theorem 6. *For $r \ge 3$, let L denote the smallest period length of the continued fraction expansion for α_{m_r}. Then the convergent p_ℓ/q_ℓ of α_{m_r} satisfies*

$$\frac{1}{\mu_r q_\ell^2} < \left|\alpha_{m_r} - \frac{p_\ell}{q_\ell}\right|$$

if and only if the index $\ell > 0$ and $\ell \not\equiv -1 \bmod L$.

An aside. Thus, while it is well-known that there are infinitely many solutions to

$$\left|\alpha_{m_r} - \frac{p_\ell}{q_\ell}\right| \le \frac{1}{\mu_r q_\ell^2} \ ,$$

the previous theorem implies that those solutions are *precisely* those p_ℓ/q_ℓ for which $\ell \equiv -1 \bmod L$.

Some remarks on the proof of Theorem 6. The proof has the same structure as the *easy case* $\left(\frac{p}{q} < \frac{p_{nL-1}}{q_{nL-1}}\right)$. We first construct auxiliary numbers

$$\lambda_r(\ell) = \frac{p_{\ell L-3} - p_{\ell L-1}\alpha_{m_r}}{q_{\ell L-3} - q_{\ell L-1}\alpha_{m_r}} \sim \alpha_{m_r} \ .$$

Next we establish the delicate inequality

$$\alpha_{m_r} < \frac{p_{\ell L-1}}{q_{\ell L-1}} < \overline{\lambda_r(\ell)} < \frac{p_{\ell L-k}}{q_{\ell L-k}} < \lambda_r(\ell) \ .$$

We then replace the Markoff forms with a new class of quadratic forms and proceed as in the easy case. Thus we have just established our main result in the case when $\alpha = \alpha_{m_r}$.
(*ii*) If $\alpha \sim \alpha_m$, for some $m \geq m_r$, then we use the structure of the continued fraction $\alpha_m = [0, \overline{2, W, 1, 1, 2}]$ and consider a large but finite number of sub-cases individually.
(*iii*) If $\alpha \not\sim \alpha_m$, for any m, then the result is trivial by classical well-known inequalities involving continued fractions. (See [2] for the technical details.)

5. A DUAL RESULT FOR ARBITRARY REAL QUADRATIC IRRATIONALS

For an irrational real number α, the *Lagrange constant* for α, $\mu(\alpha)$, is defined by

$$\mu(\alpha) = \liminf_{q\to\infty} q\|\alpha q\| \ .$$

Thus for any c, $0 < c < \mu(\alpha)$, it follows that there are only finitely many positive integer solutions q to the inequality

$$q\|\alpha q\| < c \ . \tag{5.1}$$

We define $\lambda(\alpha)$ by $\nu(\alpha) = \inf_{q>0} q\|\alpha q\|$.

In view of our previous discussion, given an α, two natural and fundamental problems are to compute $\nu(\alpha)$, and for a fixed c, $\nu(\alpha) < c < \mu(\alpha)$, to explicitly determine the complete set of solutions to (5.1).

Here in this concluding section we offer an overview these issues for reduced, real quadratic irrationals; that is, for real numbers that have purely periodic continued fraction expansions. The general theory for arbitrary real quadratic irrationals was given by the author and Todd [3].

If $\alpha = [\overline{a_0, a_1, \ldots, a_{T-1}}]$, then for each t, $0 \leq t \leq T-1$,

$$\begin{aligned} p_{Tn+t} &= \omega(\alpha)p_{T(n-1)+t} + (-1)^{T+1}p_{T(n-2)+t} \\ q_{Tn+t} &= \omega(\alpha)q_{T(n-1)+t} + (-1)^{T+1}q_{T(n-2)+t} \ , \end{aligned}$$

for all $n = 2, 3, \ldots$, where the constant $\omega(\alpha) = p_{T-1} + q_{T-2}$, and p_n/q_n denotes the nth convergent of α (see Theorem 3 of [3]). Furthermore, for each fixed t, $0 \leq t \leq T-1$, there exist real numbers u_t, v_t, r_t, s_t, with $r_t > 0$, such that

$$p_{Tn+t} = u_t\alpha^n + v_t\overline{\alpha}^n \quad \text{and} \quad q_{Tn+t} = r_t\alpha^n + s_t\overline{\alpha}^n,$$

for all $n = 0, 1, 2, \ldots$ (see [3]).

We now define several new but natural constants that will allow us to explicitly determine $\nu(\alpha)$. For each t, $0 \le t \le T-1$, we let $d_t = r_t v_t - s_t u_t$ and define

$$\nu_t(\alpha) = \begin{cases} |d_t|\left(1+\frac{s_t}{r_t}\right) & s_t < 0 \\ |d_t| & s_t > 0 \text{ and } T \text{ even} \\ |d_t|\left(1-\frac{s_t}{r_t}\overline{\alpha}^2\right) & s_t > 0 \text{ and } T \text{ odd} \end{cases} .$$

Given the above notation we have the following.

Theorem 7. *Suppose that* $\alpha = [\overline{a_0, a_1, \ldots, a_{T-1}}]$; r_t *and* s_t, d_t, *and* $\nu_t(\alpha)$ *are as defined above. Then* $\nu(\alpha) = \min\{\nu_t(\alpha) : 0 \le t \le T-1\}$. *Moreover, for any* c, $\nu(\alpha) < c < \mu(\alpha)$, *an integer* $q > 0$ *is a solution to*

$$q\|\alpha q\| < c$$

if and only if $q = q_{Tn+t}$, *where* $0 \le t \le T-1$, $(-1)^{Tn}s_t \le 0$, $\lambda_t(\alpha) < c$, *and* $n \ge 0$ *satisfies*

$$\frac{r_t}{|s_t|}\left(1-\frac{c}{|d_t|}\right) < \overline{\alpha}^{2n} .$$

As a final remark we note that upon first inspection it may appear undesirable to have n occur in the bound $(-1)^{Tn}s_t \le 0$. However as T and t are known, it is only the *parity* of n that is necessary in computing the previous inequality. Hence given c and t, one needs to find all even integers n that satisfy the conditions of the theorem and then all such odd integers. That is, implicit in the inequalities of the theorem are the cases of n even and n odd. The proof of this result and its generalizations can be found in [3].

References

1. E.B. Burger, *Exploring the Number Jungle: A Journey into Diophantine Analysis*, AMS Student Mathematical Library Series, Providence, 2000.
2. E.B. Burger, A. Folsom, A. Pekker, R. Roengpitya, J. Snyder, *On a quantitative refinement of the Lagrange spectrum*, Acta Arithmetica **102** (2002), 55–82.
3. E.B. Burger and J.M. Todd, *On diophantine approximation below the Lagrange constant*, Fibonacci Quart. **38** (2000), 136–144.
4. T.W. Cusick and M.E. Flahive, *The Markoff and Lagrange Spectra*, American Mathematical Society, Providence, 1989.
5. L.G.P. Dirichlet, *Verallgemeinerung eines Satzes aus der Lehre von den Kettenbrüchen nebst einigen Anwendungen auf die Theorie der Zahlen*, S. B. Preuss. Akad. Wiss. (1842), 93–95.
6. L.C. Eggan, *On Diophantine Approximations*, Trans. Amer. Math. Soc. **99** (1961), 102–117.
7. A. Hurwitz, *Über die angenäherte Darstellung der Irrationalzahlen durch rationale Brüche*, Math. Ann. **39** (1891), 279–284.
8. A. Markoff, *Sur les formes quadratiques binaires indéfinies*, Math. Ann. **15** (1879), 381–406.
9. A.V. Prasad, *Note on a Theorem of Hurwitz*, J. London Math. Soc. **23** (1948), 169–171.
10. M. Prasad and K.C. Prasad, *A Note on Diophantine Approximation*, Proc. Edinburgh Math. Soc. (2) **18** (1972/73), 137–142.

Department of Mathematics, Williams College, Williamstown, Massachusetts 01267 USA
E-mail address: eburger@williams.edu