Simultaneous Diophantine Approximation with Excluded Primes

Daniel Štefankovič

Department of Computer Science, University of Chicago,
1100 East 58th Street, Chicago, Illinois 60637, USA
email: stefanko@cs.uchicago.edu

June 27, 2001

Abstract

Given real numbers $\alpha_1, \ldots, \alpha_n$, a simultaneous diophantine ε-approximation is a sequence of integers $P_1, \ldots, P_n, Q$ such that $Q > 0$ and for all $j \in \{1, \ldots, n\}$, $|Q\alpha_j - P_j| \leq \varepsilon$. A simultaneous diophantine approximation is said to exclude the prime p if Q is not divisible by p. Given real numbers $\alpha_1, \ldots, \alpha_n$, a prime p and $\varepsilon > 0$ we show that at least one of the following holds

(a) there is a simultaneous diophantine ε-approximation which excludes p, or

(b) there exist $a_1, \ldots, a_n \in \mathbb{Z}$ such that $\sum a_j\alpha_j = 1/p + t,\ t \in \mathbb{Z}$ and $\sum |a_j| \leq n^{3/2}/\varepsilon$.

Note that in case (b) the a_j witness that there is no simultaneous diophantine $\varepsilon/(n^{3/2}p)$-approximation excluding p.

We generalize the result to simultaneous diophantine ε-approximations excluding several primes.

We also consider the algorithmic problem of finding, in polynomial time, a simultaneous diophantine ε-approximation excluding a set of primes.

1 Introduction

Given real numbers $\alpha_1, \ldots, \alpha_n$, a simultaneous diophantine ε-approximation is a sequence of integers $P_1, \ldots, P_n, Q$ such that $Q > 0$ and for all $j \in [n]$, $|Q\alpha_j - P_j| \leq \varepsilon$. By Dirichlet's theorem, for any $\alpha_1, \ldots, \alpha_n$ and any $\varepsilon > 0$ there is a simultaneous diophantine ε-approximation $P_1, \ldots, P_n, Q$, where $Q \leq \varepsilon^{-n}$.

We say that a diophantine approximation excludes the prime p if $p \nmid Q$. Given a prime p, real numbers $\alpha_1, \ldots, \alpha_n$ and $\varepsilon > 0$, is there a simultaneous diophantine ε-approximation excluding p? For example if $\alpha_1 = 1/p$ and $\varepsilon < 1/p$ then an ε-approximation excluding p is clearly not possible. The following proposition generalizes this observation.

Proposition 1 *Let $a_1, \ldots, a_n \in \mathbb{Z}$ be such that $\sum a_j \alpha_j = t/p$ where $p \nmid t$. If*

$$\sum |a_j| < \frac{1}{\varepsilon p}, \tag{1}$$

then there is no simultaneous diophantine ε-approximation excluding p.

Proof :
Suppose that we have $P_1, \ldots, P_n, Q$ such that $|Q\alpha_j - P_j| \le \varepsilon$. Then

$$\left| Q\frac{t}{p} - \sum a_j P_j \right| = \left| Q \sum a_j \alpha_j - \sum a_j P_j \right| \le \varepsilon \sum |a_j| < \frac{1}{p}.$$

This implies $p \mid Qt$ and therefore $p \mid Q$. ■

Proposition 1 says that certain linear relations with small coefficients are obstacles to simultaneous diophantine approximation excluding p. Our main result is a converse of this statement.

Theorem 1.1 *Let $\alpha_1, \ldots, \alpha_n$ be real numbers. Let p be a prime. If there is no simultaneous diophantine ε-approximation of $\alpha_1, \ldots, \alpha_n$ excluding p, then there exist integers $a_1, \ldots, a_n, s$ such that*

$$\sum a_j \alpha_j = \frac{1}{p} + s$$

and

$$\sum a_j^2 \le \frac{n^2}{\varepsilon^2}. \tag{2}$$

Remark 1 Note that (2) implies that $\sum |a_j| \le n^{3/2}/\varepsilon$. Hence the gap between the necessary upper bound (2) and the sufficient upper bound (1) for the absence of ε-approximation excluding p is $n^{3/2}p$ (independent of ε and the α_j).

We use the notation $[m] = \{1, \ldots, m\}$. Given real numbers $\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_m$, a nonhomogeneous diophantine ε-approximation is a sequence of integers $P_1, \ldots, P_m, Q$ such that $Q > 0$ and for all $j \in [m]$, $|Q\alpha_j - P_j - \beta_j| \le \varepsilon$. Nonhomogeneous diophantine ε-approximation need not exist.

Theorem 1.2 (Kronecker, see [Cas57, Lov86]) *Let $\alpha_1, \ldots, \alpha_m; \beta_1, \ldots, \beta_m \in \mathbb{R}$. Then exactly one of the following holds.*

- *For any $\varepsilon > 0$ there are $P_1, \ldots, P_m, Q$ such that $Q > 0$ and for all $j \in [m]$, $|Q\alpha_j - P_j - \beta_j| \le \varepsilon$.*
- *There are integers $a_1, \ldots, a_m$ such that $\sum a_j \alpha_j$ is an integer and $\sum a_j \beta_j$ is not an integer.*

■

Let $\varepsilon < 1/p$. A nonhomogeneous diophantine ε-approximation of the numbers

$$\alpha_1, \ldots, \alpha_n, \frac{1}{p}; 0, \ldots, 0, \frac{1}{p}, \tag{3}$$

gives a simultaneous diophantine ε-approximation of $\alpha_1, \ldots, \alpha_n$ excluding p. Hence the following is immediate from Kronecker's theorem.

Corollary 1.3 *Let $\alpha_1, \ldots, \alpha_n$ be real numbers. Let p be a prime. Then exactly one of the following holds*

- *For any $\varepsilon > 0$ there is a simultaneous diophantine ε-approximation of $\alpha_1, \ldots, \alpha_n$ excluding p.*
- *There are integers $a_1, \ldots, a_n, t$ such that $p \nmid t$ and $\sum a_j \alpha_j = t/p$.*

■

Theorem 1.1 is an effective version of this result.

Acknowledgements. I would like to thank László Babai for introducing me to the problem of simultaneous diophantine approximations excluding a prime and for suggesting many improvements to the paper. Thanks to Samuel Kutin for stimulating discussions.

2 Proof

We will use a technique due to Banaszczyk [Ban93]. Given a measure μ on $\mathbb{R}^d$, its Fourier transform is the function $\mathbb{R}^d \to \mathbb{R}$ given by

$$\widehat{\mu}(y) = \int \exp(2\pi i y^T x)\ d\mu(x). \tag{4}$$

For $A \subseteq \mathbb{R}^d$ we let

$$\rho(A) = \sum_{x \in A} \exp(-\pi ||x||^2).$$

Let L be a lattice in $\mathbb{R}^d$. Let σ_L be the discrete measure given by

$$\sigma_L(X) = \rho(X \cap L)/\rho(L).$$

Plugging the definition of σ_L into (4) we obtain

$$\widehat{\sigma_L}(y) = \frac{1}{\rho(L)} \sum_{x \in L} \exp(-\pi ||x||^2) \exp(2\pi i y^T x).$$

Let

$$\phi_L(x) = \rho(L + x)/\rho(L).$$

Let L^* be the dual lattice of L. Banaszczyk proved the following two results.

Lemma 2.1 ([Ban93]) *The Fourier transform of the measure σ_L associated with the lattice L is the function ϕ_{L^*} associated with the dual lattice L^*.*

$$\widehat{\sigma_L} = \phi_{L^*}.$$

■

Let B be the unit ball in $\mathbb{R}^d$.

Lemma 2.2 ([Ban93]) *For any $c \geq (2\pi)^{-1/2}$ and $u \in \mathbb{R}^d$*

$$\rho((L+u)/c\sqrt{d}B) < 2\left(c\sqrt{2\pi e}\, e^{-\pi c^2}\right)^d.$$

■

For $d \geq 3$ we let $c = \sqrt{1-1/d}$ in Lemma 2.2 and obtain following bound.

Corollary 2.3 *For any $u \in \mathbb{R}^d$*

$$\frac{\rho\left((L+u) \setminus \sqrt{d-1}B\right)}{\rho(L)} \leq 1/4.$$

■

If there is no vector in L^* at distance $\leq \sqrt{d-1}$ from u, then

$$\rho(L^*+u) = \rho\big((L^*+u) \setminus \sqrt{d-1}B\big) \leq \frac{1}{4}\rho(L^*).$$

Hence $\widehat{\sigma_L}(u) = \phi_{L^*}(u) \leq 1/4$. Thus large $\widehat{\sigma_L}(u)$ implies the existence of $w \in L^*$ close to u.

Corollary 2.4 *Let $u \in \mathbb{R}^d$. If $\widehat{\sigma_L}(u) > 1/4$ then there is a vector w in the dual lattice L^* such that $||u-w|| \leq \sqrt{d-1}$.*

■

Proof of Theorem 1.1

Let $d = n+1$. Let ν be a positive rational number to be chosen later. Let $L \subseteq \mathbb{R}^d$ be the lattice generated by the columns $b_1, \ldots, b_{n+1}$ of the matrix B,

$$B = \frac{\sqrt{n}}{\varepsilon}\begin{pmatrix} & & & \alpha_1 \\ & I & & \vdots \\ & & & \alpha_n \\ 0 & \ldots & 0 & \nu \end{pmatrix}.$$

The dual lattice $L^* \subseteq \mathbb{R}^d$ is generated by the columns $b_1^*, \ldots, b_{n+1}^*$ of the matrix B^{-T} (inverse-transpose),

$$B^{-T} = \frac{\varepsilon}{\sqrt{n}}\begin{pmatrix} & & & 0 \\ & I & & \vdots \\ & & & 0 \\ -\alpha_1/\nu & \ldots & -\alpha_n/\nu & 1/\nu \end{pmatrix}.$$

Given a vector $w \in L$, let $U(w)$ be the coefficient of b_{n+1} in the expression of w. We can tell the coefficient by looking at the last coordinate of w, i. e.,

$$U(w) = \frac{\varepsilon}{\nu\sqrt{n}}e_{n+1}^T w,$$

where $e_{n+1} = (0, \ldots, 0, 1)$.

If there is a vector w in L of euclidean norm $||w||_2 \le \sqrt{n}$ such that $U(w) \not\equiv 0 \pmod p$, then we have an diophantine ε-approximation of $\alpha_1, \ldots, \alpha_n$ excluding p (we use $||w||_\infty \le ||w||_2$). Thus by the assumption of Theorem 1.1 all vectors $w \in L$ with $||w||_2 \le \sqrt{n}$ have $U(w) \equiv 0 \pmod p$.

Let $u = \dfrac{\varepsilon}{p\nu\sqrt{n}} e_{n+1}$. We have

$$\widehat{\sigma_L}(u) = \frac{1}{\rho(L)} \sum_{x \in L} \exp(-\pi ||x||^2) \exp(2\pi i U(x)/p) \ge \left| \frac{1}{\rho(L)} \sum_{x \in L \cap \sqrt{n}B} \exp(-\pi ||x||^2) \exp(2\pi i U(x)/p) \right| - \left| \frac{1}{\rho(L)} \sum_{x \in L \setminus \sqrt{n}B} \exp(-\pi ||x||^2) \exp(2\pi i U(x)/p) \right|. \tag{5}$$

All vectors $x \in L$ of norm $||x||_2 \le \sqrt{n}$ have $\exp(2\pi i U(x)/p) = 1$. Hence

$$\widehat{\sigma_L}(u) \ge \frac{1}{\rho(L)} \sum_{x \in L \cap \sqrt{n}B} \exp(-\pi ||x||^2) - \frac{1}{\rho(L)} \sum_{x \in L \setminus \sqrt{n}B} \exp(-\pi ||x||^2) =$$
$$1 - \frac{2}{\rho(L)} \sum_{x \in L \setminus \sqrt{n}B} \exp(-\pi ||x||^2) = 1 - 2\frac{\rho(L \setminus \sqrt{n}B)}{\rho(L)}$$

Thus, using Corollary 2.3,

$$\widehat{\sigma_L}(u) \ge 1 - 2/4. \tag{6}$$

Hence from Corollary 2.4 it follows that there is a vector $w \in L^*$, $w = a_1 b_1^* + \ldots a_n b_n^* + c b_{n+1}^*$ such that w is at distance $\le \sqrt{d-1} = \sqrt{n}$ from u. We have

$$\sum a_j^2 \le \frac{n^2}{\varepsilon^2} \qquad \text{and} \qquad \left| \sum a_j \alpha_j - \frac{1}{p} - c \right| \le \frac{\nu n}{\varepsilon}. \tag{7}$$

Let $\nu \to 0$. There are finitely many choices for the a_j and c, hence there exist integers a_j and c such that

$$\sum a_j^2 \le \frac{n^2}{\varepsilon^2} \qquad \text{and} \qquad \left| \sum a_j \alpha_j - \frac{1}{p} - c \right| = 0.$$

■

3 Excluding several primes

We say that a diophantine approximation excludes a set of primes $\{p_1, \ldots, p_k\}$ if it excludes all the p_ℓ. The following observation is a generalization of Proposition 1.

Proposition 2 *Let $a_1, \ldots, a_n \in \mathbb{Z}$ be such that $\sum a_j \alpha_j = \sum \frac{t_\ell}{p_\ell}$ where for at least one $\ell \in [k]$, $p_\ell \nmid t_\ell$. If*

$$\sum |a_j| < \frac{1}{\varepsilon p_1 \cdots p_k}, \tag{8}$$

then there is no ε-simultaneous diophantine approximation excluding $\{p_1, \ldots, p_k\}$.

We can generalize Theorem 1.1 to approximations excluding a set of primes.

Theorem 3.1 *If there is no simultaneous diophantine ε-approximation excluding $\{p_1, \ldots, p_k\}$, then there exist integers $a_1, \ldots, a_n, s$ and $A \subseteq [k]$ such that*

$$\sum a_j \alpha_j = \sum_{\ell \in A} \frac{1}{p_\ell} + s$$

and

$$\sum a_j^2 \leq \max\{n^2, k^2\}/\varepsilon^2. \tag{9}$$

The proof of Theorem 3.1 is similar to the proof of Theorem 1.1. Instead of (5) we consider following sum

$$\frac{1}{\rho(L)} \sum_{x \in L} \exp(-\pi ||x||^2) \prod_{t \in [k]} (1 - \exp(2\pi i U(x)/p_t)).$$

We also use that for $m = \max\{\sqrt{d-1}, \sqrt{k}\}$, any $u \in \mathbb{R}^d$ and any lattice $L \subseteq \mathbb{R}^d$, $d \geq 3$

$$\rho\big((L+u) \setminus mB\big) < \frac{1}{2^{k+1}} \rho(L).$$

Following result is used in the proof instead of Corollary 2.4.

Corollary 3.2 *If $\widehat{\sigma}_L(u) > 1/2^{k+1}$, then there is a vector w in the dual lattice L^* such that $||u - w|| \leq \max\{\sqrt{d-1}, \sqrt{k}\}$.*

■ ■

Remark 2 Note that (9) implies that $\sum |a_j| \leq n^{1/2} \max\{n, k\}/\varepsilon$. Hence the gap between the necessary upper bound (9) and the sufficient upper bound (8) for the absence of ε-approximation excluding $\{p_1, \ldots, p_k\}$ is $n^{1/2} \max\{n, k\} p_1 \cdots p_k$ (independent of ε and the α_j).

4 A polynomial-time algorithm

Suppose that there exists a simultaneous diophantine ε-approximation $P_1, \ldots, P_n, Q$ of $\alpha_1, \ldots, \alpha_n$ excluding p. Is there a way to efficiently find a simultaneous diophantine $f(n)\varepsilon$-approximation of $\alpha_1, \ldots, \alpha_n$ excluding p?

We assume that $\alpha_1, \ldots, \alpha_n$ are rational numbers. The length of the input is the sum of the lengths of the input numbers $\alpha_1, \ldots, \alpha_n, \varepsilon$ and p. The length of $\alpha = a/b$ is the length of a in binary plus length of b in binary. By efficiently we mean in polynomial time in the input length.

Theorem 4.1 *Let $\alpha_1, \ldots, \alpha_n$ be rational numbers. Let p be a prime. Suppose that there exists a simultaneous diophantine ε-approximation $P_1, \ldots, P_n, Q$ of $\alpha_1, \ldots, \alpha_n$ excluding p. We can find in polynomial time a simultaneous diophantine $C_{n+1} p \varepsilon$-approximation of $\alpha_1, \ldots, \alpha_n$ excluding p, where $C_n = 4\sqrt{n} 2^{n/2}$.*

We will use Babai's modification [Bab86] of Lovász's lattice algorithm [LLL82, Lov86]. In [Bab86] the following result is proven for $\varepsilon_1 = \cdots = \varepsilon_m$; the general case follows from the same proof.

Theorem 4.2 ([Bab86],Theorem 7.1) *Let $\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_m, \varepsilon_1 > 0, \ldots, \varepsilon_m > 0$ be given rational numbers. Let $q > 0$ be the smallest integer Q for which there exist $P_1, \ldots, P_m$ such that $|Q\alpha_j - P_j - \beta_j| \leq \varepsilon_j$ for all $j \in [m]$; we let $q = \infty$ if no such q exists. One can find in polynomial time either*

(a) *a proof that $q = \infty$, or*

(b) *integers $P_1, \ldots, P_m, Q$ such that*

- $|Q\alpha_j - P_j - \beta_j| \leq C_m\varepsilon_j$ *for all $j \in [m]$, and*
- $|Q| \leq C_m q$,

where $C_m = 4\sqrt{m}2^{m/2}$.

■

Proof of Theorem 4.1
Multiplying $P_1, \ldots, P_n, Q$ by the multiplicative inverse of Q in $\mathbb{Z}/p\mathbb{Z}$ we obtain a simultaneous diophantine $p\varepsilon$-approximation $P'_1, \ldots, P'_n, Q'$ of $\alpha_1, \ldots, \alpha_n$ with $Q' \equiv 1 \pmod p$. Hence there exists a nonhomogeneous diophantine approximation of $\alpha_1, \ldots, \alpha_n, 1/p; 0, \ldots, 0, 1/p$ with $\varepsilon_1 = \cdots = \varepsilon_n = p\varepsilon$ and $\varepsilon_{n+1} = \varepsilon$. Now by Theorem 4.2 we can find, in polynomial time, $P''_1, \ldots, P''_{n+1}, Q''$ such that $|Q''\alpha_j - P''_j| \leq C_{n+1}p\varepsilon$ and $|Q''/p - P''_{n+1} - 1/p| < C_{n+1}\varepsilon$. Hence if $C_{n+1}p\varepsilon < 1$ we have $Q'' \equiv 1 \pmod p$. Therefore $Q'', P''_1, \ldots, P''_n$ is a simultaneous diophantine $C_{n+1}p\varepsilon$-approximation of $\alpha_1, \ldots, \alpha_n$ excluding p. For $C_{n+1}p\varepsilon \geq 1$, Theorem 4.1 holds vacuously. ■

We can generalize Theorem 4.1 to several primes.

Theorem 4.3 *Let $\alpha_1, \ldots, \alpha_n, \varepsilon$ be rational numbers. Let $p_1, \ldots, p_k$ be primes. Suppose that there exists a simultaneous diophantine ε-approximation $P_1, \ldots, P_n, Q$ of $\alpha_1, \ldots, \alpha_n$ excluding $\{p_1, \ldots, p_k\}$. We can find, in polynomial time, a simultaneous diophantine $C_{n+k}p_1 \cdots p_k\varepsilon$-approximation of $\alpha_1, \ldots, \alpha_n$ excluding $\{p_1, \ldots, p_k\}$, where $C_n = 4\sqrt{n}2^{n/2}$.*

Proof sketch
We multiply $P_1, \ldots, P_n, Q$ by the multiplicative inverse of Q in the ring $\mathbb{Z}/p_1 \cdots p_k\mathbb{Z}$. Then, similarly as in the proof of Theorem 4.1, we use nonhomogeneous diophantine approximation for

$$\alpha_1, \ldots, \alpha_n, 1/p_1, \ldots, 1/p_k; 0, \ldots, 0, 1/p_1, \ldots, 1/p_k.$$

■

References

[Bab86] L. Babai. On Lovász lattice reduction and the nearest lattice point problem. *Combinatorica*, 6(1):1–13, 1986.

[Ban93] W. Banaszczyk. New bounds in some transference theorems in the geometry of numbers. *Mathematische Annalen*, 296(4):625–635, 1993.

[Cas57] J. Cassels. *An Introduction to Diophantine Approximations*. Cambridge University Press, Cambridge, 1957.

[LLL82] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261:515–534, 1982.

[Lov86] L. Lovász. *An Algorithmic Theory of Numbers, Graphs, and Convexity*. SIAM, Philadelphia, PA, 1986.