Simultaneous Diophantine Approximation with Excluded Primes

László Babai* Daniel Štefankovič*

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 $j\in\{1,\ldots,n\}$, $|Q\alpha_j-P_j|\le\varepsilon$. 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 $\sum|a_j|\le n^{3/2}/\varepsilon$.

Note that these two conditions are mutually nearly exclusive in the sense that in case (b) the a_j witness that there is no simultaneous diophantine $\varepsilon/(n^{3/2}p)$-approximation excluding p. The proof method is Fourier analysis using results and techniques of Banaszczyk [Ban93].

As an application we show that for p a prime and bounded $d\,|\,p-1$ the ring $\mathbb{Z}/p^k\mathbb{Z}$ contains a number all of whose d-th roots (mod p^k) are small.

We generalize the result to simultaneous diophantine ε-approximations excluding several primes and 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 $j\in[n]$, $|Q\alpha_j-P_j|\le\varepsilon$. By Dirichlet's theorem (see e.g. [Lov86]), 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 $Q\le\varepsilon^{-n}$. Given $\alpha_1,\ldots,\alpha_n$ and an integer $q>0$ it is NP-hard to find the best simultaneous diophantine approximation with $Q\le q$ ([Lag85]). It is possible to find, in polynomial time, an approximation with $Q\le q$ and $\varepsilon\le 2^{n^2}q^{-1/n}$ [LLL82, Lov86]. This found numerous applications such as factoring of polynomials with rational coefficients [LLL82] and more generally over algebraic number fields, breaking of knapsack-type cryptosystems [Lag84],[Sha82] or in the disproof of the Mertens conjecture via explicit computation [OT85]. In this paper we will consider the following modification of the simultaneous diophantine approximation problem. Instead of giving an upper bound on Q we will require that Q be not divisible by a given prime p. Potential applications of this problem arose recently in extremal combinatorics, coding theory and the study of the diameter of Cayley graphs.

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 1.1. *Let $a_1,\ldots,a_n\in\mathbb{Z}$ be such that $\sum_{j=1}^n a_j\alpha_j = t/p$ where $p\nmid t$. If*

$$\sum_{j=1}^n |a_j| < \frac{1}{\varepsilon p}, \tag{1.1}$$

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

$$\left|Q\frac{t}{p}-\sum_{j=1}^n a_jP_j\right| = \left|Q\sum_{j=1}^n a_j\alpha_j-\sum_{j=1}^n a_jP_j\right| \le \varepsilon\sum_{j=1}^n|a_j| < \frac{1}{p}.$$

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

Proposition 1.1 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 for any t there exist integers $a_1,\ldots,a_n,s$ such that*

$$\sum_{j=1}^n a_j\alpha_j = \frac{t}{p}+s$$

*Department of Computer Science, University of Chicago, Chicago, IL 60637, {babai,stefanko}@cs.uchicago.edu.

and

$$\sum_{j=1}^{n} a_j^2 \leq \frac{n^2}{\varepsilon^2}. \tag{1.2}$$

REMARK 1. Note that (1.2) implies that $\sum_{j=1}^{n} |a_j| \leq n^{3/2}/\varepsilon$. Hence the gap between the necessary upper bound (1.2) and the sufficient upper bound (1.1) for the absence of ε-approximation excluding p is a factor of $n^{3/2}p$ (independent of ε and the α_j).

Theorem 1.1 does not impose a bound on the denominator. For algorithmic applications it is natural to impose such a bound. This problem is addressed in our next result.

THEOREM 1.2. *Let $\alpha_1, \ldots, \alpha_n$ be real numbers. Let p be a prime and let $q > 0$ be an integer. If there is no simultaneous diophantine ε-approximation $P_1, \ldots, P_n, Q \leq q$ of $\alpha_1, \ldots, \alpha_n$ excluding p, then for any t there exist integers $a_1, \ldots, a_n, s$ and a real number κ of absolute value $|\kappa| \leq n/q$ such that*

$$\sum_{j=1}^{n} a_j \alpha_j = \frac{t}{p} + s + \kappa$$

and

$$\sum_{j=1}^{n} a_j^2 \leq \frac{n^2}{\varepsilon^2}. \tag{1.3}$$

REMARK 2. The numbers $a_1, \ldots, a_n$ are witnesses that there is no simultaneous diophantine $\varepsilon/(2n^{3/2}p)$-approximation $P_1, \ldots, P_n, Q$ of $\alpha_1, \ldots, \alpha_n$ with $Q \leq 2p/|\kappa|$.

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

THEOREM 1.3. (KRONECKER, SEE [CAS57, LOV86]) *Let $\alpha_1, \ldots, \alpha_n; \beta_1, \ldots, \beta_n \in \mathbb{R}$. Then exactly one of the following holds.*

- *For all $\varepsilon > 0$ there exist $P_1, \ldots, P_n, Q$ such that $Q > 0$ and for all $j \in [n]$, $|Q\alpha_j - P_j - \beta_j| \leq \varepsilon$.*
- *There exist integers $a_1, \ldots, a_n$ such that $\sum_{j=1}^{n} a_j \alpha_j$ is an integer and $\sum_{j=1}^{n} a_j \beta_j$ is not an integer.*

■

This classical result is relevant to our problem through the following reduction:

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

$$\alpha_1, \ldots, \alpha_n, \frac{1}{p}; 0, \ldots, 0, \frac{1}{p}, \tag{1.4}$$

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

COROLLARY 1.1. *Let $\alpha_1, \ldots, \alpha_n$ be real numbers. Let p be a prime. Then exactly one of the following holds*

- *For all $\varepsilon > 0$ there exists a simultaneous diophantine ε-approximation of $\alpha_1, \ldots, \alpha_n$ excluding p.*
- *There exist integers $a_1, \ldots, a_n, t$ such that $p \nmid t$ and $\sum_{j=1}^{n} a_j \alpha_j = t/p$.*

■

Theorem 1.1 is an effective version of this result.

We also consider the algorithmic problem of finding, in polynomial time, a simultaneous diophantine ε-approximation of $\alpha_1, \ldots, \alpha_n$ excluding p. We assume that $\alpha_1, \ldots, \alpha_n$ are rational numbers given by a numerator and a denominator encoded in binary. The number p, encoded in binary, is also part of the input.

THEOREM 1.4. *Let $\alpha_1, \ldots, \alpha_n$ be rational numbers. Let p be a prime. Let $\varepsilon \geq 0$ be the smallest real number such that there exists a simultaneous diophantine ε-approximation $P_1, \ldots, P_n, Q$ of $\alpha_1, \ldots, \alpha_n$ excluding p. Then we can find, in polynomial time, a simultaneous diophantine $2C_{n+1}p\varepsilon$-approximation of $\alpha_1, \ldots, \alpha_n$ excluding p, where $C_n = 4\sqrt{n}2^{n/2}$.*

Note that ε is not part of the input in the "polynomial time" statement above. In fact either $\varepsilon = 0$ or $1/\varepsilon \leq$ the largest denominator of $\alpha_1, \ldots, \alpha_n$.

PROPOSITION 1.2. *If $\alpha_j = a_j/b_j \in \mathbb{Q}$, $j \in [n]$ then there exists a smallest ε for which an ε-approximation of $\alpha_1, \ldots, \alpha_n$ exists. Moreover, this smallest ε is a fraction with denominator b_j for some j. In particular, either $\varepsilon = 0$ or $\varepsilon \geq \frac{1}{\max_{j \in [n]} b_j}$.*

Proof: If $P_1, \ldots, P_n, Q$ is an ε-approximation then ε can be taken to be $\max_{j \in [n]} |Q\alpha_j - P_j|$ and therefore $b_j\varepsilon$ is an integer for some $j \in [n]$. ■

Acknowledgements. We wish to thank Samuel Kutin for stimulating discussions and for suggesting a potential combinatorial application to simultaneous diophantine approximation with an excluded prime.

2 Proofs

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

$$\widehat{\mu}(y) = \int_{\mathbb{R}^d} \exp(2\pi i y^T x)\, d\mu(x). \tag{2.5}$$

For a countable subset $A \subseteq \mathbb{R}^d$ consider the discrete measure

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

where $||x|| = \sqrt{\sum_{j=1}^d x_j^2}$ is the euclidean norm. Let L be a lattice in $\mathbb{R}^d$, i.e., L is the set of linear combinations with integer coefficients of a basis in $\mathbb{R}^d$: $L = \sum_{j=1}^d \mathbb{Z} b_j$. 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 (2.5) we obtain

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

Note that $\widehat{\sigma_L}(y)$ is always real and $|\widehat{\sigma_L}(y)| \leq 1$. Let

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

Let L^* be the lattice dual to L, i.e.

$$L^* = \{x \in \mathbb{R}^d \mid (\forall y \in L)(x^T y \in \mathbb{Z})\}.$$

Banaszczyk proved the following 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^*:*

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

■

If follows, in particular, that for every lattice L and for all $x \in \mathbb{R}^d$, $0 \leq \widehat{\sigma_L}(x) \leq 1$ and $0 \leq \phi_L(x) \leq 1$. Indeed $\phi_L(x) \geq 0$ by definition and $\widehat{\sigma_L}(x) \leq 1$ by the observation above.

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

$$\mathcal{B} = \{x \in \mathbb{R}^d \mid ||x|| \leq 1\}.$$

Banaszczyk has shown that most of the ρ-measure of each translate of L is concentrated in a ball of radius $O(\sqrt{d})$ about the origin. The following lemma formalizes this phenomenon.

LEMMA 2.2. ([BAN93]) *For any $c \geq (2\pi)^{-1/2}$ and $u \in \mathbb{R}^d$,*

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

■

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

COROLLARY 2.1. *For any $u \in \mathbb{R}^d$*

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

■

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

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

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 2.2. *Let $u \in \mathbb{R}^d$. If $\widehat{\sigma_L}(u) > 1/4$ then there exists $w \in L^*$ 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),

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

Given $w \in L$, let $U(w)$ denote 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 exists $w \in L$ of euclidean norm $||w|| \leq \sqrt{n}$ 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 $||w||_\infty \leq ||w||$). Thus by the assumption of Theorem 1.1, all $w \in L$ with $||w|| \leq \sqrt{n}$ satisfy $U(w) \equiv 0 \pmod p$.

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

(2.6)

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

Now all $x \in L$ of norm $||x|| \leq \sqrt{n}$ satisfy $\exp(2t\pi i U(x)/p) = 1$. Hence

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

Thus, using Corollary 2.1,

(2.7) $$\widehat{\sigma_L}(u) \geq 1 - 2/4 = 1/2.$$

Hence from Corollary 2.2 it follows that there exists $w \in L^*$, $w = a_1 b_1^* + \ldots a_n b_n^* + c b_{n+1}^*$ such that w is at distance $\leq \sqrt{d-1} = \sqrt{n}$ from u. We have

(2.8)

$$\sum_{j=1}^n a_j^2 \leq \frac{n^2}{\varepsilon^2} \quad \text{and} \quad \left| \sum_{j=1}^n a_j \alpha_j - \frac{t}{p} - c \right| \leq \frac{\nu n}{\varepsilon}.$$

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

$$\sum_{j=1}^n a_j^2 \leq \frac{n^2}{\varepsilon^2} \quad \text{and} \quad \left| \sum_{j=1}^n a_j \alpha_j - \frac{t}{p} - c \right| = 0.$$

■

Proof of Theorem 1.2: In the proof of Theorem 1.1 we choose $\nu = \varepsilon/q$. We note that for $w \in L$, if $|U(w)| \geq q$ then $||w|| \geq \sqrt{n}$. The rest of the proof is the same. ■

3 Excluding several primes

We say that a diophantine approximation excludes a set $\{p_1, \ldots, p_k\}$ of primes if it excludes all the p_ℓ. The following observation is a generalization of Proposition 1.1. We use the notation $[k] = \{1, \ldots, k\}$.

PROPOSITION 3.1. *Let $a_1, \ldots, a_n \in \mathbb{Z}$ be such that $\sum_{j=1}^n a_j \alpha_j = \sum_{j=1}^n \frac{t_\ell}{p_\ell}$ where for at least one $\ell \in [k]$, $p_\ell \nmid t_\ell$. If*

(3.9) $$\sum_{j=1}^n |a_j| < \frac{1}{\varepsilon p_1 \cdots p_k},$$

then there is no simultaneous diophantine ε-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*

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

and

(3.10) $$\sum_{j=1}^n a_j^2 \leq \max\{n^2, k^2\}/\varepsilon^2.$$

The proof of Theorem 3.1 is similar to the proof of Theorem 1.1. Instead of (2.6) 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 need to modify Corollary 2.1 as follows.

COROLLARY 3.1. *For any $u \in \mathbb{R}^d$*

$$\frac{\rho((L+u) \setminus m\mathcal{B})}{\rho(L)} < \frac{1}{2^{k+1}}.$$

where $m = \max\{\sqrt{d-1}, \sqrt{k}\}$ and $d \geq 3$.

In the place of Corollary 2.2 we use the following result.

COROLLARY 3.2. *Let $u \in \mathbb{R}^d$. If $\widehat{\sigma}_L(u) > 1/2^{k+1}$, then there exists w in the dual lattice L^* such that*

$$||u - w|| \leq \max\{\sqrt{d-1}, \sqrt{k}\}.$$

REMARK 3. Note that (3.10) implies that $\sum_{j=1}^{n} |a_j| \leq n^{1/2} \max\{n,k\}/\varepsilon$. Hence the gap between the necessary upper bound (3.10) and the sufficient upper bound (3.9) for the absence of ε-approximation excluding $\{p_1,\ldots,p_k\}$ is a factor of $n^{1/2}\max\{n,k\}p_1\cdots p_k$ (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 for some function f?

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

THEOREM 4.1. ([BAB86],THEOREM 7.1) *Let $\alpha_1,\ldots,\alpha_n,\beta_1,\ldots,\beta_n,\varepsilon_1 > 0,\ldots,\varepsilon_n > 0$ be given rational numbers. Let $q > 0$ be the smallest integer Q for which there exist $P_1,\ldots,P_n$ such that $|Q\alpha_j - P_j - \beta_j| \leq \varepsilon_j$ for all $j \in [n]$; we let $q = \infty$ if no such q exists. One can find in polynomial time either*

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

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

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

where $C_n = 4\sqrt{n}2^{n/2}$.

■

Proof of Theorem 1.4: If none of the denominators of $\alpha_1,\ldots,\alpha_n$ is divisible by p then $\varepsilon = 0$ and we can easily find a 0-approximation of $\alpha_1,\ldots,\alpha_n$ excluding p. If some denominator b_j of $\alpha_1,\ldots,\alpha_n$ is divisible by p then $\varepsilon \geq 1/b_j$.

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 $\varepsilon_{n+1} = \varepsilon$.

If $2C_{n+1}p\varepsilon \geq 1$, Theorem 1.4 holds vacuously. Hence we assume $2C_{n+1}p\varepsilon < 1$. By Theorem 4.1 for $\delta \geq \varepsilon$ we can find, in polynomial time, $P_1'',\ldots,P_{n+1}'',Q''$ such that $|Q''\alpha_j - P_j''| \leq C_{n+1}p\delta$ and $|Q''/p - P_{n+1}'' - 1/p| < C_{n+1}\delta$. Hence if $C_{n+1}p\delta < 1$ we have $Q'' \equiv 1 \pmod p$. Therefore $Q'',P_1'',\ldots,P_n''$ is a simultaneous diophantine $C_{n+1}p\delta$-approximation of $\alpha_1,\ldots,\alpha_n$ excluding p. Since ε is not part of the input, we try $\delta = 2^{-k}$, $k = 1,2,\ldots$. Since we have a lower bound on ε we shall try at most polynomially many values of δ. ■

We can generalize Theorem 1.4 to several primes.

THEOREM 4.2. *Let $\alpha_1,\ldots,\alpha_n,\varepsilon$ be rational numbers. Let $p_1,\ldots,p_k$ be primes. Let $\varepsilon \geq 0$ be the smallest real number such 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 $2C_{n+k}p_1\cdots p_k\varepsilon$-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 1.4, we use nonhomogeneous diophantine approximation for

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

■

5 Application

5.1 Contracting a set of residue classes

The following type of question recently arose in a number of contexts including coding theory [BSŠ03], extremal combinatorics [Kut01] and the study of the diameters of certain Cayley graphs (in progress).

Let $(x \bmod m)$ denote an integer y with smallest absolute value under the constraint $y \equiv x \pmod m$. **Question:** Let $A \subseteq \mathbb{Z}/m\mathbb{Z}$. Does there exist an integer Q such that $\gcd(Q,m) = 1$ and for all $a \in A$, $|aQ \pmod m|$ is small?

This in effect is a simultaneous approximation problem with denominator relatively prime to m. Indeed, for $A = \{a_1,\ldots,a_n\}$, our question asks the existence of $P_1,\ldots,P_n$ and Q such that $\gcd(Q,m) = 1$ and $|a_jQ - mP_j| \leq \varepsilon m$. Equivalently, we need $|\alpha_jQ - P_j| \leq \varepsilon$ where $\alpha_j = a_j/m$. Note that if such a Q exists then w.l.o.g. $0 \leq Q < m$. Theorem 1.1 states the essentially exact obstacle to this.

5.2 Finding a small cyclotomic class

In a case of particular interest we can show that the answer is always positive by proving that the obstacle cannot exist. The case in point occurring in several of the applications indicated is addressed by the Theorem 5.1 below.

We use the following notation. Given a polynomial $p(x) = a_nx^n + \cdots + a_0$ we let $||p||_1 = \sum_{j=0}^{n} |a_j|$ and $||p|| = (\sum_{j=0}^{n} a_j^2)^{1/2}$. As usual, Φ_d denotes the d-th

cyclotomic polynomial and $\varphi(d) = \deg \Phi_d$ is Euler's φ function.

THEOREM 5.1. *Let $m = p^k$ be a prime power and let $d \mid p-1$. There exist integers $t_1, \dots, t_d$ from distinct residue classes* mod p *such that*

- $|t_j| \le C_d p^{k-(k-1)/\varphi(d)}$; *and*
- $t_1^d \equiv \cdots \equiv t_d^d \pmod{p^k}$,

where

$$C_d = d\|\Phi_d\|^{(d-1)/\varphi(d)}.$$

In the case that d is a prime power we have

$$C_d \le d^{3/2}.$$

We devote the rest of this section to the proof of Theorem 5.1.

5.3 A lower bound on the coefficients

Let w be a primitive d-th root of unity in $\mathbb{Z}/p^k\mathbb{Z}$, so $A := \{w^0, \dots, w^{d-1}\}$ is the set of d-th roots of unity in $\mathbb{Z}/p^k\mathbb{Z}$. Then $t_j = w^{i-1}t_1$, so we are looking for $Q := t_1$ such that all the elements of QA are small in absolute value mod p^k. To eliminate the obstacle stated in Theorem 1.1, we need to show that there is no integer combination of $w^0/p^k, \dots, w^{d-1}/p^k$ with small coefficients that is congruent to $1/p$ modulo 1. This will follow from the following result.

LEMMA 5.2. *Let $w^0, \dots, w^{d-1}$ be the d-th roots of unity in $\mathbb{Z}/p^k\mathbb{Z}$. Suppose that $a_1, \dots, a_d \in \mathbb{Z}$ are such that $\sum_{j=1}^d a_j w^{j-1} = p^\ell \cdot s$, where $\gcd(s,p) = 1$ and $\ell < k$. Then*

$$\sum_{j=1}^d a_j^2 \ge \frac{p^{2\ell/\varphi(d)}}{D_d},$$

where

$$D_d = \|\Phi_d\|^{2(d-1)/\varphi(d)}.$$

For estimates of $\|\Phi_d\|$, see the end of this section.

Proof of Theorem 5.1 from Lemma 5.2: Let $\alpha_j = w^j/p^k$. From Lemma 5.2 it follows that for any $a_1, \dots, a_d$ such that

$$\sum_{j=1}^d a_j \alpha_j = \frac{1}{p} + t, \ t \in \mathbb{Z},$$

their ℓ_2-norm must be large;

$$\sum_{j=1}^d a_j^2 \ge \frac{p^{2(k-1)/\varphi(d)}}{D_d}.$$

Hence, by Theorem 1.1, there exists a simultaneous diophantine ε-approximation $P_1, \dots, P_d, Q$ of $\alpha_1, \dots, \alpha_d$ excluding p with

$$\varepsilon = \frac{d\sqrt{D_d}}{p^{(k-1)/\varphi(d)}}.$$

Noting that $C_d = d\sqrt{D_d}$, we have $|Qw^j - P_j p^k| \le \varepsilon p^k \le C_d p^{k-(k-1)/\varphi(d)}$ and hence we can take $t_j = Qw^j - P_j p^k$.

If d is a prime power, $d = r^t$, we know the exact value of the ℓ_2-norm of Φ_d, $\|\Phi_d\| = \sqrt{r}$. Hence

$$C_d \le d(\sqrt{d^{1/t}})^{(r^t-1)/((r-1)r^{t-1})} \le d^{3/2}.$$

■

5.4 Proof of the lower bound

In this section we prove Lemma 5.2. Let $(\mathbb{Z}/m\mathbb{Z})^\times$ denote the group of units of the ring $\mathbb{Z}/m\mathbb{Z}$.

As before, let w be a primitive d-th root of unity in $\mathbb{Z}/p^k\mathbb{Z}$ where $d \mid p-1$.

PROPOSITION 5.1. $\Phi_d(w) \equiv 0 \pmod{p^k}$.

Proof: We have $\prod_{t \mid d} \Phi_t(w) = w^d - 1 \equiv 0 \pmod{p^k}$. On the other hand, the order of w in $\mathbb{Z}/p\mathbb{Z}$ is d (since $\gcd(d,p) = 1$). Therefore for $t < d$ we have $w^t - 1 \not\equiv 0 \pmod{p}$ and hence $\Phi_t(w) \not\equiv 0 \pmod{p}$. ■

Let $\mathrm{Res}(f,g)$ denote the resultant of the polynomials $f, g \in \mathbb{Z}[x]$. Recall that

(i) $\mathrm{Res}(f,g)$ is an integer;

(ii) $\mathrm{Res}(f,g) = 0$ if and only in $\gcd(f,g) \ne 1$;

(iii) There exist $u, v \in \mathbb{Z}[x]$ such that $\deg u < \deg g$, $\deg v < \deg f$ and $uf + vg = \mathrm{Res}(f,g)$;

(iv) $|\mathrm{Res}(f,g)| \le \|f\|^{\deg g} \|g\|^{\deg f}$.

Property **(iv)** follows by Hadamard's inequality applied to the Sylvester determinant form of the resultant.

In the next statement we do not assume that m is a prime power.

PROPOSITION 5.2. *Let $m \in \mathbb{Z}$. Let $f(x), g(x) \in \mathbb{Z}[x]$. If there is $a \in \mathbb{Z}$ such that $f(a) \equiv g(a) \equiv 0 \pmod{m}$ then* $\mathrm{Res}(f,g) \equiv 0 \pmod{m}$.

Proof: Substituting $x = a$ into **(iii)** we obtain the desired result. ■

Proof of Lemma 5.2: Let $f(x) = \sum_{j=1}^d a_j x^{j-1}$. We have $f(w) \equiv 0 \pmod{p^\ell}$. By Proposition 5.1 we have $\Phi_d(w) \equiv 0 \pmod{p^k}$. Hence by Proposition 5.2, $\mathrm{Res}(f, \Phi_d) \equiv 0 \pmod{p^\ell}$. Clearly f is not a multiple of Φ_d, because $f(w) \not\equiv 0 \pmod{p^k}$. Since Φ_d is irreducible

over $\mathbb{Q}$, $\mathrm{Res}(f, \Phi_d) \neq 0$. Thus, by properties **(i)**, **(ii)**, $|\mathrm{Res}(f, \Phi_d)| \geq p^\ell$. On the other hand, by property **(iv)**,

$$|\mathrm{Res}(f, \Phi_d)| \leq ||\Phi_d||^{d-1} ||f||^{\varphi(d)}.$$

Hence

$$\frac{p^{2\ell/\varphi(d)}}{||\Phi_d||^{2(d-1)/\varphi(d)}} \leq \sum_{j=1}^{d} a_j^2.$$

■

REMARK: The following two results give the logarithmic order of magnitude of $||\Phi_n||$ for the worst values of n.

THEOREM 5.3. (BATEMAN,[BAT49]) *For all n,*

$$||\Phi_n|| \leq ||\Phi_n||_1 \leq n^{d(n)/2} \leq \exp\left(n^{(1+o(1))\ln 2/\ln\ln n}\right)$$

where $d(n)$ is the number of positive divisors of n.

THEOREM 5.4. (ERDŐS,[ERD49]) *For infinitely many n,*

$$||\Phi_n|| \geq \exp\left(n^{c/\ln\ln n}\right)$$

for some constant $c > 0$.

6 Aproximating algebraic integers: an open problem

While our existence results (Theorems 1.1, 1.2, 3.1) concern the simultaneous approximability of sequences of *real* numbers α_i, our algorithmic results (Theorem 1.4) are limited to the case when the α_i are *rational*. A reviewer challenged us to extend the results to the case when the α_i are *algebraic*. (An algebraic number is represented by its minimal polynomial and an interval in which it lies).

A particularly interesting case arises when all the α_i are *algebraic integers*. In this case, our results guarantee that ϵ-approximations avoiding any finite set of primes always exist (since, if an integral linear combination of the α_i is rational then it is an integer). So, unlike in Theorem 1.4, there is no smallest ϵ and ϵ needs to be made part of the input.

It is conceivable, however, that the α_i have an integral linear combination with small coefficients which is doubly exponentially close to a non-integral rational number, say 1/2; in any case, doubly exponential is the best separation we are able to give. (The proof of the separation is modeled after Liouville's classical proof of the transcendence of certain real numbers.)

If the doubly exponential separation (say, from 1/2) is indeed nearly optimal then a $1/N$-approximation avoiding $p = 2$, where the bit-length of N is polynomially bounded in the description length of the α_i, would require Q to have exponentially many digits. We don't know whether this case can actually occur but it might, even in the special case when the α_i are square roots of integers.

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.

[Bat49] P. T. Bateman. Note on the coefficients of the cyclotomic polynomial. *Bulletin of the A. M. S.*, 55:1180–1181, 1949.

[BSŠ03] L. Babai, A. Shpilka, and D. Štefankovič. Locally testable cyclic codes. In *44th IEEE Symposium on Foundations of Computer Science (FOCS 2003)*. IEEE Computer Society, 2003.

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

[Erd49] P. Erdős. On the coefficients of the cyclotomic polynomial. *Portugaliae Mathematica*, 8:63–71, 1949.

[Kut01] S. Kutin. Personal communication. 2001.

[Lag84] J. C. Lagarias. Knapsack-type public key cryptosystems and diophantine approximation. *Advances in Cryptology (Santa Barbara, 1983)*, pages 3–23, 1984.

[Lag85] J. C. Lagarias. The computational complexity of simultaneous diophantine approximation problems. *SIAM Journal of Computing*, 14(1):196–209, 1985.

[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.

[OT85] A. M. Odlyzko and H. Te Reile. Disproof of the Mertens conjecture. *J. Reine Angew. Math.*, (357):138–160, 1985.

[Sha82] A. Shamir. A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystems. In *23rd IEEE Symposium on Foundations of Computer Science (FOCS 1982)*, pages 145–152. IEEE Computer Society, 1982.