Proof Mining in Diophantine Approximation Theory

(joint work Rob Arthan)

Paulo Oliva
Queen Mary University of London

Proof Mining Seminar
13 July 2022

Diophantine Approximation

Diophantine Approximation

Approximation of reals $\mathbb{R}$ by rationals $\mathbb{Q}$

- Rationals are dense in the real, so it's always possible to approximate a real by rationals
- But some approximations are better than others:

$$\pi \simeq \frac{314159}{100000} \text{ (good)} \qquad \pi \simeq \frac{355}{113} \text{ (better)}$$

Goal: Given $\alpha \in \mathbb{R}$ we want to study $p, q \in \mathbb{N}$ with $\gcd(p, q) = 1$ such that:

$$|\alpha - \frac{p}{q}| \text{ is small} \quad \text{(or equivalently, } |q\alpha - p| \text{ is small)}$$

Simple Lower Bound

Lemma. Let $\alpha = a/b \in \mathbb{Q}$ where $\gcd(a, b) = 1$. For any $p, q \in \mathbb{Z}$ such that $\alpha \neq p/q$ we have that $|q\alpha - p| \geq 1/b$.

Proof: If $a/b \neq p/q$ then $|qa - pb| \geq 1$ and hence:

$$|q\alpha - p| = |\frac{qa}{b} - p| \geq \frac{|qa - pb|}{b} \geq \frac{1}{b}$$

An Upper Bound

Theorem (Dirichlet Approximation Theorem). For any $\alpha \in \mathbb{R}$ and $Q \in \mathbb{N}$ there are coprime $p, q \in \mathbb{Z}$ such that $1 \leq q \leq Q$

$$|q\alpha - p| < \frac{1}{Q}$$

Proof:

1. Divide the interval $[0,1)$ into Q intervals of equal size $1/Q$
2. Look at fractional parts of $0, \alpha, 2\alpha, 3\alpha, \ldots, Q\alpha$
3. Two of these (say $\{i\alpha\}, \{j\alpha\}$) will fall into the same interval
4. Then $|\{j\alpha\} - \{i\alpha\}| < 1/Q$
5. $|\{j\alpha\} - \{i\alpha\}| = |j\alpha - p_j - (i\alpha - p_i)| = |(j-i)\alpha - (p_j - p_i)|$

A Corollary

Corollary. If $\alpha \in \mathbb{R}$ is irrational then there are infinitely many $p/q \in \mathbb{Q}$ with $\gcd(p, q) = 1$, $q \geq 1$, such that

$$|\alpha - \frac{p}{q}| < \frac{1}{q^2}$$

Proof:

1. Assume there are only finitely many $p_1/q_1, \ldots, p_n/q_n$
2. Since $\alpha \notin \mathbb{Q}$ we have that $|\alpha - p_i/q_i| \neq 0$
3. Chose Q such that $1/Q < \min |\alpha - p_i/q_i|$
4. From theorem, $|\alpha - p/q| < 1/qQ$, for some p and $q \leq Q$
5. So, $p/q \neq p_i/q_i$ but $|\alpha - p/q| < 1/qQ \leq 1/q^2$, contradiction

Roth’s Theorem

Theorem (1955). If $\alpha \in \mathbb{R}$ is an irrational algebraic number then for every $\varepsilon > 0$ then the following has only finitely many solutions (p, q) with $\gcd(p, q) = 1$

$$|\alpha - \frac{p}{q}| < \frac{1}{q^{2+\varepsilon}}$$

- Roth’s proof is ineffective
- Focus of early work on “proof mining” (Kreisel and Luckhardt)

Khintchine Theorem

Khintchine Theorem

Let $\psi: \mathbb{N} \rightarrow \mathbb{R}^+$ such that $q\psi(q)$ is non-decreasing. A real number $\alpha \in [0,1]$ is call ψ-**approximable** if there are infinitely many rationals p/q such that

$$|\alpha - \frac{p}{q}| < \frac{\psi(q)}{q}$$

Theorem (Khintchine, 1926).

- If $\Sigma_q \psi(q)$ diverges almost every $x \in [0,1]$ is ψ-**approximable**
- If $\Sigma_q \psi(q)$ converges almost every $x \in [0,1]$ is not ψ-**approximable**

2022 Fields Medal…

- Duffin & Schaeffer (1941) proved a generalisation of Khintchine's result…
- …and posed what is known as the **Duffin-Schaeffer conjecture**, an analogue of Khintchine's result for ψ which are not necessarily decreasing
- Dimitris Koukoulopoulos and **James Maynard** announced proof of this conjecture in 2019
- James Maynard was awarded the **Fields Medal** this year for "contributions to analytic number theory, which have led to major advances in the understanding of the structure of prime numbers and in **Diophantine approximation**"

Generalisation

For $\mathbf{X} \in \mathbb{I}^{nm}$ (unit cube) and $\psi : \mathbb{N} \to \mathbb{R}^+$

supremum norm

- $N(\psi, \mathbf{X}) \equiv |\{(p,q) \mid |q\mathbf{X} - p| < \psi(|q|), \gcd(p,q) = 1\}|$
- $\mathscr{A}_{n,m}(\psi) \equiv \{\mathbf{X} \in \mathbb{I}^{nm} \mid N(\psi, \mathbf{X}) = \infty\}$

$p \in \mathbb{Z}^m, q \in \mathbb{Z}^n$

Theorem (Khintchine-Groshev).

Lebesgue measure

- If $\Sigma_q q^{n-1}\psi(q)^m$ diverges (ψ mon.) then $|\mathscr{A}_{n,m}(\psi)| = 1$
- If $\Sigma_q q^{n-1}\psi(q)^m$ converges then $|\mathscr{A}_{n,m}(\psi)| = 0$

Beresnevich-Velani Proof

Theorem (Khintchine-Groshev).

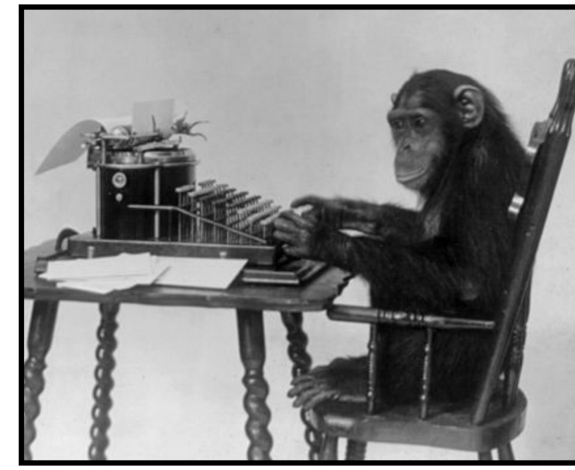
- If $\Sigma_q q^{n-1}\psi(q)^m$ (ψ mon.) diverges then $|\mathscr{A}_{n,m}(\psi)| = 1$

Proof: Two key lemmas

- Lemma 1: For all $n, m \geq 1$ and $\psi : \mathbb{N} \to \mathbb{R}^+$
$$|\mathscr{A}_{n,m}(\psi)| > 0 \quad \Rightarrow \quad |\mathscr{A}_{n,m}(\psi)| = 1$$
- Lemma 2: Given sequence of measurable sets $E_k \subset \mathbb{I}^{nm}$ such that $\Sigma_{k=1}^{\infty} |E_k| = \infty$ then
$$|\limsup_{k\to\infty} E_k| \geq \limsup_{N\to\infty} \frac{(\Sigma_{s=1}^{N} |E_s|)^2}{\Sigma_{s,t=1}^{N} |E_s \cap E_t|}$$

Borel-Cantelli Lemma

The Infinite Monkey Theorem



Theorem (Borel, 1913). A monkey hitting keys at random on a typewriter keyboard for an infinite amount of time will almost surely type any given text, such as the complete works of William Shakespeare.

Proof: Let A_i be the event that the text is typed at the i-th block. Since the A_i are independent and have fixed non-zero probability

$$\sum_i P[A_i] = \infty$$

By the second **Borel-Cantelli** lemma the probability of A_i *i.o.* is 1

$(\Omega, \mathscr{F}, P)$ a **probability space**:

- Ω is the **sample space** (elements of Ω are called **outcomes**)
- $\mathscr{F} \subseteq 2^{\Omega}$ is **event space** (set of events)
- $P : \mathscr{F} \to [0,1]$ is the **probability function**

Definition. Given $(A_i)_{i\in\mathbb{N}}$ a sequence of events, we denote by "$(A_i)_{i\in\mathbb{N}}$ *i.o.*" the event

$$(A_i)_{i\in\mathbb{N}}\ i.o. = \{x \in \Omega \mid \forall i\, \exists j \geq i (x \in A_j)\}$$

or equivalently

$$(A_i)_{i\in\mathbb{N}}\ i.o. = \bigcap_i \bigcup_{j\geq i} A_j$$

Question. When do we have $P[(A_i)_{i\in\mathbb{N}}\ i.o] = 1$ or 0?

Borel-Cantelli Lemmas

1st B-C Lemma. If $\Sigma_i P[A_i] < \infty$ then $P[(A_i)_{i \in \mathbb{N}}\ i.o] = 0$.

2nd B-C Lemma. If the events are mutually independent then $\Sigma_i P[A_i] = \infty$ implies $P[(A_i)_{i \in \mathbb{N}}\ i.o] = 1$.

An example of **0-1 law**: For mutually independent events A_i we have that $P[(A_i)_{i \in \mathbb{N}}\ i.o]$ is either 0 or 1, depending on whether $\Sigma_i P[A_i]$ converges or diverges.

2nd B-C Lemma. If the events are mutually independent then $\Sigma_i P[A_i] = \infty$ implies $P[(A_i)_{i\in\mathbb{N}}\ i.o] = 1$.

Generalisation 1 (Erdős-Rényi, 1959). If $\Sigma_i P[A_i] = \infty$ and

$$\liminf_{n\to\infty} \frac{\sum_{i,k=1}^{n} P[A_i A_k]}{\left(\sum_{k=1}^{n} P[A_k]\right)^2} = 1$$

then $P[(A_i)_{i\in\mathbb{N}}\ i.o] = 1$.

Generalisation 2 (Kochen-Stone, 1964). If $\Sigma_i P[A_i] = \infty$ then

$$P[(A_i)_{i\in\mathbb{N}}\ i.o] \geq \limsup_{n\to\infty} \frac{\left(\sum_{k=1}^{n} P[A_k]\right)^2}{\sum_{i,k=1}^{n} P[A_i A_k]}$$

Quantitative versions of the four above results…

$$\Sigma_i P[A_i] < \infty$$

$$\forall l \exists k \forall m \geq k \left(\sum_{i=k}^{m} P[A_i] \leq \frac{1}{2^l} \right)$$

$$P[(A_i)_{i \in \mathbb{N}}\ i.o] = 0$$

$$\forall l \exists k \forall m \geq k \left(P\left[\bigcup_{i=k}^{m} A_i \right] \leq \frac{1}{2^l} \right)$$

1st B-C Lemma

1st B-C Lemma. If $\Sigma_i P[A_i] < \infty$ then $P[(A_i)_{i \in \mathbb{N}}\ i.o] = 0$.

Quantitative version (Arthan-O'2020). Let $\phi : \mathbb{N} \to \mathbb{N}$ be such that for all $l \geq 0$ and $m \geq \phi(l)$

$$\sum_{i=\phi(l)}^{m} P[A_i] \leq \frac{1}{2^l}$$

Then for all $l \geq 0$ and $m \geq \phi(l)$

$$P\left[\bigcup_{i=\phi(l)}^{m} A_i\right] \leq \frac{1}{2^l}$$

2nd B-C Lemma

2nd B-C Lemma. If the events are mutually independent then $\Sigma_i P[A_i] = \infty$ implies $P[(A_i)_{i \in \mathbb{N}}\ i.o] = 1$.

Quantitative version (Arthan-O'2020). Let $\omega : \mathbb{N} \to \mathbb{N}$ be such that for all N

$$\sum_{i=1}^{\omega(N)} P[A_i] \geq N$$

Then for all n and l

$$P\left[\bigcup_{i=n}^{\omega(n+l-1)} A_i\right] \geq 1 - e^{-l}$$

Erdős-Rényi Generalisation

$$\liminf_{n\to\infty} \frac{\sum_{i,k=1}^{n} P[A_i A_k]}{(\sum_{k=1}^{n} P[A_k])^2} = 1$$

$$\forall \varepsilon, n \, \exists m \geq n \left(\left| \frac{\sum_{i,k=1}^{m} P[A_i A_k]}{(\sum_{k=1}^{m} P[A_k])^2} - 1 \right| < \varepsilon \right)$$

Quantitative Erdős-Rényi Theorem (Arthan-O'2020). Let $\omega\colon \mathbb{N} \to \mathbb{N}$ be such that

$$\forall N \left(\sum_{i=1}^{\omega(N)} P[A_i] \geq N \right)$$

Quantitative Erdős-Rényi Theorem (Arthan-O'2020). Let $\omega \colon \mathbb{N} \to \mathbb{N}$ be such that

$$\forall N \left(\sum_{i=1}^{\omega(N)} P[A_i] \geq N \right)$$

and let $\phi \colon \mathbb{Q} \times \mathbb{N} \to \mathbb{N}$ be such that

$$\forall \varepsilon, n \left(\phi(\varepsilon, n) \geq n \wedge \frac{\sum_{i,k=1}^{\phi(\varepsilon,n)} P[A_i A_k]}{(\sum_{i=1}^{\phi(\varepsilon,n)} P[A_i])^2} \leq 1 + \varepsilon \right)$$

Quantitative Erdős-Rényi Theorem (Arthan-O'2020). Let $\omega\colon \mathbb{N} \to \mathbb{N}$ be such that

$$\forall N \left(\sum_{i=1}^{\omega(N)} P[A_i] \geq N \right)$$

and let $\phi\colon \mathbb{Q} \times \mathbb{N} \to \mathbb{N}$ be such that

$$\forall \varepsilon, n \left(\phi(\varepsilon, n) \geq n \wedge \frac{\sum_{i,k=1}^{\phi(\varepsilon,n)} P[A_i A_k]}{(\sum_{i=1}^{\phi(\varepsilon,n)} P[A_i])^2} \leq 1 + \varepsilon \right)$$

Let $n_1 = \phi(1/2, 1)$ and $n_{i+1} = \phi(1/2^{i+1}, n_i)$. Then

$$\forall n, l \left(P\left[\bigcup_{i=n}^{n_m} A_i \right] \geq 1 - 2^{-l} \right)$$

where $m = \max(\omega(2n), l + 3)$

Kochen-Stone Theorem

$$P[(A_i)_{i\in\mathbb{N}}\ i.o] \geq \limsup_{n\to\infty} \frac{\left(\sum_{k=1}^{n} P[A_k]\right)^2}{\sum_{i,k=1}^{n} P[A_i A_k]}$$

$$\Downarrow$$

$$\forall m, l\, \exists n > m\, \forall j > n \left(P\left[\bigcup_{i=m+1}^{n} A_i\right] + \frac{1}{2^l} \geq \frac{\left(\sum_{k=1}^{j} P[A_k]\right)^2}{\sum_{i,k=1}^{j} P[A_i A_k]} \right)$$

Theorem (Arthan-O'2020). There is a sequence of events $(A_i)_{i=1}^{\infty}$ and a computable function $\omega : \mathbb{N} \to \mathbb{N}$ such that

$$\forall N \left(\sum_{i=1}^{\omega(N)} P[A_i] \geq N \right)$$

for which there is no computable function $\phi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ such that $\forall m, l \exists n \in [m, \phi(m, l)]$

$$P\left[\bigcup_{i=m+1}^{n} A_i \right] + \frac{1}{2^l} \geq \limsup_{j \to \infty} \frac{\left(\sum_{k=1}^{j} P[A_k] \right)^2}{\sum_{i,k=1}^{j} P[A_i A_k]}$$

Hence, we consider the **meta-stable** version of the Kochen-Stone theorem

Quantitative (meta-stable) Kochen-Stone (Arthan-O'2020).

Let $\omega : \mathbb{N} \to \mathbb{N}$ be such that

$$\forall N \left(\sum_{i=1}^{\omega(N)} P[A_i] \geq N \right)$$

Then, for all m and l and $g : \mathbb{N} \to \mathbb{N}$ (with $g(i) > i$) there exists an $n \in [m, g^{(2^{l+1})}(\max(\omega(2^{l+2}\Sigma_{i=1}^{m} P[A_i]), m)]$ such that

$$\forall j \in [n, g(n)] \left(P\left[\bigcup_{i=m+1}^{n} A_i \right] + \frac{1}{2^l} \geq \frac{(\sum_{i=1}^{j} P[A_i])^2}{\sum_{i,k=1}^{j} P[A_i A_k]} \right)$$

Work in Progress…

METRIC SIMULTANEOUS DIOPHANTINE APPROXIMATION (II)

P. X. GALLAGHER

THEOREM 1. *Let* $r \geqslant 2$. *For each sequence of numbers* a_n *between* 0 *and* 1, *there are infinitely many solutions* n, $\mathbf{l}$ *of*

$$n\mathbf{x} - \mathbf{l} \in U(a_n), \quad (\mathbf{l}, n) = 1 \tag{2}$$

for almost all $\mathbf{x}$ *or almost no* $\mathbf{x}$ *according as* $\sum a_n{}^r$ *diverges or converges.*

[MATHEMATIKA 12 (1965), 123–127]

J

THEOREM 1. *Let* $r \geqslant 2$. *For each sequence of numbers* a_n *between* 0 *and* 1, *there are infinitely many solutions* n, $\mathbf{l}$ *of*

$$n\mathbf{x} - \mathbf{l} \in U(a_n), \quad (\mathbf{l}, n) = 1 \tag{2}$$

for almost all $\mathbf{x}$ *or almost no* $\mathbf{x}$ *according as* $\Sigma a_n{}^r$ *diverges or converges.*

Let $r \geq 2$ and $(a_n)_{n \in \mathbb{N}} \in [0,1]$

- $U(a) = \{(y_1, \ldots, y_r) \in \mathbb{R}^r \mid 0 \leq y_i < a\}$
- $T_N(\mathbf{x}) = \{(n, l) \mid n\mathbf{x} - l \in U(a_n) \wedge (l, n) = 1 \wedge n \leq N\}$
- $E(K) = \{\mathbf{x} \in U(1) \mid \exists N(T_N(\mathbf{x}) \geq K\}$
- $E = \cap_K E(K)$

Theorem (Gallagher, 1965).

- If $\Sigma_n a_n^r$ converges then $|E| = 0$
- If $\Sigma_n a_n^r$ diverges then $|E| = 1$

Theorem (Gallagher, 1965).

- If $\Sigma_n a_n^r$ diverges then $|E| = 1$

Proof: Assume $\Sigma_n a_n^r$ diverges

- Use Schwarz inequality to show that $|E(K)| \geq C$
- Find sequence $(b_n)_{n\in\mathbb{N}} \in [0,1]$ which is $b_n = o(a_n)$ such that $\Sigma_n b_n^r$ also diverges (call corresponding set E^*)
- Identify $U(1)$ with torus $T^r = \mathbb{R}^r/$(lattice vectors)
- Show that for the ergodic automorphism
  $$\sigma(x_1, x_2, \ldots, x_r) = (x_2, x_3, \ldots, x_1 + \ldots + x_r)$$
  we have $\sigma U(c) \subset U(rc)$
- $\sigma^q E^* \subset E$, for all q, so $\cup_q \sigma^q E^* \subset E$
- Since σ is ergodic and $\cup_q \sigma^q E^* > 0$ then $\cup_q \sigma^q E^* = 1$

Final Mining Step

Theorem (qualitative). Given a torus automorphism σ and some $|E| > 0$ we have that

$$|\bigcup_{q \in \mathbb{N}} \sigma^{-q}(E)| = 1$$

Theorem (quantitative). Given a torus automorphism σ, there exists a function η such that

$$\forall \varepsilon, \delta \left(|E| > \varepsilon \to |\bigcup_{1 \le q \le \eta(\varepsilon, \delta)} \sigma^{-q}(E)| > 1 - \delta \right)$$

Conclusion

- Quantitative version of the (**constructive**) proofs of 1st and 2nd Borel-Cantelli lemmas, and Erdős-Rényi generalisation.
- Quantitative (meta-stable) version of the (**classical**) proof of the Kochen-Stone theorem.
- Original motivation for quantitative version of Borel-Cantelli lemma lies on current proof mining project on **Diophantine approximation** (Khintchine's convergence and divergence theorems).

References

[1] Pál Erdős and Alfréd Rényi. On Cantor's series with convergent $\sum 1/q_n$. *Ann. Univ. Sci. Budap. Rolando Eötvös, Sect. Math.*, 2:93–109, 1959.

[2] W. Feller. *An Introduction to Probability Theory and Its Applications. I. Third Edition.* John Wiley and Sons, Inc., 1968.

[3] S. Kochen and C. Stone. A note on the Borel-Cantelli lemma. *Ill. J. Math.*, 8:248–251, 1964.

[4] Ernst Specker. Nicht konstruktiv beweisbare Sätze der Analysis. *J. Symb. Log.*, 14:145–158, 1949.

[5] Jia-An Yan. A simple proof of two generalized Borel-Cantelli lemmas. In Michel Émery and Marc Yor, editors, *In memoriam Paul-André Meyer. Séminaire de probabilités XXXIX*, volume 1874 of *Lecture Notes in Mathematics*, pages 77–79. Springer, 2006.