

Diophantine approximation in positive characteristic and linear complexity profiles

Simon Kristensen

Department of Mathematical Sciences
University of Aarhus

Aarhus, 14/4/2009

Linear complexity profiles

Diophantine approximation over \mathbb{R}

Diophantine approximation in positive characteristic

Higher dimensional problems

Ideas of proofs

Outline

1 Linear complexity profiles

Linear complexity profiles

Diophantine approximation over \mathbb{R}

Diophantine approximation in positive characteristic

Higher dimensional problems

Ideas of proofs

Outline

- 1 Linear complexity profiles
- 2 Diophantine approximation over \mathbb{R}

Outline

- 1 Linear complexity profiles
- 2 Diophantine approximation over \mathbb{R}
- 3 Diophantine approximation in positive characteristic

Outline

- 1 Linear complexity profiles
- 2 Diophantine approximation over \mathbb{R}
- 3 Diophantine approximation in positive characteristic
- 4 Higher dimensional problems

Outline

- 1 Linear complexity profiles
- 2 Diophantine approximation over \mathbb{R}
- 3 Diophantine approximation in positive characteristic
- 4 Higher dimensional problems
- 5 Ideas of proofs

Outline

- 1 Linear complexity profiles
- 2 Diophantine approximation over \mathbb{R}
- 3 Diophantine approximation in positive characteristic
- 4 Higher dimensional problems
- 5 Ideas of proofs

Stream ciphers

A *stream cipher* over \mathbb{F}_q is a cryptosystem as follows.

Stream ciphers

A *stream cipher* over \mathbb{F}_q is a cryptosystem as follows.

- A *message* M is a (possibly finite) sequence in $\mathbb{F}_q^{\mathbb{N}}$.

Stream ciphers

A *stream cipher* over \mathbb{F}_q is a cryptosystem as follows.

- A *message* M is a (possibly finite) sequence in $\mathbb{F}_q^{\mathbb{N}}$.
- A *keystream* K is a (private) sequence in $\mathbb{F}_q^{\mathbb{N}}$.

Stream ciphers

A *stream cipher* over \mathbb{F}_q is a cryptosystem as follows.

- A *message* M is a (possibly finite) sequence in $\mathbb{F}_q^{\mathbb{N}}$.
- A *keystream* K is a (private) sequence in $\mathbb{F}_q^{\mathbb{N}}$.
- Encryption is termwise addition of M with K .

Stream ciphers

A *stream cipher* over \mathbb{F}_q is a cryptosystem as follows.

- A *message* M is a (possibly finite) sequence in $\mathbb{F}_q^{\mathbb{N}}$.
- A *keystream* K is a (private) sequence in $\mathbb{F}_q^{\mathbb{N}}$.
- Encryption is termwise addition of M with K .
- Decryption is termwise subtraction of K from encrypted message.

Stream ciphers

A *stream cipher* over \mathbb{F}_q is a cryptosystem as follows.

- A *message* M is a (possibly finite) sequence in $\mathbb{F}_q^{\mathbb{N}}$.
- A *keystream* K is a (private) sequence in $\mathbb{F}_q^{\mathbb{N}}$.
- Encryption is termwise addition of M with K .
- Decryption is termwise subtraction of K from encrypted message.

Evidently, the keystream should be as random as possible to avoid Caesar ciphers and simple modifications.

Linear complexity

Definition

Let $n \in \mathbb{N}$ and let S be a finite or infinite sequence over \mathbb{F}_q . The n 'th linear complexity is given by

$$L_n(S) = \min\{k \in \mathbb{N} : (s_1, \dots, s_n) \\ \text{are generated by a } k\text{-term recurrence}\}$$

Linear complexity

Definition

Let $n \in \mathbb{N}$ and let S be a finite or infinite sequence over \mathbb{F}_q . The n 'th linear complexity is given by

$$L_n(S) = \min\{k \in \mathbb{N} : (s_1, \dots, s_n) \\ \text{are generated by a } k\text{-term recurrence}\}$$

- $0 \leq L_n(S) \leq n$.

Linear complexity

Definition

Let $n \in \mathbb{N}$ and let S be a finite or infinite sequence over \mathbb{F}_q . The n 'th linear complexity is given by

$$L_n(S) = \min\{k \in \mathbb{N} : (s_1, \dots, s_n) \\ \text{are generated by a } k\text{-term recurrence}\}$$

- $0 \leq L_n(S) \leq n$.
- Extremal values give non-random behaviour.

Linear complexity

Definition

Let $n \in \mathbb{N}$ and let S be a finite or infinite sequence over \mathbb{F}_q . The n 'th linear complexity is given by

$$L_n(S) = \min\{k \in \mathbb{N} : (s_1, \dots, s_n) \\ \text{are generated by a } k\text{-term recurrence}\}$$

- $0 \leq L_n(S) \leq n$.
- Extremal values give non-random behaviour.
- The Berlekamp–Massey algorithm gives a way of determining the value.

Linear complexity profiles

- **Problem:** The longer the message, the longer the needed keystream.

Linear complexity profiles

- **Problem:** The longer the message, the longer the needed keystream.
- It is desirable to have a complexity measure, which works at all scales.

Linear complexity profiles

- **Problem:** The longer the message, the longer the needed keystream.
- It is desirable to have a complexity measure, which works at all scales.

Definition

Let S be an infinite sequence over \mathbb{F}_q . The sequence $L_1(S), L_2(S), \dots$ is called the linear complexity profile of S .

Linear complexity profiles

- **Problem:** The longer the message, the longer the needed keystream.
- It is desirable to have a complexity measure, which works at all scales.

Definition

Let S be an infinite sequence over \mathbb{F}_q . The sequence $L_1(S), L_2(S), \dots$ is called the linear complexity profile of S .

- It can be shown that for a ‘random’ (whatever that means) sequence S ,

$$L_n(S) = \frac{n}{2} + O(\log n).$$

Linear complexity profiles

- **Problem:** The longer the message, the longer the needed keystream.
- It is desirable to have a complexity measure, which works at all scales.

Definition

Let S be an infinite sequence over \mathbb{F}_q . The sequence $L_1(S), L_2(S), \dots$ is called the linear complexity profile of S .

- It can be shown that for a ‘random’ (whatever that means) sequence S ,

$$L_n(S) = \frac{n}{2} + O(\log n).$$

- It is desirable that the error term is as small as possible.

(Almost) Perfection

- Perfection of a sequence is a measure of the deviation from the main term.

(Almost) Perfection

- Perfection of a sequence is a measure of the deviation from the main term.
- Let $d \in \mathbb{N}$. A sequence S is called *d-perfect* if for any $n \geq 1$,

$$|2L_n(S) - n| \leq d.$$

(Almost) Perfection

- Perfection of a sequence is a measure of the deviation from the main term.
- Let $d \in \mathbb{N}$. A sequence S is called *d-perfect* if for any $n \geq 1$,

$$|2L_n(S) - n| \leq d.$$

- A 1-perfect sequence is called *perfect*.

(Almost) Perfection

- Perfection of a sequence is a measure of the deviation from the main term.
- Let $d \in \mathbb{N}$. A sequence S is called *d-perfect* if for any $n \geq 1$,

$$|2L_n(S) - n| \leq d.$$

- A 1-perfect sequence is called *perfect*.
- A sequence, which is *d-perfect* for some d , is called *almost perfect*.

(Almost) Perfection

- Perfection of a sequence is a measure of the deviation from the main term.
- Let $d \in \mathbb{N}$. A sequence S is called *d-perfect* if for any $n \geq 1$,

$$|2L_n(S) - n| \leq d.$$

- A 1-perfect sequence is called *perfect*.
- A sequence, which is *d-perfect* for some d , is called *almost perfect*.
- Two good questions:

(Almost) Perfection

- Perfection of a sequence is a measure of the deviation from the main term.
- Let $d \in \mathbb{N}$. A sequence S is called d -perfect if for any $n \geq 1$,

$$|2L_n(S) - n| \leq d.$$

- A 1-perfect sequence is called *perfect*.
- A sequence, which is d -perfect for some d , is called *almost perfect*.
- Two good questions:
 - ① How many d -perfect/almost perfect sequences are there?

(Almost) Perfection

- Perfection of a sequence is a measure of the deviation from the main term.
- Let $d \in \mathbb{N}$. A sequence S is called *d-perfect* if for any $n \geq 1$,

$$|2L_n(S) - n| \leq d.$$

- A 1-perfect sequence is called *perfect*.
- A sequence, which is *d-perfect* for some d , is called *almost perfect*.
- Two good questions:
 - 1 How many *d-perfect/almost perfect* sequences are there?
 - 2 How can we make one?

A curious relation

For a sequence $S = (s_i)$, define the *generating function*

$$G = \sum_{i=1}^{\infty} s_i T^{-i}.$$

A curious relation

For a sequence $S = (s_i)$, define the *generating function*

$$G = \sum_{i=1}^{\infty} s_i T^{-i}.$$

Theorem (Niederreiter (1988))

A sequence S is d -perfect iff the generating function G is *irrational* and has *partial quotients* of degree bounded by d .

A curious relation

For a sequence $S = (s_i)$, define the *generating function*

$$G = \sum_{i=1}^{\infty} s_i T^{-i}.$$

Theorem (Niederreiter (1988))

A sequence S is d -perfect iff the generating function G is *irrational* and has *partial quotients* of degree bounded by d .

- This looks like mathematics!

A curious relation

For a sequence $S = (s_i)$, define the *generating function*

$$G = \sum_{i=1}^{\infty} s_i T^{-i}.$$

Theorem (Niederreiter (1988))

A sequence S is d -perfect iff the generating function G is *irrational* and has *partial quotients* of degree bounded by d .

- This looks like mathematics!
- It even looks like number theory!!

A curious relation

For a sequence $S = (s_i)$, define the *generating function*

$$G = \sum_{i=1}^{\infty} s_i T^{-i}.$$

Theorem (Niederreiter (1988))

A sequence S is d -perfect iff the generating function G is *irrational* and has *partial quotients* of degree bounded by d .

- This looks like mathematics!
- It even looks like number theory!!
- This makes me happy!!!

Outline

- 1 Linear complexity profiles
- 2 Diophantine approximation over \mathbb{R}**
- 3 Diophantine approximation in positive characteristic
- 4 Higher dimensional problems
- 5 Ideas of proofs

Dirichlet's Theorem

- We briefly review some classical theory.

Dirichlet's Theorem

- We briefly review some classical theory.
- Applying the pigeon hole principle, we show that if $x \in \mathbb{R} \setminus \mathbb{Q}$, then

$$\left| x - \frac{p}{q} \right| < \frac{1}{q^2}$$

for infinitely many $p/q \in \mathbb{Q}$.

Dirichlet's Theorem

- We briefly review some classical theory.
- Applying the pigeon hole principle, we show that if $x \in \mathbb{R} \setminus \mathbb{Q}$, then

$$\left| x - \frac{p}{q} \right| < \frac{1}{q^2}$$

for infinitely many $p/q \in \mathbb{Q}$.

- There are numbers x for which there is a $K(x) > 0$ such that

$$\left| x - \frac{p}{q} \right| \geq \frac{K(x)}{q^2}$$

Dirichlet's Theorem

- We briefly review some classical theory.
- Applying the pigeon hole principle, we show that if $x \in \mathbb{R} \setminus \mathbb{Q}$, then

$$\left| x - \frac{p}{q} \right| < \frac{1}{q^2}$$

for infinitely many $p/q \in \mathbb{Q}$.

- There are numbers x for which there is a $K(x) > 0$ such that

$$\left| x - \frac{p}{q} \right| \geq \frac{K(x)}{q^2}$$

- **Questions:** How do we find the p/q from the first condition, and how do we determine whether a number is badly approximable?

Continued fractions

- Continued fractions provide an answer (construction on blackboard).

Continued fractions

- Continued fractions provide an answer (construction on blackboard).
- The a_i are the *partial quotients*.

Continued fractions

- Continued fractions provide an answer (construction on blackboard).
- The a_i are the *partial quotients*.
- The rationals p_n/q_n determined by the recurrences

$$q_{-1} = 0, q_0 = 1, q_n = a_n q_{n-1} + q_{n-2}$$

$$p_{-1} = 1, p_0 = a_0, p_n = a_n p_{n-1} + p_{n-2}$$

give best approximants.

Continued fractions

- Continued fractions provide an answer (construction on blackboard).
- The a_i are the *partial quotients*.
- The rationals p_n/q_n determined by the recurrences

$$q_{-1} = 0, q_0 = 1, q_n = a_n q_{n-1} + q_{n-2}$$

$$p_{-1} = 1, p_0 = a_0, p_n = a_n p_{n-1} + p_{n-2}$$

give best approximants.

- A number is badly approximable iff the sequence of partial quotients is bounded.

Continued fractions

- Continued fractions provide an answer (construction on blackboard).
- The a_i are the *partial quotients*.
- The rationals p_n/q_n determined by the recurrences

$$q_{-1} = 0, q_0 = 1, q_n = a_n q_{n-1} + q_{n-2}$$

$$p_{-1} = 1, p_0 = a_0, p_n = a_n p_{n-1} + p_{n-2}$$

give best approximants.

- A number is badly approximable iff the sequence of partial quotients is bounded.
- Note:** The latter resembles the condition in Niederreiter's result.

Metrical results

Theorem (Khintchine (1924))

Let $\psi : \mathbb{N} \rightarrow \mathbb{R}_+$ be non-increasing. The set of $x \in \mathbb{R}$ for which

$$\left| x - \frac{p}{q} \right| < \psi(q)$$

has infinitely many solutions p/q is null (full) with respect to Lebesgue measure according to the convergence (divergence) of $\sum q\psi(q)$.

Metrical results

Theorem (Khintchine (1924))

Let $\psi : \mathbb{N} \rightarrow \mathbb{R}_+$ be non-increasing. The set of $x \in \mathbb{R}$ for which

$$\left| x - \frac{p}{q} \right| < \psi(q)$$

has infinitely many solutions p/q is null (full) with respect to Lebesgue measure according to the convergence (divergence) of $\sum q\psi(q)$.

Corollary

Almost no numbers are badly approximable.

Hausdorff dimension

- Hausdorff measure and dimension give an estimate of the size of a null-set.

Hausdorff dimension

- Hausdorff measure and dimension give an estimate of the size of a null-set.
- For $s \geq 0$ and $E \subseteq X$, a metric space, let

$$\mathcal{H}^s(E) = \liminf_{\delta \rightarrow 0} \inf_{\mathcal{C}_\delta} \sum_{U \in \mathcal{C}_\delta} (\text{diam } U)^s,$$

where the infimum is over δ -covers.

Hausdorff dimension

- Hausdorff measure and dimension give an estimate of the size of a null-set.
- For $s \geq 0$ and $E \subseteq X$, a metric space, let

$$\mathcal{H}^s(E) = \liminf_{\delta \rightarrow 0} \inf_{\mathcal{C}_\delta} \sum_{U \in \mathcal{C}_\delta} (\text{diam } U)^s,$$

where the infimum is over δ -covers.

- Define the *Hausdorff dimension* of E by

$$\dim(E) = \inf\{s \geq 0 : \mathcal{H}^s(E) = 0\} = \sup\{s > 0 : \mathcal{H}^s(E) = \infty\}.$$

Exceptional sets

Theorem (Jarník (1928))

The set of badly approximable real numbers has Hausdorff dimension 1.

Exceptional sets

Theorem (Jarník (1928))

The set of badly approximable real numbers has Hausdorff dimension 1.

Theorem (Jarník (1929), Besicovitch (1934))

Let $v > 2$. The set of numbers for which

$$\left| x - \frac{p}{q} \right| < \frac{1}{q^v}$$

for infinitely many $p/q \in \mathbb{Q}$, has Hausdorff dimension $2/v$.

Outline

- 1 Linear complexity profiles
- 2 Diophantine approximation over \mathbb{R}
- 3 Diophantine approximation in positive characteristic**
- 4 Higher dimensional problems
- 5 Ideas of proofs

A dictionary

	char 0	char p
Integers	\mathbb{Z} Euclidean ring	$\mathbb{F}_q[T]$ Euclidean ring
Rationals	\mathbb{Q} field of fractions over \mathbb{Z}	$\mathbb{F}_q(T)$ field of fractions over $\mathbb{F}_q[T]$
Norm	the Euclidean norm	$ P = q^{\deg(P)}$
Reals	\mathbb{R} completion of \mathbb{Q}	$\mathbb{F}((T^{-1}))$ completion of $\mathbb{F}_q(T)$
Unit ball	$[0, 1]$	Generating functions
Measure	Lebesgue	Haar

Dirichlet's Theorem

- We do it all over again.

Dirichlet's Theorem

- We do it all over again.
- Applying the pigeon hole principle, we show that if $X \in \mathbb{F}((T^{-1})) \setminus \mathbb{F}(T)$, then

$$\left| X - \frac{P}{Q} \right| < \frac{1}{|Q|^2}$$

for infinitely many $P, Q \in \mathbb{F}[T]$.

Dirichlet's Theorem

- We do it all over again.
- Applying the pigeon hole principle, we show that if $X \in \mathbb{F}((T^{-1})) \setminus \mathbb{F}(T)$, then

$$\left| X - \frac{P}{Q} \right| < \frac{1}{|Q|^2}$$

for infinitely many $P, Q \in \mathbb{F}[T]$.

- There are numbers x for which there is a $K(x) > 0$ such that

$$\left| x - \frac{p}{q} \right| \geq \frac{K(x)}{q^2}$$

Continued fractions

- Continued fractions work analogously (Artin (1924)).

Continued fractions

- Continued fractions work analogously (Artin (1924)).
- The A_i are the *partial quotients*.

Continued fractions

- Continued fractions work analogously (Artin (1924)).
- The A_i are the *partial quotients*.
- The rationals P_n/Q_n determined by the recurrences

$$Q_{-1} = 0, Q_0 = 1, Q_n = A_n Q_{n-1} + Q_{n-2}$$

$$P_{-1} = 1, P_0 = A_0, P_n = A_n P_{n-1} + P_{n-2}$$

give best approximants.

Continued fractions

- Continued fractions work analogously (Artin (1924)).
- The A_i are the *partial quotients*.
- The rationals P_n/Q_n determined by the recurrences

$$Q_{-1} = 0, Q_0 = 1, \quad Q_n = A_n Q_{n-1} + Q_{n-2}$$

$$P_{-1} = 1, P_0 = A_0, \quad P_n = A_n P_{n-1} + P_{n-2}$$

give best approximants.

- A number is badly approximable iff the sequence of partial quotients is norm-bounded.

Metrical results

Theorem (de Mathan (1970))

Let $(l_n) \subseteq \mathbb{N}$ be non-decreasing. The set of $X \in \mathbb{F}((T^{-1}))$ for which

$$\left| X - \frac{P}{Q} \right| < \frac{1}{|Q|^2 q^{l_n}}$$

has infinitely many solutions $P, Q \in \mathbb{F}[X]$ is null (full) with respect to Lebesgue measure according to the convergence (divergence) of $\sum_n q^{-l_n}$.

Metrical results

Theorem (de Mathan (1970))

Let $(l_n) \subseteq \mathbb{N}$ be non-decreasing. The set of $X \in \mathbb{F}((T^{-1}))$ for which

$$\left| X - \frac{P}{Q} \right| < \frac{1}{|Q|^2 q^{l_n}}$$

has infinitely many solutions $P, Q \in \mathbb{F}[X]$ is null (full) with respect to Lebesgue measure according to the convergence (divergence) of $\sum_n q^{-l_n}$.

Corollary

Almost no numbers are badly approximable.

Exceptional sets

Theorem (Niederreiter and Vielhaber (1997))

The set of badly approximable formal power series (or sequences with almost perfect linear complexity profile) has Hausdorff dimension 1.

Exceptional sets

Theorem (Niederreiter and Vielhaber (1997))

The set of badly approximable formal power series (or sequences with almost perfect linear complexity profile) has Hausdorff dimension 1.

Theorem (K (2003))

Let $v > 2$. The set $X \in \mathbb{F}((T^{-1}))$ for which

$$\left| X - \frac{P}{Q} \right| < \frac{1}{|Q|^v}$$

for infinitely many $P, Q \in \mathbb{F}[T]$, has Hausdorff dimension $2/v$.

Outline

- 1 Linear complexity profiles
- 2 Diophantine approximation over \mathbb{R}
- 3 Diophantine approximation in positive characteristic
- 4 Higher dimensional problems**
- 5 Ideas of proofs

The Diophantine properties have generalisations:

Simultaneous approximation: For a vector

$\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{R}^n$ or $\mathbb{F}((T^{-1}))^n$, we study

$$\max_{1 \leq i \leq n} \left| x_i - \frac{p_i}{q} \right| < \psi(q)$$

Dual approximation: We study

$$|\mathbf{q} \cdot \mathbf{x} - p| < \psi(|\mathbf{q}|), \quad \mathbf{q} \in \mathbb{Z}^n \setminus \{0\}, p \in \mathbb{Z}.$$

In combination: For an $m \times n$ matrix A with entries in \mathbb{R}^n or $\mathbb{F}((T^{-1}))^n$, we study

$$|\mathbf{q}A - \mathbf{p}| < \psi(|\mathbf{q}|)$$

Dirichlet's Theorem (positive characteristic)

Theorem (K (2006), Corollary of Mahler (1941))

Let A be an $m \times n$ matrix A with entries in $\mathbb{F}((T^{-1}))^n$ and let $Q \geq 0$ be an integer with $n|Qm$. There is a $\mathbf{q} \in \mathbb{F}[T]^m$ with $|\mathbf{q}| \leq q^Q$ such that

$$\|\mathbf{q}A\|^n \leq \frac{1}{q^{Qm}}$$

Dirichlet's Theorem (positive characteristic)

Theorem (K (2006), Corollary of Mahler (1941))

Let A be an $m \times n$ matrix A with entries in $\mathbb{F}((T^{-1}))^n$ and let $Q \geq 0$ be an integer with $n|Qm$. There is a $\mathbf{q} \in \mathbb{F}[T]^m$ with $|\mathbf{q}| \leq q^Q$ such that

$$\|\mathbf{q}A\|^n \leq \frac{1}{q^{Qm}}$$

Corollary

With A as above, the inequality

$$|\mathbf{q}A - \mathbf{p}| \leq \frac{1}{|\mathbf{q}|^{m/n}}$$

has infinitely many solutions.

Khintchine-type results

Let ψ be non-increasing and define

$$\mathcal{S}(\psi) = \{A \in I^{mn} : \|\mathbf{q}A\| < \psi(\mathbf{q}) \text{ for infinitely many } \mathbf{q} \in \mathbb{F}[X]^m\}.$$

Khintchine-type results

Let ψ be non-increasing and define

$$\mathcal{S}(\psi) = \{A \in I^{mn} : \|\mathbf{q}A\| < \psi(\mathbf{q}) \text{ for infinitely many } \mathbf{q} \in \mathbb{F}[X]^m\}.$$

Theorem (K (2003))

Let $\psi : \mathbb{F}[X]^m \rightarrow \mathbb{R}^+$ be a function such that $\psi(\mathbf{q}) = \psi(|\mathbf{q}|)$.

(a)

$$\text{If } \sum_{\mathbf{q} \in \mathbb{F}[X]^m} \psi(\mathbf{q})^n < \infty, \text{ then } \mu(\mathcal{S}(\psi)) = 0.$$

(b)

$$\text{If } m > 1 \text{ and } \sum_{\mathbf{q} \in \mathbb{F}[X]^m} \psi(\mathbf{q})^n = \infty, \text{ then } \mu(\mathcal{S}(\psi)) = 1.$$

Even more specific information

Theorem (Dodson, Levesley, K (2005))

Let $\epsilon > 0$, let $\psi : \mathbb{R}_+ \rightarrow \mathbb{R}$ and let $N(Q, A)$ denote the number of solutions to

$$|\mathbf{q}A - \mathbf{p}| < \psi(|\mathbf{q}|)$$

with $|\mathbf{q}| \leq k^Q$. Let $\Phi(Q) = m(k-1)k^{m-1} \sum_{r=0}^Q k^{rm} \psi(k^r)^n$. Then

$$N(Q, A) = \Phi(Q) + O\left(\Phi(Q)^{1/2} \log^{3/2+\epsilon}(\Phi(Q))\right)$$

for almost every $m \times n$ matrix A with entries from $\mathbb{F}((T^{-1}))$.

Exceptional sets – well-approximables

Let for $\nu > 0$ and define

$$\mathcal{S}(\nu) = \{A \in I^{mn} : \|\mathbf{q}A\| < |\mathbf{q}|^{-\nu} \text{ for infinitely many } \mathbf{q} \in \mathbb{F}[X]^m\}.$$

Exceptional sets – well-approximables

Let for $\nu > 0$ and define

$$\mathcal{S}(\nu) = \{A \in I^{mn} : \|\mathbf{q}A\| < |\mathbf{q}|^{-\nu} \text{ for infinitely many } \mathbf{q} \in \mathbb{F}[X]^m\}.$$

Theorem (K 2003)

Let $\nu \geq \frac{m}{n}$. Then

$$\dim(\mathcal{S}(\nu)) = (m-1)n + \frac{m+n}{\nu+1}.$$

Exceptional sets - badly approximables

- Let Bad denote the systems of linear forms A for which

$$|\mathbf{q}A - \mathbf{p}| \geq \frac{K(A)}{|\mathbf{q}|^{m/n}}$$

for all $\mathbf{q} \neq 0$ and all \mathbf{p} .

Exceptional sets - badly approximables

- Let Bad denote the systems of linear forms A for which

$$|\mathbf{q}A - \mathbf{p}| \geq \frac{K(A)}{|\mathbf{q}|^{m/n}}$$

for all $\mathbf{q} \neq 0$ and all \mathbf{p} .

- This is a Haar-null set by the above.

Exceptional sets - badly approximables

- Let Bad denote the systems of linear forms A for which

$$|\mathbf{q}A - \mathbf{p}| \geq \frac{K(A)}{|\mathbf{q}|^{m/n}}$$

for all $\mathbf{q} \neq 0$ and all \mathbf{p} .

- This is a Haar-null set by the above.

Theorem (K 2006)

The Hausdorff dimension of the set Bad is mn , the maximal possible.

Outline

- 1 Linear complexity profiles
- 2 Diophantine approximation over \mathbb{R}
- 3 Diophantine approximation in positive characteristic
- 4 Higher dimensional problems
- 5 Ideas of proofs

Ubiquity

- Both the Khintchine-type theorem and the Jarník–Besicovitch type theorem are proved using the notion of ubiquity.

Ubiquity

- Both the Khintchine-type theorem and the Jarník–Besicovitch type theorem are proved using the notion of ubiquity.
- The idea was introduced by Dodson, Rynne and Vickers (1990) and reached a peak with Beresnevich, Dickinson and Velani (2006).

Ubiquity

- Both the Khintchine-type theorem and the Jarník–Besicovitch type theorem are proved using the notion of ubiquity.
- The idea was introduced by Dodson, Rynne and Vickers (1990) and reached a peak with Beresnevich, Dickinson and Velani (2006).
- It is a quantitative notion of density, which implies measure theoretic laws for limsup sets.

Ubiquity

- Both the Khintchine-type theorem and the Jarník–Besicovitch type theorem are proved using the notion of ubiquity.
- The idea was introduced by Dodson, Rynne and Vickers (1990) and reached a peak with Beresnevich, Dickinson and Velani (2006).
- It is a quantitative notion of density, which implies measure theoretic laws for limsup sets.
- At the end of the day, applying the framework boils down to estimating the measure of resonant neighbourhoods.

More ubiquity

Definition

Let (X, d, m) be a metric measure space, let $\mathcal{R} = (R_\alpha)$ be a family of subsets with weights $\beta_\alpha > 0$. Let l, u be increasing sequences of integers and let $\rho : \mathbb{R}_+ \rightarrow \mathbb{R}_+$. Define

$$\Delta_l^u(\rho, n) = \bigcup_{\alpha: l_n < \beta_\alpha \leq u_n} \{x \in X : \text{dist}(x, R_\alpha) < \rho(u_\alpha)\}.$$

If there is a $\kappa > 0$ such that for any small ball $B \subseteq X$ and any n large enough,

$$m(B \cap \Delta_l^u(\rho, n)) \geq \kappa m(B),$$

the system (\mathcal{R}, β) is locally m -ubiquitous with respect to (l, u, ρ) .

More ubiquity

Definition

Let (X, d, m) be a metric measure space, let $\mathcal{R} = (R_\alpha)$ be a family of subsets with weights $\beta_\alpha > 0$. Let l, u be increasing sequences of integers and let $\rho : \mathbb{R}_+ \rightarrow \mathbb{R}_+$. Define

$$\Delta_l^u(\rho, n) = \bigcup_{\alpha: l_n < \beta_\alpha \leq u_n} \{x \in X : \text{dist}(x, R_\alpha) < \rho(u_\alpha)\}.$$

If there is a $\kappa > 0$ such that for any small ball $B \subseteq X$ and any n large enough,

$$m(B \cap \Delta_l^u(\rho, n)) \geq \kappa m(B),$$

the system (\mathcal{R}, β) is locally m -ubiquitous with respect to (l, u, ρ) .

NB: There are some additional technical conditions. 

Quasi-orthogonality

To get asymptotic formulae, the key is again the intersections of resonant neighbourhoods and the following:

Theorem (Rademacher)

Let (X, \mathcal{B}, μ) a prob. sp. and let $f_k(x)$ a sequence of r.v. Let $0 \leq f_k \leq \phi_k \leq 1$ be sequences and suppose that for $m, n \in \mathbb{N}$,

$$\int_X \left(\sum_{m < k \leq n} (f_k(x) - f_k) \right)^2 d\mu \leq C \sum_{m < k \leq n} \phi_k.$$

Then, for a.a. $x \in X$ and any $\epsilon > 0$, with $\Phi(n) = \sum_{1 \leq k \leq n} \phi_k$,

$$\sum_{1 \leq k \leq n} f_k(x) = \sum_{1 \leq k \leq n} f_k + O(\Phi^{1/2}(n) \log^{3/2+\epsilon} \Phi(n)).$$

Schmidt games

- For badly approximables, the basic technique is a game.

Schmidt games

- For badly approximables, the basic technique is a game.
- Let $\alpha, \beta \in (0, 1)$ and let $S \subseteq X$, a metric space.

Schmidt games

- For badly approximables, the basic technique is a game.
- Let $\alpha, \beta \in (0, 1)$ and let $S \subseteq X$, a metric space.
- Black chooses a closed ball $B_1 \subseteq X$ of radius $\rho(B_1)$.

Schmidt games

- For badly approximables, the basic technique is a game.
- Let $\alpha, \beta \in (0, 1)$ and let $S \subseteq X$, a metric space.
- Black chooses a closed ball $B_1 \subseteq X$ of radius $\rho(B_1)$.
- White chooses a closed ball $W_1 \subseteq B_1$ of radius $\alpha\rho(B_1)$.

Schmidt games

- For badly approximables, the basic technique is a game.
- Let $\alpha, \beta \in (0, 1)$ and let $S \subseteq X$, a metric space.
- Black chooses a closed ball $B_1 \subseteq X$ of radius $\rho(B_1)$.
- White chooses a closed ball $W_1 \subseteq B_1$ of radius $\alpha\rho(B_1)$.
- Black chooses a closed ball $B_2 \subseteq W_1$ of radius $\beta\rho(W_1)$ and so on.

Schmidt games

- For badly approximables, the basic technique is a game.
- Let $\alpha, \beta \in (0, 1)$ and let $S \subseteq X$, a metric space.
- Black chooses a closed ball $B_1 \subseteq X$ of radius $\rho(B_1)$.
- White chooses a closed ball $W_1 \subseteq B_1$ of radius $\alpha\rho(B_1)$.
- Black chooses a closed ball $B_2 \subseteq W_1$ of radius $\beta\rho(W_1)$ and so on.
- If $\bigcap B_i \subseteq S$, White wins. Otherwise, Black wins.

Schmidt games

- For badly approximables, the basic technique is a game.
- Let $\alpha, \beta \in (0, 1)$ and let $S \subseteq X$, a metric space.
- Black chooses a closed ball $B_1 \subseteq X$ of radius $\rho(B_1)$.
- White chooses a closed ball $W_1 \subseteq B_1$ of radius $\alpha\rho(B_1)$.
- Black chooses a closed ball $B_2 \subseteq W_1$ of radius $\beta\rho(W_1)$ and so on.
- If $\bigcap B_i \subseteq S$, White wins. Otherwise, Black wins.
- If White has a winning strategy, S is (α, β) -winning.

Schmidt games

- For badly approximables, the basic technique is a game.
- Let $\alpha, \beta \in (0, 1)$ and let $S \subseteq X$, a metric space.
- Black chooses a closed ball $B_1 \subseteq X$ of radius $\rho(B_1)$.
- White chooses a closed ball $W_1 \subseteq B_1$ of radius $\alpha\rho(B_1)$.
- Black chooses a closed ball $B_2 \subseteq W_1$ of radius $\beta\rho(W_1)$ and so on.
- If $\bigcap B_i \subseteq S$, White wins. Otherwise, Black wins.
- If White has a winning strategy, S is (α, β) -winning.
- With α fixed, if White has a winning strategy for any β , S is α -winning.

More Schmidt games

- One can show that the set of almost perfect sequences is α -winning for some α .

More Schmidt games

- One can show that the set of almost perfect sequences is α -winning for some α .
- With great care and some pain, one can show that the systems of linear forms are also α -winning.

More Schmidt games

- One can show that the set of almost perfect sequences is α -winning for some α .
- With great care and some pain, one can show that the systems of linear forms are also α -winning.
- Under mild assumptions on the ambient space, an α -winning set has maximal dimension.