Denominators of rational numbers in or close to Cantor sets

Igor Shparlinski

The University of New South Wales

Introduction

Let $\mathcal{D} \subset \{0, 1, \ldots, g-1\}$ be a non-empty set of g-ary digits.

We define a generalised Cantor set $\mathcal{C}_g(\mathcal{D})$ as

$$\mathcal{C}_g(\mathcal{D}) = \left\{ \alpha = \sum_{i=1}^{\infty} d_i g^{-i}, \qquad d_i \in \mathcal{D} \right\}.$$

In particular, we denote by $\mathcal{K} = \mathcal{C}_3(\{0, 2\})$ the classical Cantor set.

We will discuss the *distribution* and *arithmetic structure* of integer denominators q for which for some integer r with $\gcd(r, q) = 1$ and some $\alpha \in \mathcal{C}_g(\mathcal{D})$ the difference $\alpha - r/q$ is very small (i.e., much smaller than $1/q$), including the special case when it is zero, i.e. $r/q \in \mathcal{C}_g(\mathcal{D})$.

Conventions: $1 \leq \#\mathcal{D} < g$ and r/q is always with $\gcd(rg, q) = 1$

Outline of this talk

- We start with a short survey of results . . . by someone who had never heard about this less that 12 month ago before *'Dynamics and Number Theory'*, Univ. of Sydney, 12–14 June 2019.
- We discuss what bounds of short exponential sums with exponential functions due to *Korobov* (**1972**) can tell us about denominators of rationals close to Cantor sets $\mathcal{C}_g(\mathcal{D})$.
- We present a new approach and results about the arithmetic structure of denominators of rationals in Cantor sets $\mathcal{C}_g(\mathcal{D})$, improving those of *Schleischitz* (**2019**).

Counting rationals in Cantor sets

Define

$$N_g(\mathcal{D};Q) = \#\{r/q \in \mathcal{C}_g(\mathcal{D}) :\ 1 \le q \le Q\}.$$

Important quantity: $\vartheta_g(\mathcal{D}) = \dfrac{\log \#\mathcal{D}}{\log g}$, the Hausdorff dimension of $\mathcal{C}_g(\mathcal{D})$.

Conjecture: Broderick, Fishman and Reich (2011)

We have $N_g(\mathcal{D};Q) \le Q^{\vartheta_g(\mathcal{D})+o(1)}$.

Schleischitz (2019)

We have $Q^{\vartheta_g(\mathcal{D})+o(1)} \le N_g(\mathcal{D};Q) \le Q^{2\vartheta_g(\mathcal{D})+o(1)}$.

Denominators of rationals in Cantor sets

Motivation:

> Sets $\mathcal{C}_g(\mathcal{D})$ are very **special** sets of g-ary numbers; can they contain rationals r/q with very **special** denominators q?

For an integer $q \geq 2$, let

$$P(q) = \max_{\substack{p|q,\\ p \text{ prime}}} p \qquad \text{and} \qquad \mathrm{rad}(q) = \prod_{\substack{p|q,\\ p \text{ prime}}} p.$$

Using some techniques from ergodic theory, as a result of a more general statement:

Schleischitz (2019)

If $r/q \in \mathcal{C}_g(\mathcal{D})$ *then* $P(q) \to \infty$ *as* $q \to \infty$.

Using results of *Korobov* (**1970**):

Shparlinski (2019)

There is a constant $c > 0$ *depending only on* g, *such that if* $r/q \in \mathcal{C}_g(\mathcal{D})$ *then*

$$P(q) \geq c\sqrt{\log q \log\log q} \qquad \text{and} \qquad \mathrm{rad}(q) \geq c \log q.$$

Denominators of rationals close to Cantor sets

Let $\|\xi\|$ be the distance between a real ξ and the closest integer.

We have the following general result:

Schleischitz (2019)

There is a constant $c > 0$ depending only on g, such that for any $\xi \in \mathcal{C}_g(\mathcal{D}) \setminus \mathbb{Q}$, for all but finitely many q:

$$\|q\xi\| \geq g^{-cq^{\vartheta_g(\mathcal{D})}}.$$

Question: What about small values of $\|q\xi\|$ for "special" q?

The above results show that for any $\xi \in \mathcal{C}_g(\mathcal{D})$ the equation

$$\|q\xi\| = 0$$

is possible only for finitely many "special" q (e.g. for $g = 3$ and $q = 2^n$).

Can we say more?

Perfect powers:

Bugeaud (2012)

There is an absolute constant $c > 0$ such that there are uncountably many real numbers $\xi \in \mathcal{K}$ which for all integers $m \geq 2$ and $k \geq 1$, satisfy

$$\|m^k \xi\| > e^{-cm(\log m)^2}.$$

Open Question: What about $\|a^n \xi\|$ for all or almost all $\xi \in \mathcal{K} \setminus \mathbb{Q}$?

Powers of 2:

Let as before $\vartheta = \log 2/\log 3$ be the Hausdorff dimension of $\mathcal{C}$.

Allen, Chow, Yu (2020)

For **almost all** *$\xi \in \mathcal{C}$, w.r.t. a natural measure on $\mathcal{K}$, for $q = 2^n$ we have*

$$\|q\xi\| > (\log q)^{-1/\vartheta + o(1)}$$

Remark: Both works are based on Diophantine approximation theory.

Using results of *Korobov* (**1972**), we have a result for arbitrary sets $\mathcal{C}_g(\mathcal{D})$ and products of arbitrary finite sets of primes.

Shparlinski (2019)

Let $\mathcal{S}$ be a finite set of primes such that $\gcd(g,p) = 1$ for any $p \in \mathcal{S}$. For any $\varepsilon > 0$, for all but finitely many q with all prime factors in $\mathcal{S}$, for any $\xi \in \mathcal{C}_g(\mathcal{D})$ we have

$$\|q\xi\| > g^{-\exp\left((\log q)^{2/3+\varepsilon}\right)}.$$

Idea of the proof: By *Korobov* (**1972**), rational fractions r/q with q as above, have uniformly distributed g-ary digits starting with segments of length $N \geq \exp\left((\log q)^{2/3+\varepsilon}\right)$ and hence disagree with $\xi \in \mathcal{C}_g(\mathcal{D})$.

Remark: The method of *Korobov* (**1972**), uses bounds on *exponential sums (Weyl sums)* and in particular the *Vinogradov Mean Value Theorem.* Unfortunately, it is not affected by the spectacular progress due to *Bourgain, Demeter and Guth* (**2016**) and *Wooley* (**2016–2019**).

Sketch of the proof of lower bounds on $P(q)$ and $\mathrm{rad}(q)$

Recall:

Using results of *Korobov* (**1970**):

Shparlinski (2019)

There is a constant $c > 0$ *depending only on* g, *such that if* $r/q \in \mathcal{C}_g(\mathcal{D})$ *then*

$$P(q) \geq c\sqrt{\log q \log\log q} \qquad \textit{and} \qquad \mathrm{rad}(q) \geq c \log q.$$

This improves $P(q) \to \infty$ as $q \to \infty$ due to *Schleischitz* (**2019**).

Preparations

Let $\tau(q)$ be the multiplicative order of g modulo q, that is, the smallest integer $t \geq 1$ with $g^t \equiv 1 \pmod{q}$.

We also define

$$\tau_0(q) = \tau\left(\mathrm{rad}(q)\right).$$

For any integer $r \geq 1$ with $\gcd(gr, q) = 1$, the g-ary expansion of r/q is purely periodic with period $\tau(q)$.

For a g-ary digit $d \in \{0, 1, \ldots, g-1\}$ we denote by $N_{r,q}(d)$ the number of occurrences of d in the full period of the g-ary expansion of r/q.

Korobov (1970)

For any positive integers r and q with $\gcd(gr, q) = 1$ we have

$$\left| N_{r,q}(d) - \frac{1}{g}\tau(q) \right| < 2\tau_0(q).$$

Upper bound

To simplify the notation we denote

$$t = \tau(q) \qquad \text{and} \qquad t_0 = \tau_0(q).$$

We fix some $d \in \{0, 1, \ldots, g-1\} \setminus \mathcal{D}$ and $r/q \in \mathcal{C}_g(\mathcal{D})$.

Clearly $N_{r,q}(d) = 0$. Hence, by *Korobov* (**1970**)

$$t/g = |0 - t/g| = |N_{r,q}(d) - t/g| \le 2t_0$$

Hence

$$\boxed{t \le 2gt_0}$$

Lower bound

Let

$$q = p_1^{\alpha_1} \dots p_s^{\alpha_s} \qquad \text{and} \qquad \mathrm{rad}(q) = p_1 \dots p_s$$

for some distinct primes $p_1, \dots, p_s$ and integers $\alpha_1, \dots, \alpha_s \geq 1$.

To show the ideas we ignore $p = 2$ as if it never existed.

We write

$$g^{t_0} = 1 + u_0 p_1^{\beta_1} \dots, p_s^{\beta_s}, \qquad (q \text{ is odd}).$$

The following is very elementary and can also be found in *Korobov* (**1970**):

$$t = t_0 p_1^{\gamma_1} \dots p_s^{\gamma_s}$$

where

$$\gamma_\nu = \max\{0, \alpha_\nu - \beta_\nu\}, \qquad \nu = 1, \dots, s.$$

Hence

$$t \geq t_0 p_1^{\alpha_1 - \beta_1} \dots p_s^{\alpha_s - \beta_s} = t_0 q p_1^{-\beta_1} \dots p_s^{-\beta_s}.$$

Combining lower and upper bounds on t

So we have

$$2gt_0 \geq t \geq t_0 p_1^{\alpha_1-\beta_1} \dots p_s^{\alpha_s-\beta_s} = t_0 q p_1^{-\beta_1} \dots p_s^{-\beta_s}.$$

Hence

$$p_1^{\beta_1} \dots p_s^{\beta_s} \geq \frac{1}{2g} q.$$

We are now **done** since the LHS can be upper bounded in terms of $p_1, \dots, p_s$ rather than q leading to a statement of the form $F(p_1, \dots, p_s) \geq q$ for some explicit function F. From here we estimate

$$P(q) = \max_{i=1,\dots,s} p_i \qquad \text{and} \qquad \mathrm{rad}(q) = p_1 \dots p_s$$

Gory details

So we now examine this more carefully:

$$\bigstar \qquad p_1^{\beta_1} \dots p_s^{\beta_s} \gg q$$

Let $\nu_p(a)$ be the p-adic order of $a \in \mathbb{Z}$: the largest integer α with $p^\alpha \mid a$.

By *Korobov* (**1970**) we have the following elementary relation

$$\beta_i = \nu_{p_i}\left(g^{\tau(p_i)} - 1\right) + \nu_{p_i} t_0, \qquad (p_i \geq 3).$$

Using the trivial bounds

$$p^{\nu_p(g^{\tau(p)}-1)} < g^{\tau(p)} < g^p \qquad \text{and} \qquad t_0 \leq p_1 \dots p_s,$$

we derive

$$\bullet \qquad p_1^{\beta_1} \dots p_s^{\beta_s} = \prod_{i=1}^{s} p_i^{\nu_{p_i}\left(g^{\tau(p_i)}-1\right)+\nu_{p_i} t_0} = t_0 g^{p_1} \dots g^{p_s} \leq g^{2(p_1+\dots+p_s)}.$$

Putting together $\bigstar$ and $\bullet$:

$$p_1 + \dots + p_s \gg \log\left(g^{p_1+\dots+p_s}\right) \gg \log\left(p_1^{\beta_1} \dots p_s^{\beta_s}\right) \gg \log q.$$

So arrive to our main inequality

$$p_1 + \ldots + p_s \gg \log q.$$

Using the trivial inequality

$$\mathrm{rad}(q) = p_1 \ldots p_s \geq p_1 + \ldots + p_s,$$

we derive the desired lower bound on $\mathrm{rad}(q)$.

Remark

This looks very crude, but what if $s = 1$? Or $s = 5$, $p_1 = 3$, $p_2 = 5$, $p_3 = 7$, $p_4 = 11$, $p_5 = P(q)$? We only lose a constant.

Furthermore, we have

$$sP(q) \geq p_1 + \ldots + p_s.$$

By the PNT, $P(q) \gg s \log(s+1)$ or $s \ll P(q)/\log P(q)$. Hence

$$P(q)^2/\log P(q) \gg \log q$$

and we derive the desired lower bound on $P(q)$.

Question

How tight are the bounds

$$P(q) \geq c\sqrt{\log q \log\log q} \qquad \textit{and} \qquad \operatorname{rad}(q) \geq c \log q?$$

...perhaps not so much. However Cantor sets do contain infinitely many rational numbers with denominators free of large prime divisors.

Construction

For $m \to \infty$ we define

$$t_m = \prod_{\substack{p \leq m \\ p \text{ prime}}} p = \exp(m + o(m)),$$

and

$$r_m/q_m = \frac{1}{g^{t_m} - 1} = \sum_{i=1}^{\infty} \frac{1}{g^{t_m i}} \in \mathcal{C}_g\left(\{0,1\}\right).$$

Using factorisation of $X^t - 1$ into cyclotomic polynomials $\Phi_u(X)$,

$$q_m = g^{t_m} - 1 = \prod_{u | t_m} \Phi_u(g).$$

Since the $\Phi_u(g)$ are positive integers of size at most

$$\Phi_u(g) = \prod_{\substack{k=1 \\ \gcd(k,u)=1}}^{u} (g - \exp(2\pi i k/u)) \leq (g+1)^{\varphi(u)},$$

where φ is the Euler function, we see that

$$P(q_m) = P\left(g^{t_m} - 1\right) \leq (g+1)^{\varphi(t_m)}.$$

By the Mertens formula,

$$\varphi(t_m) = t_m \prod_{\substack{p \leq m \\ p \text{ prime}}} (1 - 1/p) \ll t_m / \log m \ll t_m / \log\log t_m.$$

Therefore there are infinitely many rational fractions $r/q \in \mathcal{C}_g\left(\{0,1\}\right)$ with

$$P(q) \leq q^{O(1/\log\log q)}.$$