Rational numbers in $\times b$-invariant sets

Ruofan Li

South China University of Technology

Joint work with Bing Li and Yufeng Wu
One World Numeration Seminar, July 12, 2022

Rational numbers in Cantor set

Let C be the classical middle-third Cantor set, which consists of real numbers in $[0, 1]$ whose ternary expansions do not contain digit 1.

For any $n \geq 1$, we know that there are exactly 2^{n+1} rational numbers of the form $\frac{a}{3^n}$ in C with $a \in \mathbb{Z}$.

Rational numbers in Cantor set

$$\frac{1}{4} = \sum_{n=1}^{\infty} \frac{2}{3^{2n}} = \frac{2}{9} + \frac{2}{81} + \cdots \in C.$$

$$\frac{3}{4} = \sum_{n=1}^{\infty} \frac{2}{3^{2n-1}} = \frac{2}{3} + \frac{2}{27} + \cdots \in C.$$

Theorem (Wall, 1983)

$$C \cap \left\{ \frac{a}{2^n} : n \in \mathbb{N}, 0 < a < 2^n, \right\} = \left\{ \frac{1}{4}, \frac{3}{4} \right\}.$$

Theorem (Nagy, 2001)

Let $p \geq 5$ be a prime, then

$$C \cap \left\{ \frac{a}{p^n} \colon n \in \mathbb{N}, 0 < a < p^n, \right\}$$

is finite.

S-integers

Let S be a finite set of primes, then the set of S-**integers** $\mathbb{Z}_S$ is defined to be the set of rational numbers whose denominators can only be divided by primes in S. Equivalently,

$$\mathbb{Z}_S = \{\alpha \in \mathbb{Q} \colon v_p(\alpha) < 0 \text{ implies } p \in S\},$$

where $v_p(\alpha)$ is the unique integer such that $\alpha = p^{v_p(\alpha)} \frac{m}{n}$ for some $m, n \in \mathbb{Z}$ coprime with p.

S-integers in Cantor set

Nagy's theorem can be rephrased as follows.

Theorem (Nagy, 2001)

Let $p \geq 5$ be a prime and $S = \{p\}$, then $C \cap \mathbb{Z}_S$ is finite.

When $S = \{2, 5\}$, we have the following result.

Theorem (Wall, 1990)

$$\mathbb{Z}_{\{2,5\}} \cap C$$

consists of exactly 14 elements.

Generalized Cantor sets

Let $b \geq 2$ be an integer and $\mathcal{D}$ be a non-empty subset of $\{0, 1, \ldots, b-1\}$, the generalized Cantor set $C(b, \mathcal{D})$ is the set of real numbers in $[0, 1]$ whose base b expansions only consist of digits in $\mathcal{D}$.

The classical middle-third Cantor set is $C = C(3, \{0, 2\})$.

Generalized Cantor sets

Theorem (Bloshchitsyn, 2015)

Suppose $b \geq 3$ is an integer, $\mathcal{D} \subseteq \{0, 1, \ldots, b-1\}$ has cardinality $b-1$ and p is a prime satisfying $p > b^2$. Then the set

$$\mathbb{Z}_{\{p\}} \cap C(b, \mathcal{D})$$

is finite.

Theorem (Schleischitz, 2021)

Suppose $b \geq 3$ is an integer, $\mathcal{D} \subseteq \{0, 1, \ldots, b-1\}$ be a non-empty set of cardinality at most $b-1$ and S is a finite set of primes not containing any divisor of b. Then the set

$$\mathbb{Z}_S \cap C(b, \mathcal{D})$$

is finite.

Quantitative result

Theorem (Shparlinski, 2021)

Let $b \geq 2$ be an integer and $\mathcal{D} \subseteq \{0, 1, \ldots, b-1\}$ be a non-empty set of cardinality at most $b-1$. Then there exists a constant $c_b > 0$, depending only on b, such that for any rational number $\frac{a}{d}$ in $C(b, \mathcal{D})$ with $\gcd(ab, d) = 1$, we have

$$P(d) \geq c_b \sqrt{\log d \log \log d},$$

where $P(d)$ denotes the largest prime divisor of d.

T_b-invariant

For any integer $b \geq 2$, the transformation $T_b\colon [0,1) \to [0,1)$ is defined by

$$T_b(x) = bx \pmod 1.$$

We say that a set $A \subseteq [0,1)$ is T_b-*invariant* if $T_b(A) \subseteq A$.

All generalized Cantor sets $C(b, \mathcal{D})$ are T_b-invariant.

Main results

Theorem (Li, L. and Wu)

Let $b \geq 2$ be an integer, S be a non-empty finite set of primes not containing any prime divisor of b, and A be a subset of $[0, 1)$. If A is not dense in $[0, 1]$ and $T_b(A \cap \mathbb{Q}) \subseteq A$, then A contains at most finitely many S-integers.

Main results

Theorem (Li, L. and Wu)

Let $b \geq 2$ *be an integer and* $A \subseteq [0,1)$ *be a set satisfying* $T_b(A \cap \mathbb{Q}) \subseteq A$. *Suppose* A *is not dense in* $[0,1]$ *and let* $\varepsilon = \sup\{\mathrm{dist}(x, A)\colon x \in [0,1)\}$, *where* $\mathrm{dist}(x, A)$ *denotes the distance between* x *and* A. *Then there exists an absolute constant* $K > 0$, *which can be effectively computed, such that for any rational number* $\frac{a}{d}$ *in* A *with* $\gcd(ab, d) = 1$ *and* $\varepsilon d \geq 3$, *we have*

$$P(d) \geq \begin{cases} K\sqrt{\frac{1}{\log b}\log(2\varepsilon d)\log\log(2\varepsilon d)} & \text{if} \quad P(d) > b, \\ K\sqrt{\frac{1}{\log b}\log(2\varepsilon d)} & \text{if} \quad P(d) < b. \end{cases}$$

Main results

Theorem (Li, L. and Wu)

Let $b \geq 2$ be an integer and S be a non-empty finite set of primes not containing any prime divisor of b. For any $\varepsilon > 0$, there exists an effectively computable positive number D, such that for any $\frac{a}{d} \in \mathbb{Z}_S \cap [0, 1)$ with $(a, d) = 1$ and $d > D$, the orbit of $\frac{a}{d}$ under T_b,

$$\mathrm{Orb}_{T_b}\left(\frac{a}{d}\right) := \left\{ T_b^i\left(\frac{a}{d}\right) : i \geq 0 \right\},$$

is ε-dense in $[0, 1]$.

Proof of finiteness result

Now we use our ε-dense theorem to deduce the finiteness of S-integers in nondense T_b-invariant set A.

Since A is not dense in $[0, 1]$, there exists $\varepsilon > 0$ such that A is not ε-dense in $[0, 1]$.

Let $\frac{a}{d} \in A \cap \mathbb{Z}_S$ with $\gcd(a, d) = 1$. Since $T_b(A \cap \mathbb{Q}) \subseteq A$, we have $\mathrm{Orb}_{T_b}\left(\frac{a}{d}\right) \subseteq A$, and so $\mathrm{Orb}_{T_b}\left(\frac{a}{d}\right)$ is also not ε-dense in $[0, 1]$.

Therefore our ε-dense theorem implies that $d < D$ for some positive number D. Clearly there are only finitely many rational numbers $\frac{a}{d} \in [0, 1)$ with $d < D$, hence A contains at most finitely many S-integers.

T_b-orbit

Since $(b, d) = 1$, there exists $k \in \mathbb{N}$ such that $b^k \equiv 1 \pmod{d}$. So $T_b^k\left(\frac{a}{d}\right) = \frac{ab^k}{d} \pmod{1} = \frac{a}{d}$, and hence

$$\mathrm{Orb}_{T_b}\left(\frac{a}{d}\right) := \left\{ T_b^i\left(\frac{a}{d}\right) : i \geq 0 \right\}$$

is a finite set.

The smallest such k is denoted by $\mathrm{ord}(\overline{b}, d)$. We use this notation because it is the order of $\overline{b} \pmod{d}$ in the multiplicative group $(\mathbb{Z}/d\mathbb{Z})^\times$.

T_b-orbit

We will find an integer $d_1 \mid d$ such that the value of d_1 is bounded and the following two sets are equal.

$$A_1 = \left\{ T_b^i \left(\frac{a}{d} \right) : 0 \le i \le \operatorname{ord}(\overline{b}, d) - 1 \right\},$$

$$A_2 = \left\{ \frac{1}{d_0} T_b^i \left(\frac{a}{d_1} \right) + \frac{j}{d_0} : 0 \le i \le \operatorname{ord}(\overline{b}, d_1) - 1, 0 \le j \le d_0 - 1 \right\},$$

where $d_0 = \frac{d}{d_1}$.
Note that A_2 is a union of $\frac{1}{2d_0}$-dense sets.
So for any $\varepsilon > 0$ and any d sufficiently large, the set A_1 is ε-dense.

$$A_1 = \left\{ T_b^i\left(\frac{a}{d}\right) : 0 \le i \le \mathrm{ord}(\overline{b}, d) - 1 \right\},$$

$$A_2 = \left\{ \frac{1}{d_0} T_b^i\left(\frac{a}{d_1}\right) + \frac{j}{d_0} : 0 \le i \le \mathrm{ord}(\overline{b}, d_1) - 1, 0 \le j \le d_0 - 1 \right\},$$

where $d_0 = \frac{d}{d_1}$.

We have $A_1 \subseteq A_2$ due to the following relation.

$$\begin{aligned} &\left\{ ab^i \pmod{d} : 0 \le i \le \mathrm{ord}(\overline{b}, d) - 1 \right\} \\ \subseteq &\left\{ ab^i \pmod{d_1} + jd_1 : 0 \le i \le \mathrm{ord}(\overline{b}, d_1) - 1, 0 \le j \le d_0 - 1 \right\}. \end{aligned}$$

Now to prove $A_1 = A_2$, it suffices to show that they have the same cardinality.

$$A_1 = \left\{ T_b^i \left(\frac{a}{d} \right) : 0 \le i \le \operatorname{ord}(\overline{b}, d) - 1 \right\},$$

$$A_2 = \left\{ \frac{1}{d_0} T_b^i \left(\frac{a}{d_1} \right) + \frac{j}{d_0} : 0 \le i \le \operatorname{ord}(\overline{b}, d_1) - 1, 0 \le j \le d_0 - 1 \right\}.$$

In other words, we need to show $\operatorname{ord}(\overline{b}, d) = d_0 \operatorname{ord}\left(\overline{b}, d_1\right)$.

Singe prime case

Lemma

Let $b \geq 2$ be an integer and p be a prime satisfies $p \nmid b$. Define

$$n_p = \begin{cases} \max\{3, v_2(b-1), v_2(b+1)\}, & \text{if } p = 2, \\ \max\{1, v_p(b^{p-1}-1)\}, & \text{if } p \neq 2, \end{cases}$$

Then for any integer $d = p^{e_p}$, we have

$$\mathrm{ord}(\overline{b}, d) = p^{\max\{0, e_p - n_p\}} \, \mathrm{ord}\left(\overline{b}, p^{\min\{e_p, n_p\}}\right).$$

The above equality is equivalent to

$$\mathrm{ord}(\overline{b}, p^{e_p}) = p^{e_p - n_p} \, \mathrm{ord}(\overline{b}, p^{n_p}) \text{ for any } e_p > n_p.$$

Singe prime case

The difference between $p = 2$ and odd primes is due to the following classical result.

Lemma

For any $n \geq 3$, we have

$$(\mathbb{Z}/2^n\mathbb{Z})^\times \cong \langle\overline{-1}\rangle \times \langle\bar{5}\rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}.$$

For any odd prime p and $n \geq 1$, we have

$$(\mathbb{Z}/p^n\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)p^{n-1}\mathbb{Z}.$$

$p = 2$ case

$$n_2 = \max\{3, v_2(b-1), v_2(b+1)\}.$$

$$(\mathbb{Z}/2^n\mathbb{Z})^\times \cong \langle\overline{-1}\rangle \times \langle\overline{5}\rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z} \text{ for } n \geq 3.$$

We are going to show $\mathrm{ord}(\overline{b}, 2^e) = 2^{e-n_2}\,\mathrm{ord}(\overline{b}, 2^{n_2})$ for any $e > n_2$.

Since $e > n_2$, we have $b \not\equiv \pm 1 \pmod{2^e}$. So $\overline{b} \in \langle\overline{5}\rangle$ or $\langle\overline{-5}\rangle$ in $(\mathbb{Z}/2^e\mathbb{Z})^\times$. Let $\overline{g} = \overline{5}$ or $\overline{-5}$ such that $\overline{b} = \overline{g}^t$ for some $t \geq 1$.
In the groups $(\mathbb{Z}/2^{n_2+1}\mathbb{Z})^\times$, $(\mathbb{Z}/2^{n_2}\mathbb{Z})^\times$ and $(\mathbb{Z}/2^e\mathbb{Z})^\times$, we have

$$\mathrm{ord}(\overline{b}, 2^{n_2+1})\gcd(t, 2^{n_2-1}) = 2^{n_2-1},$$
$$\mathrm{ord}(\overline{b}, 2^{n_2})\gcd(t, 2^{n_2-2}) = 2^{n_2-2},$$
$$\mathrm{ord}(\overline{b}, 2^e)\gcd(t, 2^{e-2}) = 2^{e-2}.$$

$p = 2$ case

$$\begin{aligned} \operatorname{ord}(\overline{b}, 2^{n_2+1}) \gcd(t, 2^{n_2-1}) &= 2^{n_2-1}, \\ \operatorname{ord}(\overline{b}, 2^{n_2}) \gcd(t, 2^{n_2-2}) &= 2^{n_2-2}, \\ \operatorname{ord}(\overline{b}, 2^{e}) \gcd(t, 2^{e-2}) &= 2^{e-2}. \end{aligned}$$

Since $b \not\equiv 1 \pmod{2^{n_2+1}}$, we have $\operatorname{ord}(\overline{b}, 2^{n_2+1}) \neq 1$ and hence the first equation shows $v_2(t) \leq n_2 - 2$, which implies that $\gcd(t, 2^{n_2-2}) = \gcd(t, 2^{e-2})$.
Then the second and third equations give $\operatorname{ord}(\overline{b}, 2^{e}) = 2^{e-n_2} \operatorname{ord}(\overline{b}, 2^{n_2})$.

General case

By the Chinese Reminder Theorem, we have a group isomorphism

$$f : (\mathbb{Z}/d\mathbb{Z})^\times \to \prod_{p\in S} (\mathbb{Z}/p^{e_p}\mathbb{Z})^\times$$
$$\overline{a} \pmod{d} \mapsto (\overline{a} \pmod{p^{e_p}})_{p\in S}$$

Therefore

$$\mathrm{ord}(\overline{b}, d) = \mathrm{lcm}\{\mathrm{ord}(\overline{b}, p^{e_p})\colon p \in S\}.$$

General case

Lemma

Let $b \geq 2$ be an integer and S be a non-empty finite set of primes not containing any prime divisor of b. Define

$$N_p = \max\{n_p - v_p(\mathrm{ord}(\overline{b}, p^{n_p})) + v_p(\mathrm{ord}(\overline{b}, q^{n_q}))\colon q \in S\}.$$

Then for any integer $d = \prod_{p \in S} p^{e_p}$, let $d_0 = \prod_{p \in S\colon\ e_p > N_p} p^{e_p - N_p}$ and $d_1 = \prod_{p \in S} p^{\min\{e_p, N_p\}}$, we have

$$\mathrm{ord}(\overline{b}, d) = d_0 \, \mathrm{ord}\left(\overline{b}, d_1\right).$$

Largest prime divisor

Suppose $\frac{a}{d}$ in A with $\gcd(ab, d) = 1$, and let S be the set of prime divisors of d. We have shown that $\mathrm{Orb}_{T_b}(\frac{a}{d})$ contains a $\frac{d_1}{2d}$-dense subset, so we must have $\frac{d_1}{2d} \geq \varepsilon$, where $\varepsilon = \sup\{\mathrm{dist}(x, A) \colon x \in [0, 1)\}$.

Since

$$d_1 = \prod_{p \in S} p^{\min\{e_p, N_p\}},$$

we have

$$2d\epsilon \leq d_1 \leq \prod_{p \in S} p^{N_p}.$$

Largest prime divisor

$$n_p = \begin{cases} \max\{3, v_2(b-1), v_2(b+1)\}, & \text{if } p = 2, \\ \max\{1, v_p(b^{p-1}-1)\}, & \text{if } p \neq 2. \end{cases}$$

Note that

$$v_p(x) \leq \frac{\log x}{\log p} \text{ for any integer } x > 0,$$

so

$$n_p \ll \frac{p \log b}{\log p}.$$

Largest prime divisor

$$n_p \ll \frac{p \log b}{\log p}.$$

$$N_p = \max\{n_p - v_p(\mathrm{ord}(\overline{b}, p^{n_p})) + v_p(\mathrm{ord}(\overline{b}, q^{n_q}))\colon q \in S\}.$$

Note that $\mathrm{ord}(\overline{b}, q^{n_q})$ cannot be bigger than the order of $(\mathbb{Z}/q^{n_q}\mathbb{Z})^\times$, which equals $(q-1)q^{n_q-1}$, so

$$v_p(\mathrm{ord}(\overline{b}, q^{n_q})) \le \frac{\log (q-1)q^{n_q-1}}{\log p} \le \frac{n_q \log q}{\log p} \ll \frac{q \log b}{\log p}.$$

Let P be the largest element in S, then

$$N_p \ll \frac{\log b}{\log p}(p+P) \ll \frac{\log b}{\log p} P$$

Largest prime divisor

$$2d\epsilon \leq \prod_{p\in S} p^{N_p} \quad \text{and} \quad N_p \ll \frac{\log b}{\log p} P$$

Then

$$\log 2d\epsilon \leq \sum_{p\in S} N_p \log p \ll (\log b) \sum_{p\in S} P = P\#S \log b.$$

The prime number theorem says that the cardinality of S satisfies $\#S \ll \frac{P}{\log P}$, hence

$$\log 2d\epsilon \ll \frac{P^2}{\log P} \log b.$$

The inequality in our theorem is deduced from above through some simple calculations.

T_b-invariant set

Corollary

Let $b \geq 2$ be an integer, S be a non-empty finite set of primes not containing any prime divisor of b, and A be a subset of $[0, 1)$. If A is not dense in $[0, 1]$ and $T_b(A) \subseteq A$, then $\overline{A}$, the closure of A, contains at most finitely many S-integers.

Proof.

Note that A is T_b-invariant implies $\overline{A}$ is also T_b-invariant. □

Rational numbers of more general form

Corollary

Let $b \geq 2$ be an integer, $d \geq 2$ be another integer such that there exists at least one prime $p \mid d$ such that $p \nmid b$, and A be a subset of $[0, 1)$. If A is not dense in $[0, 1]$ and $T_b(A \cap \mathbb{Q}) \subseteq A$, then A contains at most finitely many rational numbers of the form $\frac{a}{d^n}$, $n \in \mathbb{N}$.

Proof.

Let $\tilde{d}$ be the largest divisor of d satisfying $\gcd(\tilde{d}, b) = 1$. We choose a big enough integer m such that

$$T_b^m \left(\frac{a}{d^n} \right) = \frac{\tilde{a}}{\tilde{d}^n},$$

for some integer $\tilde{a}$. Now our theorem says that n is bounded. □

Orbit of S-integers

Corollary

Let $b \geq 2$ be an integer, S be a non-empty finite set of primes not containing any prime divisor of b. Let $X \subseteq \mathbb{Z}_S \cap [0, 1)$ be an infinite subset of S-integers. Then the set

$$\mathrm{Orb}_{T_b}(X) := \left\{ b^k x \pmod 1 : x \in X, k \geq 0 \right\}$$

is dense in $[0, 1]$.

Proof.

$X \subseteq \mathrm{Orb}_{T_b}(X) = \bigcup_{k=0}^{\infty} T_b^k X$ is T_b-invariant. If $\mathrm{Orb}_{T_b}(X)$ is not dense in $[0, 1]$, then our theorem implies that $\mathrm{Orb}_{T_b}(X)$ contains at most finitely many S-integers, which contradicts X is an infinite subset of S-integers. □

Thank you