

Let us apply the potential theory to prove the following result about random Cantor sets. $b \in \mathbb{N}, b \geq 2$.

The model: b^d cubes in \mathbb{R}^d keep each with probability p , in \mathcal{Q}_0 -uniform discard otherwise. Repeat in each cube we kept to get C_2, \dots, C_n .

Thm $p \leq b^{-d} \Rightarrow C = \emptyset$ a.s.
 $p > b^{-d} \Rightarrow C$ is either empty or $\dim C = M \dim C = d + \log_b p$. The latter occurs with positive probability.

Upper bound

Lemma (Easy bound on Minkowski): Let K be a random set and $\overline{\lim} \frac{\log |\mathcal{N}(K, \varepsilon)|}{\log \varepsilon} \leq d, d \geq 0$. Then a.s. $M \dim K \leq d$.

Pf. Take $d, p, b \geq 2$. Then, for small ε , $E|\mathcal{N}(K, 2^{-n})| \leq 2^{-nd/2}$. So $IP(|\mathcal{N}(K, 2^{-n})| > 2^{nd/2}) \leq 2^{-nd/2} E|\mathcal{N}(K, 2^{-n})| \leq 2^{-nd/2} \cdot 2^{nd/2} = 1$. By Borel-Cantelli, a.s. $\lim_{n \rightarrow \infty} \frac{\log |\mathcal{N}(K, 2^{-n})|}{n \log 2} \leq d/2$.

Return to random Cantor sets.

For any kept cube, let $q_k = \binom{b^d}{k} p^k (1-p)^{b^d-k}$ be the probability that

we kept exactly k cubes inside it. Expected number of the first level kept subcubes is

$m := p b^d = \sum_k k q_k$.
 Let $z_n(Q)$ is $n=0$ the number (random) of subcubes of b -adic Q kept after n steps. Then, by induction on n ,

$$E(z_n(Q) | Q \text{ is kept}) = m^n.$$

In particular, $E(|\mathcal{N}(C, b^{-n})|) \leq m^n$. So by Lemma, $M \dim C \leq \max(\log_b m, 0) = \max(d + \log_b p, 0)$ a.s.

Lower bound.

One can proceed by using the obvious measure on C (define inductively on C_0 , pass to the limit and use Mass Distribution Principle). But we are talking about something happening locally w.r.t. random measure. Too complicated. Instead, let us use the energy of the measure.

Lemma (b -adic friendly formula for capacity). ($d \geq 0$)

For $\mu \ll \mathcal{Q}_0$, $I_2(\mu) = \sum_{k=0}^{\infty} \left[b^{-kn} \left(\sum_{Q \in \mathcal{Q}_k} \mu(Q)^2 \right) \right]$
Pf. On one hand $I_2(\mu) \geq \sum_{k=0}^{\infty} \sum_{Q \in \mathcal{Q}_k} \mu(Q)^2 \sum_{(x,y) \in Q} \mathbb{1}_{|x-y| \leq b^{-k}} = \sum_{k=0}^{\infty} \sum_{Q \in \mathcal{Q}_k} (k_n(b^{-k}) - k_n(b^{-k+1})) \mu(Q)^2 \sum_{(x,y) \in Q} \mathbb{1}_{|x-y| \leq b^{-k}} \geq \sum_{k=0}^{\infty} b^{-kn} \sum_{Q \in \mathcal{Q}_k} \mu(Q)^2$, where $b^k \geq |Q|$.

On the other hand, $I_2(\mu) \leq \sum_{k=0}^{\infty} \sum_{Q \in \mathcal{Q}_k} \mu(Q)^2 \sum_{(x,y) \in Q} \mathbb{1}_{|x-y| \leq b^{-k+1}} \leq \sum_{k=0}^{\infty} b^{-(k-1)n} \sum_{Q \in \mathcal{Q}_k} \mu(Q)^2$.

We say that b^{-n} cube Q_1 is adjacent to Q_2 if they are neighbors. Notation: $Q_1 \sim Q_2$.

Then $\sum_{(x,y) \in Q} \mathbb{1}_{|x-y| \leq b^{-k+1}} \leq \sum_{Q_1 \sim Q_2} \mu(Q_1) \mu(Q_2)$.

Now, observe first that $\mu(Q_1) \mu(Q_2) \leq \frac{\mu(Q_1)^2 + \mu(Q_2)^2}{2}$ and second, that

$$\# \{Q_1: Q_1 \sim Q\} \leq 3^d.$$

So, we have $\sum_{(x,y) \in Q} \mathbb{1}_{|x-y| \leq b^{-k+1}} \leq 3^d \sum_{Q \sim Q_1} \mu(Q)^2$.

Let us return to the random set C .

Let $z_n(Q)$ be the number of b^{-n} cubes in C which are descendants of Q . $z_n := z_n(Q_0)$.

Then $E z_n = m^n$, and for Q being a b^{-k} -cube, ($k \leq n$)

$z_n(Q)$ has the same distribution as z_{n-k} .

Define now a (random) measure μ on C by $\mu(Q) = \lim_{n \rightarrow \infty} b^{-n} z_n(Q)$.

dependant of Q . $z_n = z_n(Q)$.

Then $E z_n = m^n$, and for Q being a b^{-k} -cube, ($k < n$)

$z_n(Q)$ has the same distribution as z_{n-k} .

Define now a (random) measure μ on C by $\mu(Q) = \lim_{n \rightarrow \infty} m^{-n} z_n(Q)$.

It is indeed a measure, since $\sum_{Q \in C} \mu(Q) = \mu(Q_1) = \lim_{n \rightarrow \infty} m^{-n} z_n(Q_1) = 1$, (since it was true for any $n > k$ and $m^{-n} z_n(Q)$)

But why does the limit exist?

Lemma. $m^{-n} z_n \rightarrow \mu(Q_0)$ a.s. and in L^2 for $n > 1$.

The sets $\{\omega: \mu(Q_0) = 0\}$ and $\{\omega: C = \emptyset\}$ are the same up to a set of probability 0.

When $m \leq 1$, these sets are of full probability.

When $m > 1$, these sets are of $p < 1$.

Assume lemma, then

$$I_2(\mu) = \sum_{n=0}^{\infty} b^{-n(n+1)} \sum_{Q \in C_n} \mu(Q)^2. \text{ Observe that } \mu(Q) \text{ has the same distribution as } m^{-n} \mu(Q_0), \text{ so}$$

$$E I_2(\mu) = \sum_{n=0}^{\infty} b^{-n(n+1)} m^{-2n} E(\mu(Q_0)^2) P(Q \in C_n) =$$

The last probability is exactly p^n (need to make the pick of Q and its ancestors n times).

$$\Rightarrow E(\mu(Q_0)^2) \sum_{n=0}^{\infty} b^{-n(n+1)} (p b^n)^{2n} p^n = E(\mu(Q_0)^2) \sum_{n=0}^{\infty} b^{-n(n+1)} p^{3n} = E(\mu(Q_0)^2) \sum_{n=0}^{\infty} b^{-n(n+1)} p^{3n}.$$

Converges for $2 < d + \log_b p$ so $I_2(\mu)$ is a.s. finite.

Thus, if $\mu(C) > 0$, μ gives a measure on C with $I_2(\mu) < \infty$. By lemma, it is no more, o.s. as $C \neq \emptyset$.

Pf of Lemma.

Let $K = E(|z_1 - m z_0|^2) < \infty$ and i independent groups $E((z_i)^2) = \sum E(z_i^2)$, if $E(z_i) = 0$.

$$\text{Then } E(|z_{n+1} - m z_n|^2) = \sum_{k=0}^n E(|z_{n+1} - m z_n|^2 | z_n = j) P(z_n = j) \leq$$

$$\sum_{k=0}^n (j E(|z_1 - m|^2)) \cdot P(z_n = j) = \sum_j j P(z_n = j) = K E(z_n) = K m^n.$$

$$\text{Then } E(|m^{-n} z_n - m^{-n-1} z_{n+1}|^2) = m^{-2n-2} E(|z_{n+1} - m z_n|^2) = K m^{-2} m^{-n}.$$

So $\sum E(|m^{-n} z_n - m^{-n-1} z_{n+1}|^2) < \infty$, which means $\lim_{n \rightarrow \infty} m^{-n} z_n$ exists.

The same inequality imply a.s. convergence.

$$\text{Thus } E \sum_{n=0}^{\infty} |m^{-n} z_n - m^{-n-1} z_{n+1}|^2 = \sum E \leq \sum E(|m^{-n} z_n - m^{-n-1} z_{n+1}|^2) < \infty.$$

So μ converges a.s.

Now, notice that $\{\omega: C = \emptyset\}$ is the same as $\{\omega: z_n = 0\}$.

More obviously $\{\omega: \mu(C) = 0\} \supset \{\omega: C = \emptyset\}$, we just need to show that the sets have the same probability.

For this, consider

generating polynomial: $f(x) = \sum_{k=0}^d q_k x^k$

Note: $f(1) = 1$, $f(0) = q_0 = 1 - p$, $f'(1) = \sum k q_k = m$.

Observe also that $f'(x) = \sum k q_k x^{k-1} \geq 0$, so f is convex.

Also $f(x) = E(x^{z_1})$.

But $z_1 = \sum_{i=1}^d \{i\}$, with $\{i\}$ distributed like z_0 and independent, so

$$E(x^{z_1}) = E(x^{\sum_{i=1}^d \{i\}}) = \sum E(x^{\{1\} + \dots + \{d\}}) P(z_1 = d) =$$

$$\sum E(x^{\{1\}}) E(x^{\{d\}}) P(z_1 = d) = \sum q_k f(x)^k = f(f(x)).$$

and, in general, by induction, the generating polynomial

$$\text{of } z_n \text{ is } E(x^{z_n}) = f^{(n)}(x) - n\text{-th iteration of } f!$$

$$\text{So } P(z_n = 0) = f^{(n)}(0).$$

$f^{(n)}(0)$ converges to the smallest fixed point of $f(x)$ at $[0, 1]$. If $m \leq 1$, there is only one such fixed point, 1, so $P(C = \emptyset) = 1$.

For $m > 1$, \exists another fixed point, x_0 . So

$$P(C = \emptyset) = x_0.$$

Now, if $r = P(\mu(C) = 0)$, then

$$r = \sum_k P(\mu(C) = 0 | z_1 = k) P(z_1 = k) = \sum r^k q_k = f(r).$$

We know that $E(\mu(C)) = \lim_{n \rightarrow \infty} E(m^{-n} z_n) = 1$, so $r < 1$,

thus $r = x_0$.