The Space Complexity of Generating Random Tent Codes

Naoaki Okada (Kyushu Univ.),

*Shuji Kijima (Shiga Univ.)

This work is supported by JSPS KAKENHI JP21H03396 and JP23K21645

“Randomized algorithms, as stochastic processes”

Prologue

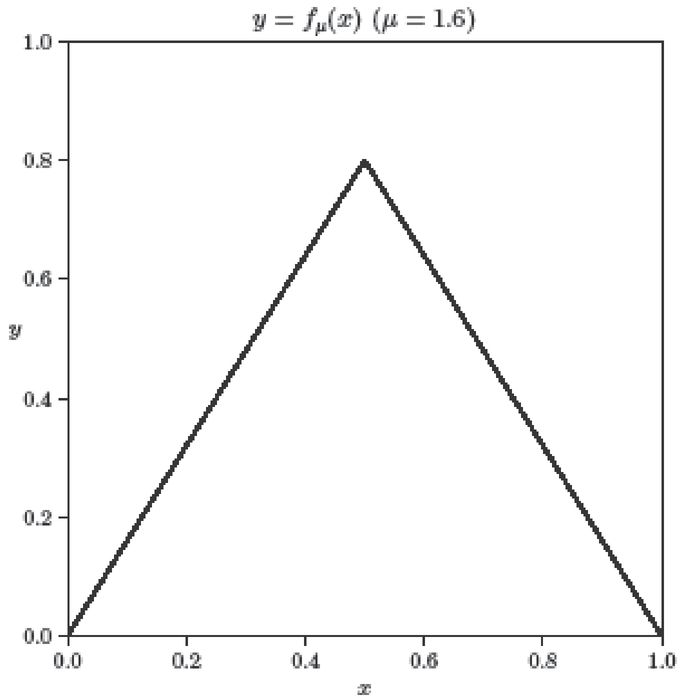
- A chaotic sequence shows a complicated behavior so that it looks unpredictable, as if a random sequence.
- Can we compute it exactly in an efficient way?
- Unfortunately, the computational complexities of chaotic sequences seem not well developed other than the numerical error arguments…
- This work investigates the computational complexity of a bit sequence generated by a tent map.

1. Tent map

Tent map

- A tent map $f: [0,1] \to [0,1]$ w/ a parameter $\mu \in (1,2)$ is given by

$$f(x) = \begin{cases} \mu x & \text{if } x \le \frac{1}{2} \\ \mu(1-x) & \text{otherwise} \end{cases}$$



$y = f(x)$

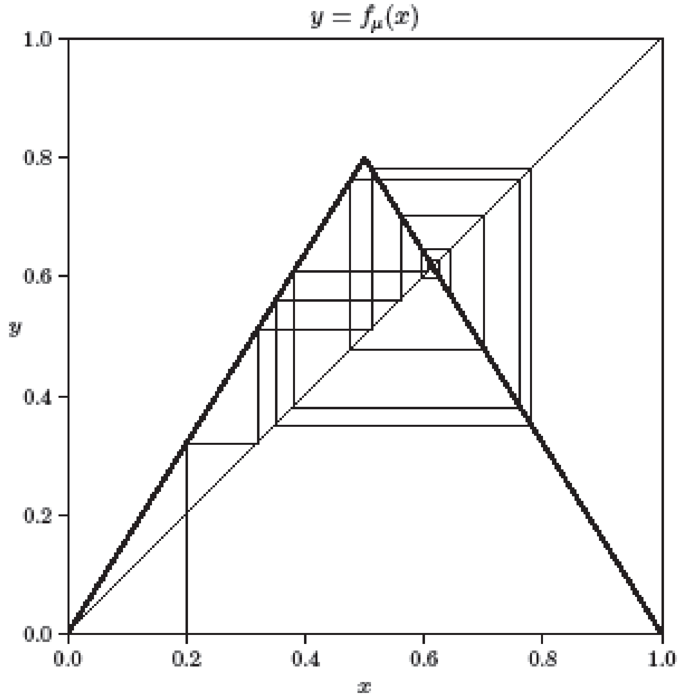
Tent map

- A tent map $f: [0,1] \to [0,1]$ w/ a parameter $\mu \in (1,2)$ is given by

$$f(x) = \begin{cases} \mu x & \text{if } x \le \frac{1}{2} \\ \mu(1-x) & \text{otherwise} \end{cases}$$

- Let $x_n = f(x_{n-1}) = f^n(x)$ for $n = 0,1,2, \dots$ where $x_0 = x$.

x_n denotes the value of iteratively n times applying the tent map to x.



cobweb

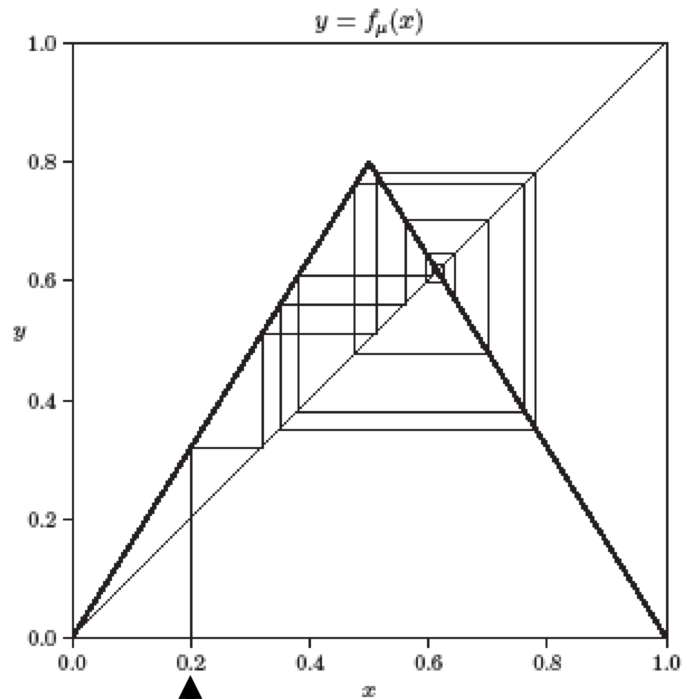
It visualizes the trajectory of x_n

Tent map

- A tent map $f:[0,1] \to [0,1]$ w/ a parameter $\mu \in (1,2)$ is given by

$$f(x) = \begin{cases} \mu x & \text{if } x \leq \dfrac{1}{2} \\ \mu(1-x) & \text{otherwise} \end{cases}$$

- Let $x_n = f(x_{n-1}) = f^n(x)$ for $n = 0,1,2,\ldots$ where $x_0 = x$.



cobweb

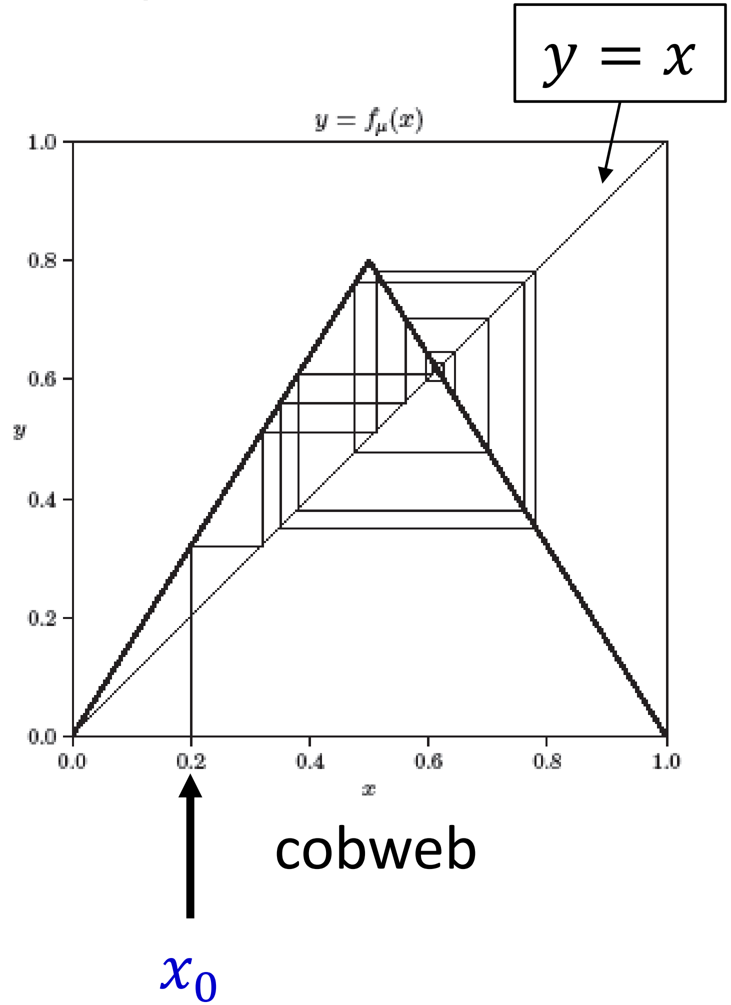
x_0

Tent map

- A tent map $f:[0,1] \to [0,1]$ w/ a parameter $\mu \in (1,2)$ is given by

$$f(x) = \begin{cases} \mu x & \text{if } x \le \dfrac{1}{2} \\ \mu(1-x) & \text{otherwise} \end{cases}$$

- Let $x_n = f(x_{n-1}) = f^n(x)$
  for $n = 0,1,2, \ldots$ where $x_0 = x$.

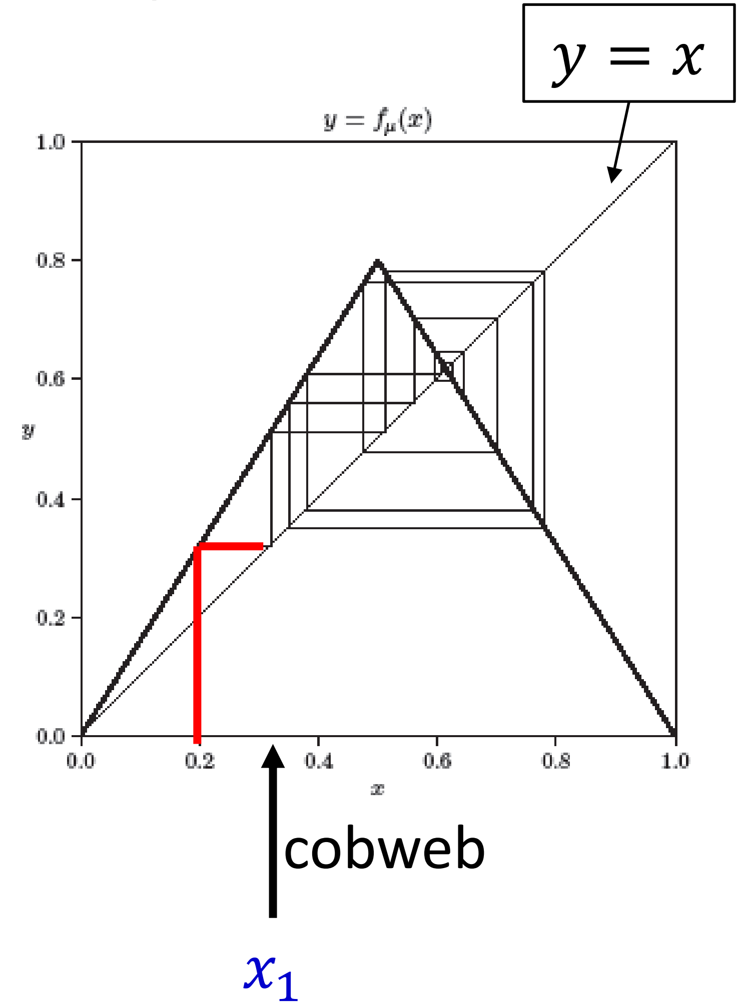


Tent map

- A tent map $f: [0,1] \to [0,1]$ w/ a parameter $\mu \in (1,2)$ is given by

$$f(x) = \begin{cases} \mu x & \text{if } x \leq \dfrac{1}{2} \\ \mu(1-x) & \text{otherwise} \end{cases}$$

- Let $x_n = f(x_{n-1}) = f^n(x)$ for $n = 0,1,2, \ldots$ where $x_0 = x$.

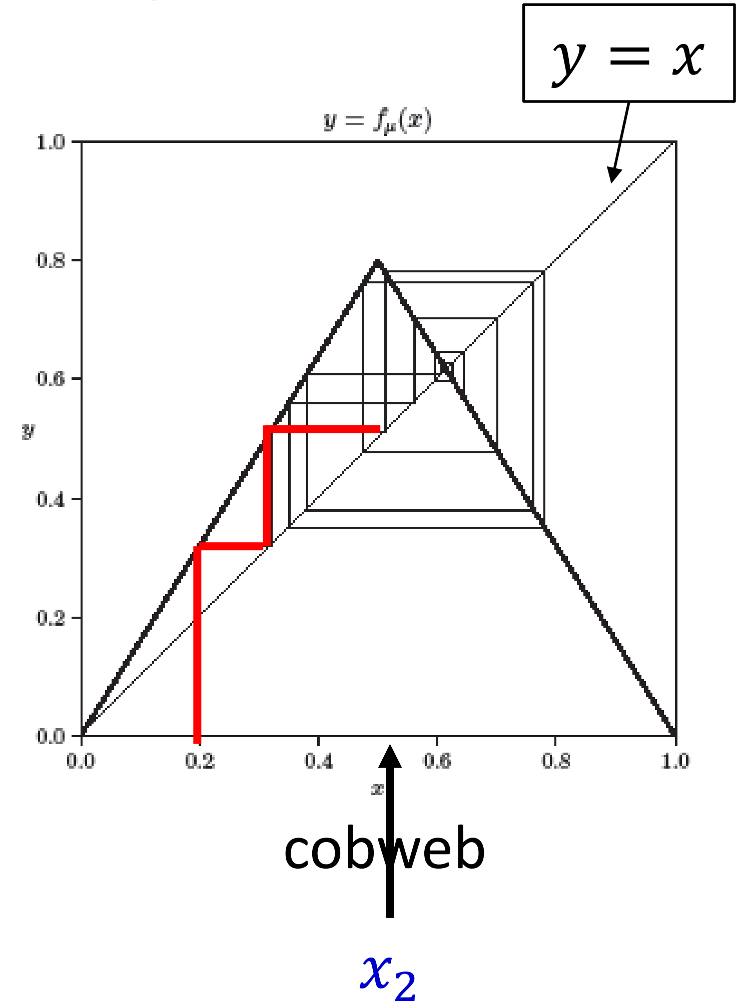


Tent map

- A tent map $f:[0,1]\to[0,1]$ w/ a parameter $\mu\in(1,2)$ is given by

$$f(x)=\begin{cases}\mu x & \text{if } x\le\frac{1}{2}\\ \mu(1-x) & \text{otherwise}\end{cases}$$

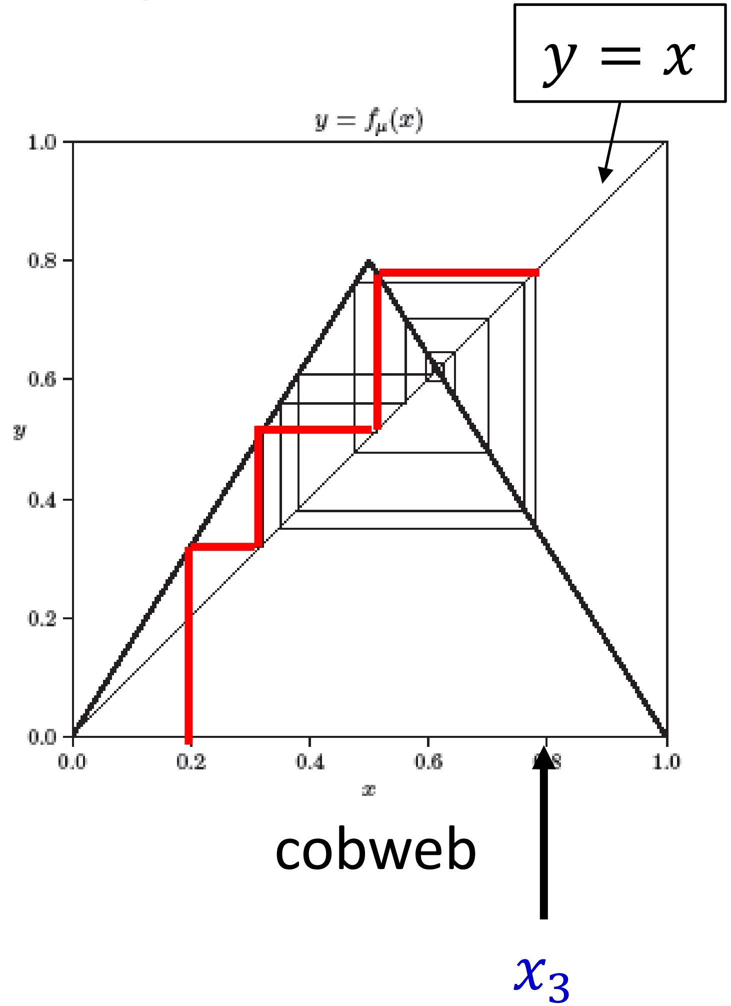
- Let $x_n = f(x_{n-1}) = f^n(x)$ for $n=0,1,2,\ldots$ where $x_0=x$.



Tent map

- A tent map $f: [0,1] \to [0,1]$ w/ a parameter $\mu \in (1,2)$ is given by

$$f(x) = \begin{cases} \mu x & \text{if } x \leq \dfrac{1}{2} \\ \mu(1-x) & \text{otherwise} \end{cases}$$



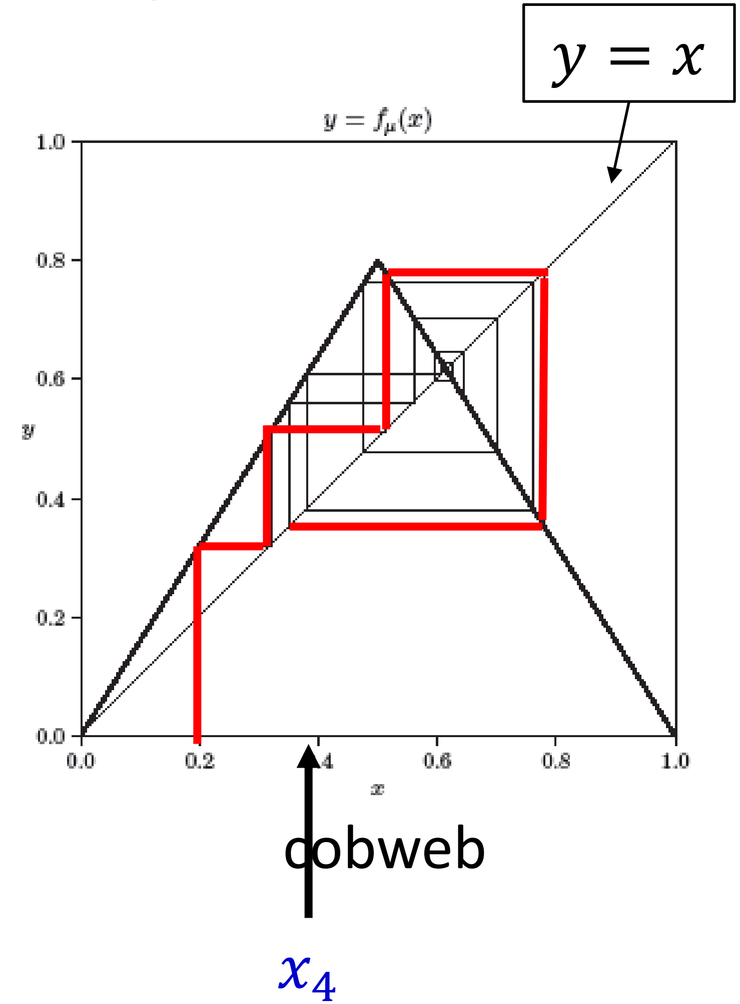
- Let $x_n = f(x_{n-1}) = f^n(x)$ for $n = 0,1,2,\ldots$ where $x_0 = x$.

Tent map

- A tent map $f: [0,1] \to [0,1]$ w/ a parameter $\mu \in (1,2)$ is given by

$$f(x) = \begin{cases} \mu x & \text{if } x \le \dfrac{1}{2} \\ \mu(1-x) & \text{otherwise} \end{cases}$$

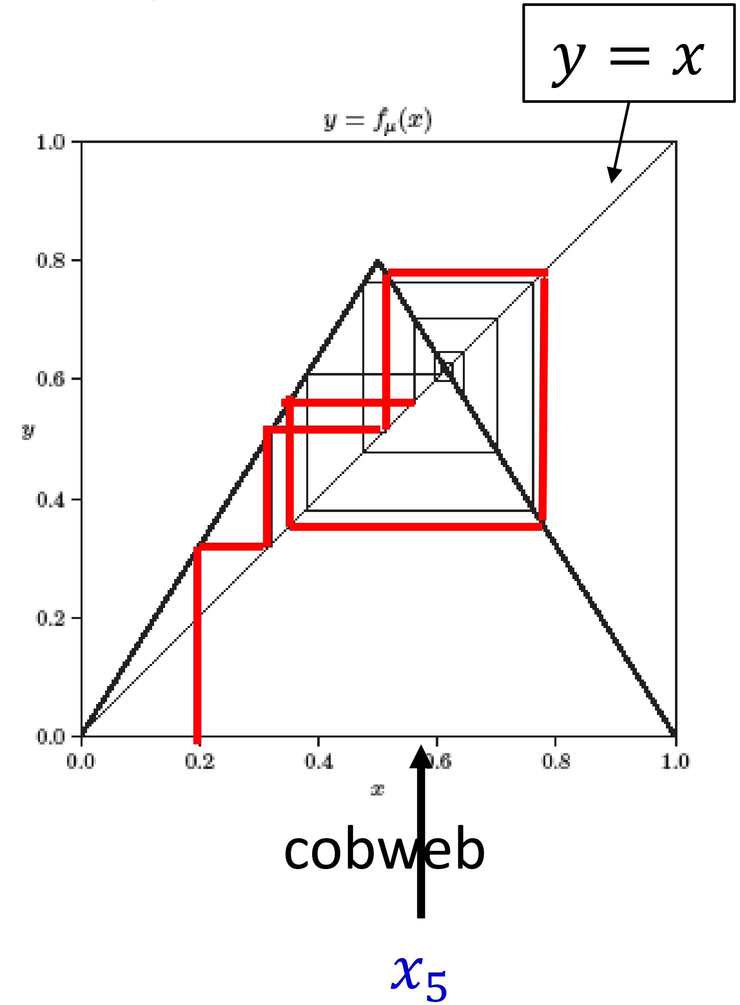
- Let $x_n = f(x_{n-1}) = f^n(x)$ for $n = 0,1,2,\ldots$ where $x_0 = x$.



Tent map

- A tent map $f: [0,1] \to [0,1]$ w/ a parameter $\mu \in (1,2)$ is given by

$$f(x) = \begin{cases} \mu x & \text{if } x \le \frac{1}{2} \\ \mu(1-x) & \text{otherwise} \end{cases}$$

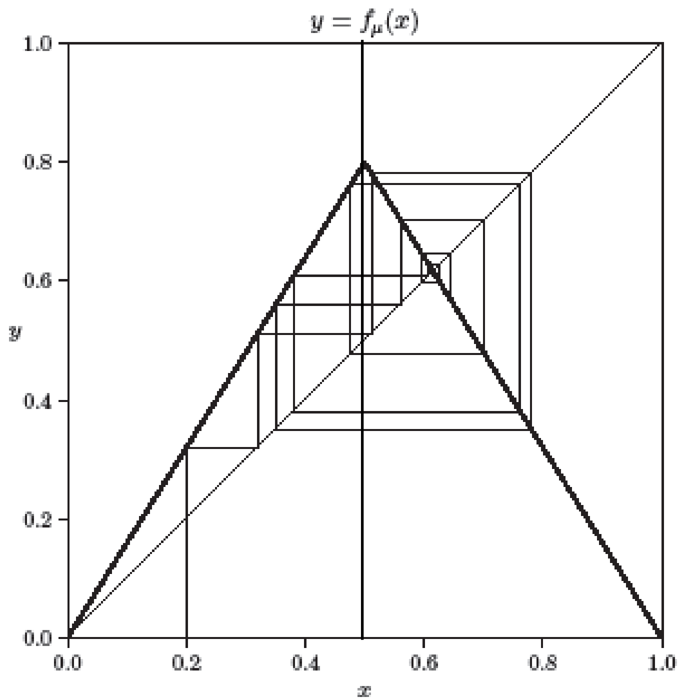


- Let $x_n = f(x_{n-1}) = f^n(x)$ for $n = 0,1,2,\ldots$ where $x_0 = x$.

Tent map

- A tent map $f: [0,1] \to [0,1]$ w/ a parameter $\mu \in (1,2)$ is given by

$$f(x) = \begin{cases} \mu x & \text{if } x \leq \frac{1}{2} \\ \mu(1-x) & \text{otherwise} \end{cases}$$



cobweb

- Let $x_n = f(x_{n-1}) = f^n(x)$ for $n = 0,1,2,\ldots$ where $x_0 = x$.

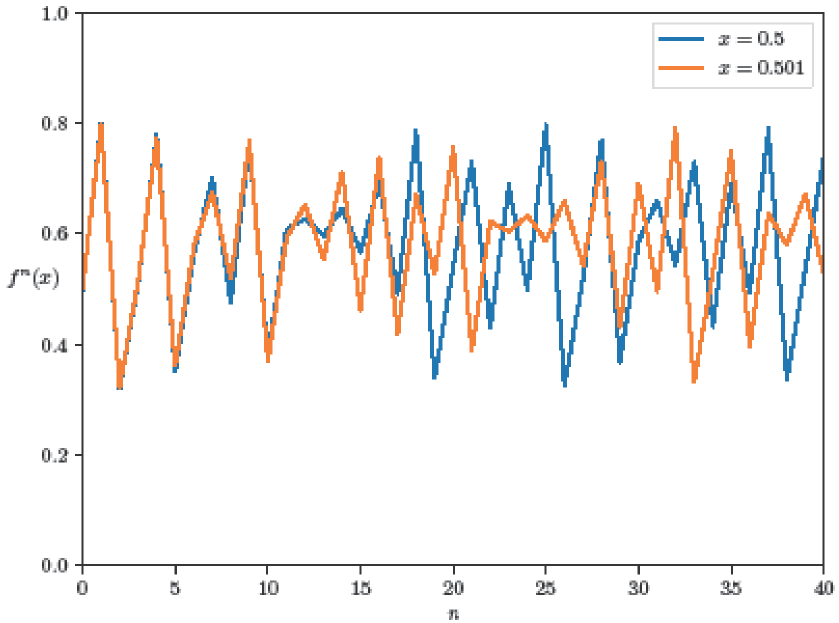
The trajectory of $x_0, x_1, \ldots$ looks very complicated.

This work is concerned with the **computational complexity** of deciding **whether $x_n \leq \frac{1}{2}$ or not** as given n.

Existing works and contribution

iterated tent map

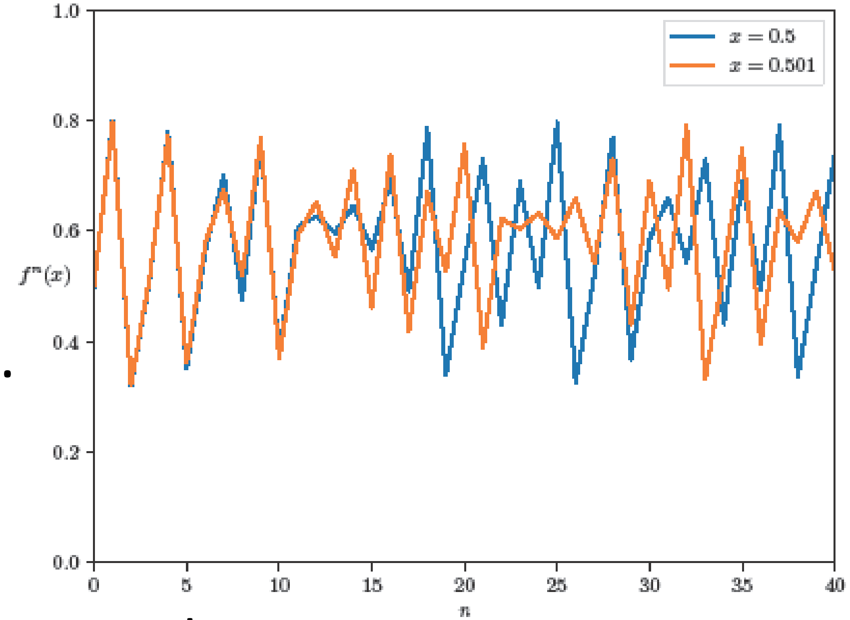
- The trajectory $x_0, x_1, x_2, \ldots$ is known to be chaotic.
  - ✓ e.g., sensitive to initial conditions.



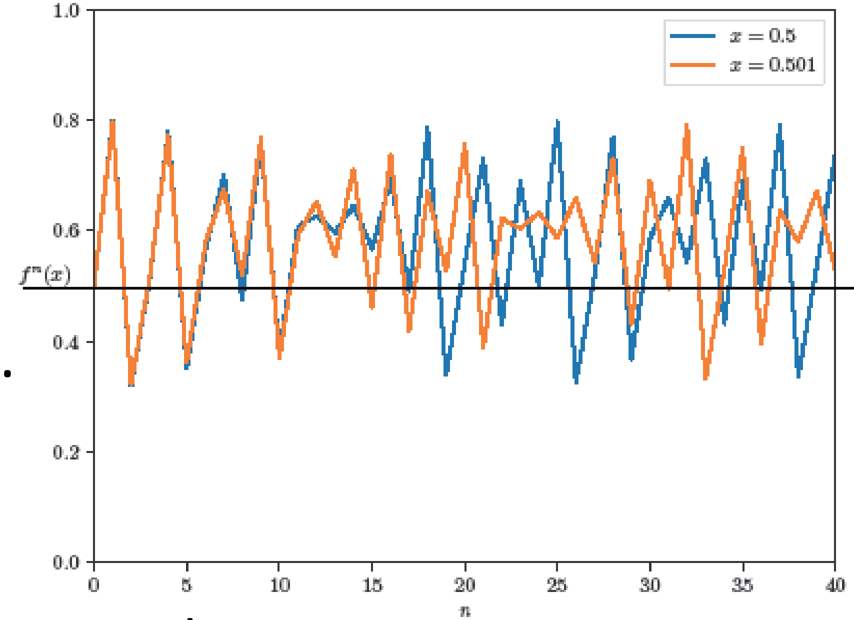
- In this figure
  - ➢ Blue line shows the trajectory starting from $x = 0.5$ and
  - ➢ Orange line shows the trajectory starting from $x = 0.501$
- In the first few steps, the trajectories look very similar, but they look completely different at 20 steps, and after that.
- This phenomenon is known as the sensitivity to initial conditions, that is a typical property of a chaotic sequence.

Existing works and contribution

- The trajectory $x_0, x_1, x_2, \ldots$ is known to be chaotic.
  - ✓ e.g., sensitive to initial conditions.
- Much is known about the tent map and many applications.
  - ✓ E.g., pseud random generator, AD converter.



Existing works and contribution



- The trajectory $x_0, x_1, x_2, \ldots$ is known to be chaotic.
  - ✓ e.g., sensitive to initial conditions.
- Much is known about the tent map and many applications.
  - ✓ E.g., pseud random generator, AD converter.
- Nevertheless, the **computational complexity** seems not established.
  e.g., the time complexity for a tent map f_μ of
  "deciding whether $x_n \leq \frac{1}{2}$ or not as given n and x"
  seems not known (maybe **NP-hard** but I don't know).

This work is concerned with the **space complexity** of a related problem.

2. Target and main result

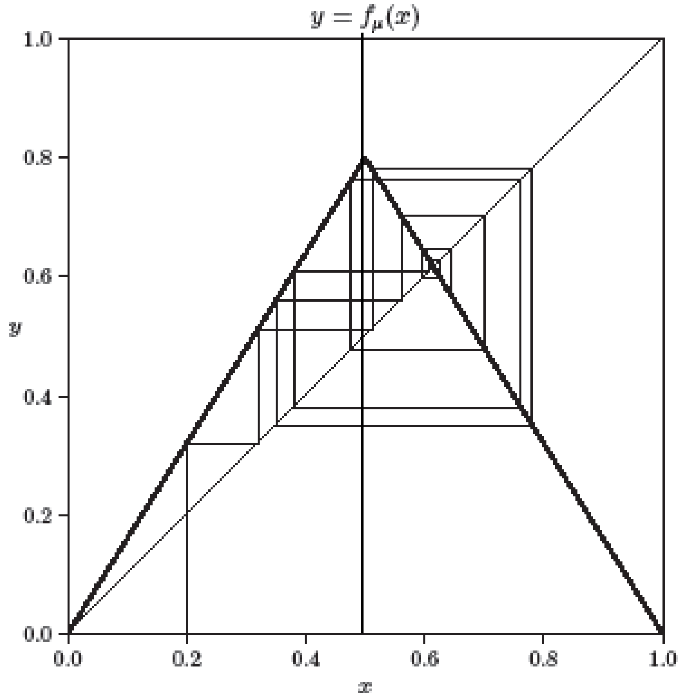
Tent code

$\gamma^n(x) = b_1 b_2 \cdots b_n$ for $x \in [0,1)$ where

$$b_1 = \begin{cases} 0 & \text{if } x < \frac{1}{2} \\ 1 & \text{otherwise} \end{cases}$$

and

$$b_{i+1} = \begin{cases} 0 & \text{if } [b_i = 0] \wedge \left[x_i < \frac{1}{2}\right] \\ 1 & \text{if } [b_i = 0] \wedge \left[x_i \geq \frac{1}{2}\right] \\ 1 & \text{if } [b_i = 1] \wedge \left[x_i \leq \frac{1}{2}\right] \\ 0 & \text{if } [b_i = 1] \wedge \left[x_i > \frac{1}{2}\right] \end{cases}$$



cobweb

Prop.

- $x = \sum_{i=1}^{\infty} \frac{1}{\mu_i} b_i$ (decodable)
- If $x \leq x'$ then $\gamma^n(x) \preccurlyeq \gamma^n\ (x')$ (order preserving)
- $\gamma^n(x) = \gamma^n(x+0)$ (right continuous)
- If $b_i = b_{i+1}$ then $x_i \leq \frac{1}{2}$. If $b_i \neq b_{i+1}$ then $x_i \geq \frac{1}{2}$ (left-right decision)

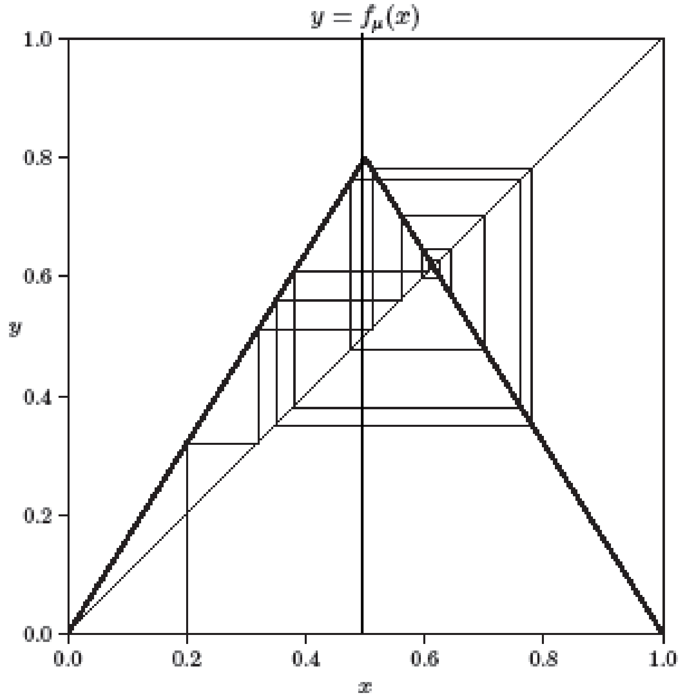
Tent code

$\gamma^n(x) = b_1 b_2 \cdots b_n$ for $x \in [0,1)$ where

$$b_1 = \begin{cases} 0 & \text{if } x < \frac{1}{2} \\ 1 & \text{otherwise} \end{cases}$$

and

$$b_{i+1} = \begin{cases} b_i & \text{if } x_i < \frac{1}{2} \\ \overline{b_i} & \text{if } x_i > \frac{1}{2} \\ 1 & \text{if } x_i = \frac{1}{2} \end{cases}$$



cobweb

Prop.

- $x = \sum_{i=1}^{\infty} \frac{1}{\mu_i} b_i$ (decodable)
- If $x \leq x'$ then $\gamma^n(x) \preccurlyeq \gamma^n\,(x')$ (order preserving)
- $\gamma^n(x) = \gamma^n(x+0)$ (right continuous)
- If $b_i = b_{i+1}$ then $x_i \leq \frac{1}{2}$. If $b_i \neq b_{i+1}$ then $x_i \geq \frac{1}{2}$ (left-right decision)

Tent code

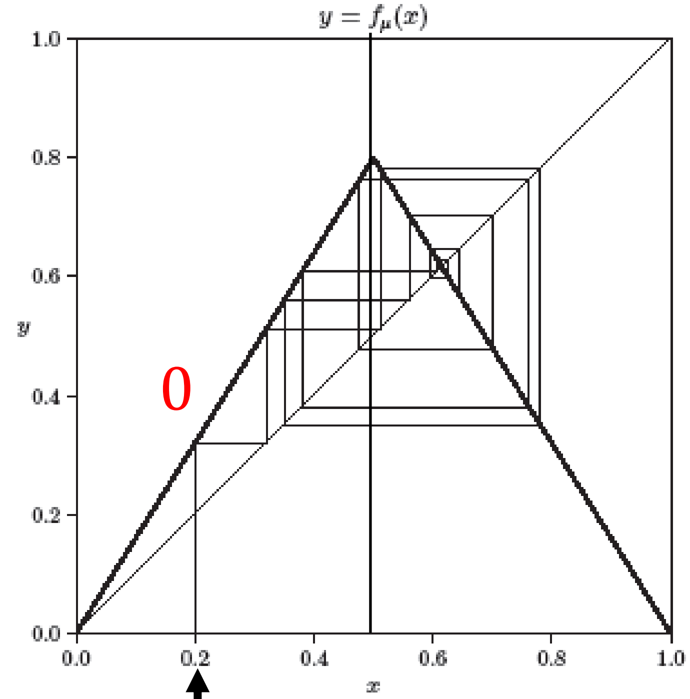
$\gamma^n(x) = b_1 b_2 \cdots b_n$ for $x \in [0,1)$ where

$$b_1 = \begin{cases} 0 & \text{if } x < \frac{1}{2} \\ 1 & \text{otherwise} \end{cases}$$

and

$$b_{i+1} = \begin{cases} b_i & \text{if } x_i < \frac{1}{2} \\ \overline{b_i} & \text{if } x_i > \frac{1}{2} \\ 1 & \text{if } x_i = \frac{1}{2} \end{cases}$$

$\gamma^1(0.2) = 0$



x_0 cobweb

Prop.

- $x = \sum_{i=1}^{\infty} \frac{1}{\mu_i} b_i$ (decodable)
- If $x \le x'$ then $\gamma^n(x) \preccurlyeq \gamma^n(x')$ (order preserving)
- $\gamma^n(x) = \gamma^n(x+0)$ (right continuous)
- If $b_i = b_{i+1}$ then $x_i \le \frac{1}{2}$. If $b_i \neq b_{i+1}$ then $x_i \ge \frac{1}{2}$ (left-right decision)

Tent code

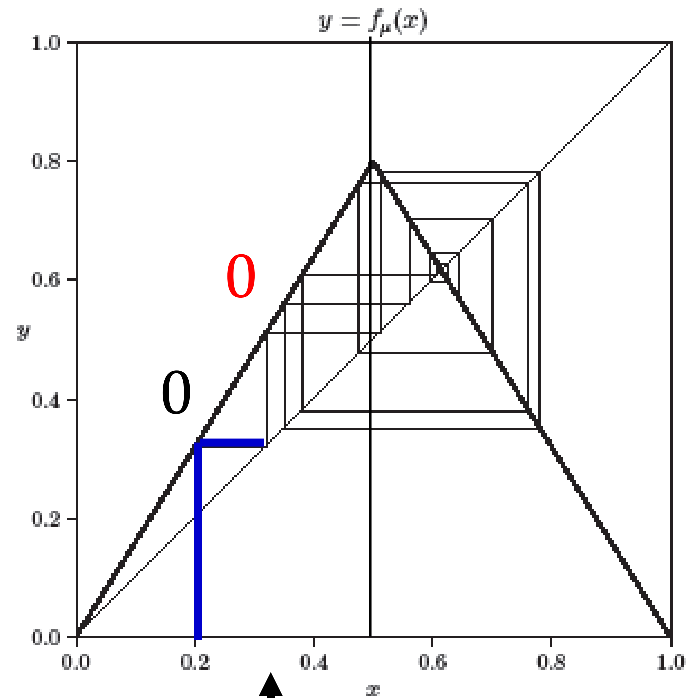
$\gamma^n(x) = b_1 b_2 \cdots b_n$ for $x \in [0,1)$ where

$$b_1 = \begin{cases} 0 & \text{if } x < \frac{1}{2} \\ 1 & \text{otherwise} \end{cases}$$

and

$$b_{i+1} = \begin{cases} b_i & \text{if } x_i < \frac{1}{2} \\ \overline{b_i} & \text{if } x_i > \frac{1}{2} \\ 1 & \text{if } x_i = \frac{1}{2} \end{cases}$$

$\gamma^2(0.2) = 00$



cobweb

x_1

Prop.

- $x = \sum_{i=1}^{\infty} \frac{1}{\mu_i} b_i$ (decodable)
- If $x \leq x'$ then $\gamma^n(x) \preccurlyeq \gamma^n(x')$ (order preserving)
- $\gamma^n(x) = \gamma^n(x+0)$ (right continuous)
- If $b_i = b_{i+1}$ then $x_i \leq \frac{1}{2}$. If $b_i \neq b_{i+1}$ then $x_i \geq \frac{1}{2}$ (left-right decision)

Tent code

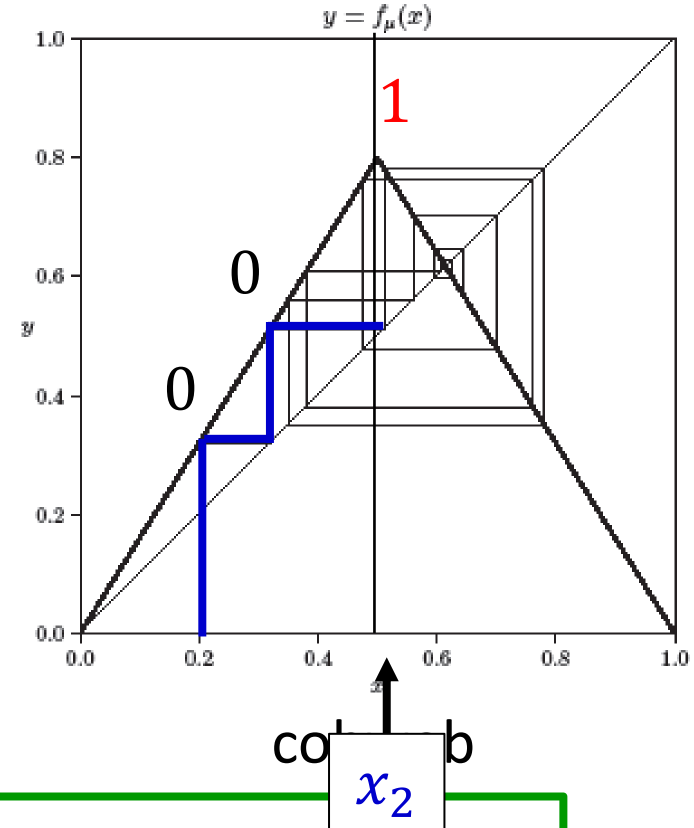
$\gamma^n(x) = b_1 b_2 \cdots b_n$ for $x \in [0,1)$ where

$$b_1 = \begin{cases} 0 & \text{if } x < \frac{1}{2} \\ 1 & \text{otherwise} \end{cases}$$

and

$$b_{i+1} = \begin{cases} b_i & \text{if } x_i < \frac{1}{2} \\ \overline{b_i} & \text{if } x_i > \frac{1}{2} \\ 1 & \text{if } x_i = \frac{1}{2} \end{cases}$$

$\gamma^3(0.2) = 001$



Prop.

- $x = \sum_{i=1}^{\infty} \frac{1}{\mu_i} b_i$ (decodable)
- If $x \leq x'$ then $\gamma^n(x) \preccurlyeq \gamma^n(x')$ (order preserving)
- $\gamma^n(x) = \gamma^n(x+0)$ (right continuous)
- If $b_i = b_{i+1}$ then $x_i \leq \frac{1}{2}$. If $b_i \neq b_{i+1}$ then $x_i \geq \frac{1}{2}$ (left-right decision)

Tent code

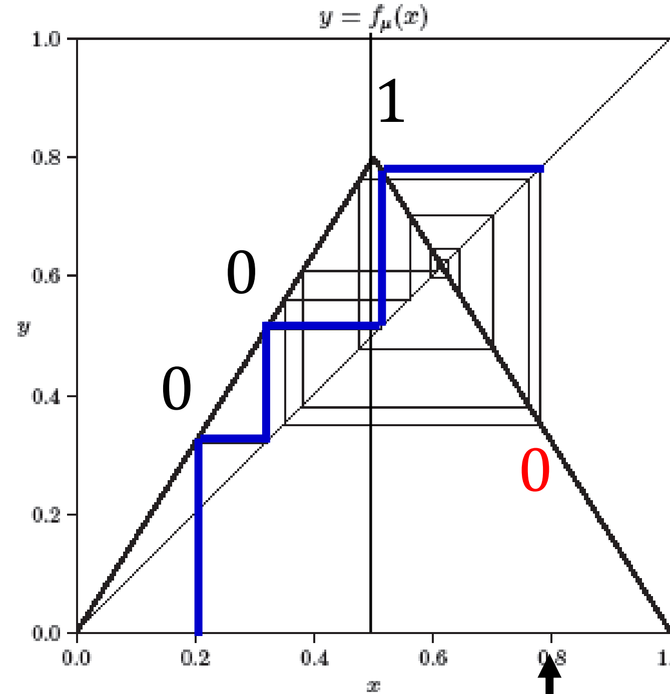
$\gamma^n(x) = b_1 b_2 \cdots b_n$ for $x \in [0,1)$ where

$$b_1 = \begin{cases} 0 & \text{if } x < \frac{1}{2} \\ 1 & \text{otherwise} \end{cases}$$

and

$$b_{i+1} = \begin{cases} b_i & \text{if } x_i < \frac{1}{2} \\ \overline{b_i} & \text{if } x_i > \frac{1}{2} \\ 1 & \text{if } x_i = \frac{1}{2} \end{cases}$$

$\gamma^4(0.2) = 0010$



cobweb

x_3

Prop.

- $x = \sum_{i=1}^{\infty} \frac{1}{\mu_i} b_i$ (decodable)
- If $x \le x'$ then $\gamma^n(x) \preccurlyeq \gamma^n(x')$ (order preserving)
- $\gamma^n(x) = \gamma^n(x+0)$ (right continuous)
- If $b_i = b_{i+1}$ then $x_i \le \frac{1}{2}$. If $b_i \ne b_{i+1}$ then $x_i \ge \frac{1}{2}$ (left-right decision)

Tent code

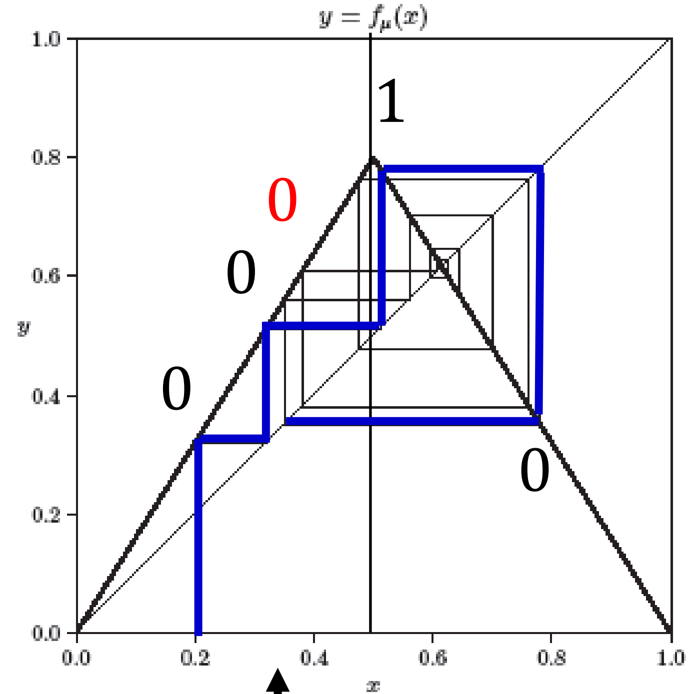
$\gamma^n(x) = b_1 b_2 \cdots b_n$ for $x \in [0,1)$ where

$$b_1 = \begin{cases} 0 & \text{if } x < \frac{1}{2} \\ 1 & \text{otherwise} \end{cases}$$

and

$$b_{i+1} = \begin{cases} b_i & \text{if } x_i < \frac{1}{2} \\ \overline{b_i} & \text{if } x_i > \frac{1}{2} \\ 1 & \text{if } x_i = \frac{1}{2} \end{cases}$$

$\gamma^5(0.2) = 00100$



cobweb

x_4

Prop.

- $x = \sum_{i=1}^{\infty} \frac{1}{\mu_i} b_i$ (decodable)
- If $x \leq x'$ then $\gamma^n(x) \preccurlyeq \gamma^n(x')$ (order preserving)
- $\gamma^n(x) = \gamma^n(x+0)$ (right continuous)
- If $b_i = b_{i+1}$ then $x_i \leq \frac{1}{2}$. If $b_i \neq b_{i+1}$ then $x_i \geq \frac{1}{2}$ (left-right decision)

Tent code

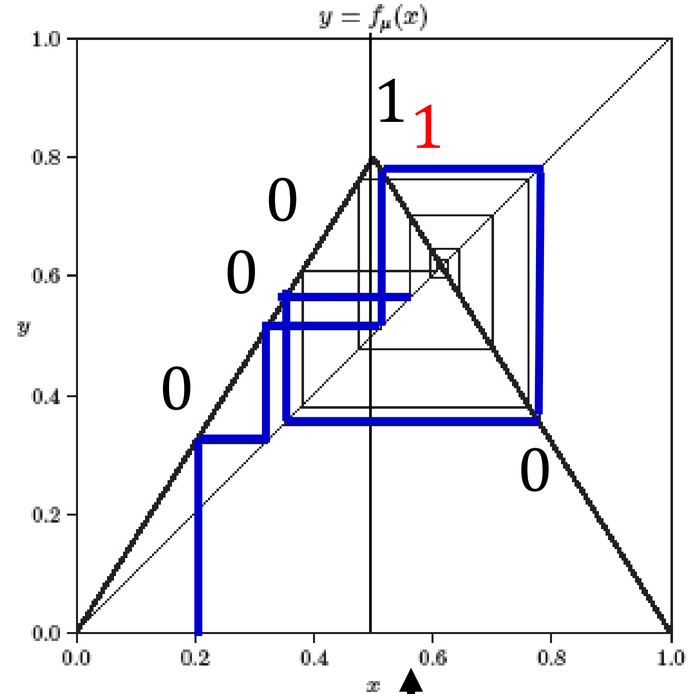
$\gamma^n(x) = b_1 b_2 \cdots b_n$ for $x \in [0,1)$ where

$$b_1 = \begin{cases} 0 & \text{if } x < \frac{1}{2} \\ 1 & \text{otherwise} \end{cases}$$

and

$$b_{i+1} = \begin{cases} b_i & \text{if } x_i < \frac{1}{2} \\ \overline{b_i} & \text{if } x_i > \frac{1}{2} \\ 1 & \text{if } x_i = \frac{1}{2} \end{cases}$$

$$\gamma^6(0.2) = 001001$$



cobweb

x_5

Prop.

- $x = \sum_{i=1}^{\infty} \frac{1}{\mu_i} b_i$ (decodable)
- If $x \le x'$ then $\gamma^n(x) \preccurlyeq \gamma^n(x')$ (order preserving)
- $\gamma^n(x) = \gamma^n(x+0)$ (right continuous)
- If $b_i = b_{i+1}$ then $x_i \le \frac{1}{2}$. If $b_i \ne b_{i+1}$ then $x_i \ge \frac{1}{2}$ (left-right decision)

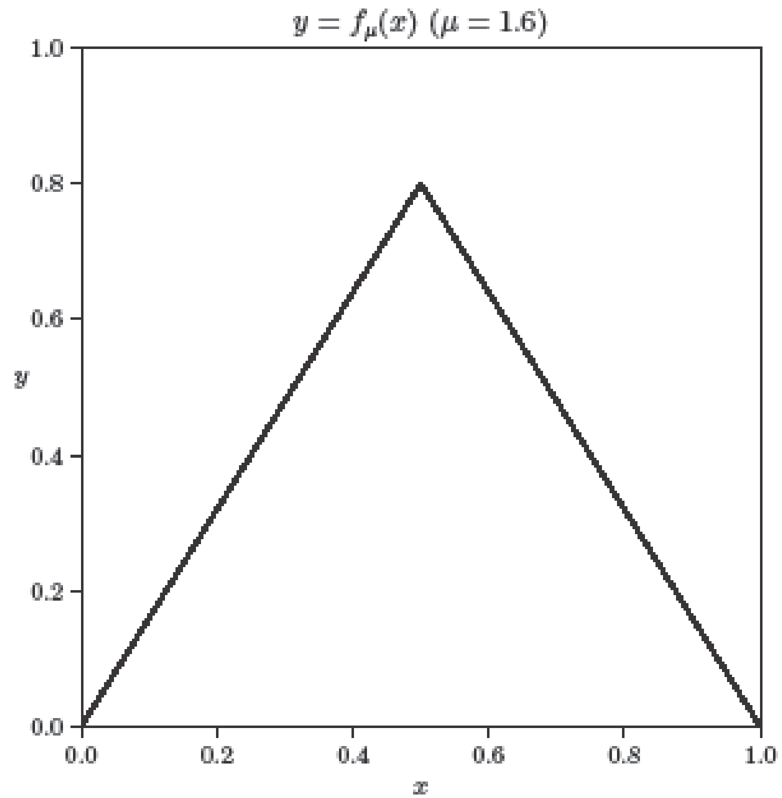
Tent code

$\gamma^n(x) = b_1 b_2 \cdots b_n$ for $x \in [0,1)$ where

$$b_1 = \begin{cases} 0 & \text{if } x < \frac{1}{2} \\ 1 & \text{otherwise} \end{cases}$$

and

$$b_{i+1} = \begin{cases} b_i & \text{if } x_i < \frac{1}{2} \\ \overline{b_i} & \text{if } x_i > \frac{1}{2} \\ 1 & \text{if } x_i = \frac{1}{2} \end{cases}$$



$y = f(x)$

Prop.

- $x = \sum_{i=1}^{\infty} \frac{1}{\mu_i} b_i$ (decodable)
- If $x \leq x'$ then $\gamma^n(x) \preccurlyeq \gamma^n\ (x')$ (order preserving)
- $\gamma^n(x) = \gamma^n(x+0)$ (right continuous)
- If $b_i = b_{i+1}$ then $x_i \leq \frac{1}{2}$. If $b_i \neq b_{i+1}$ then $x_i \geq \frac{1}{2}$ (left-right decision)

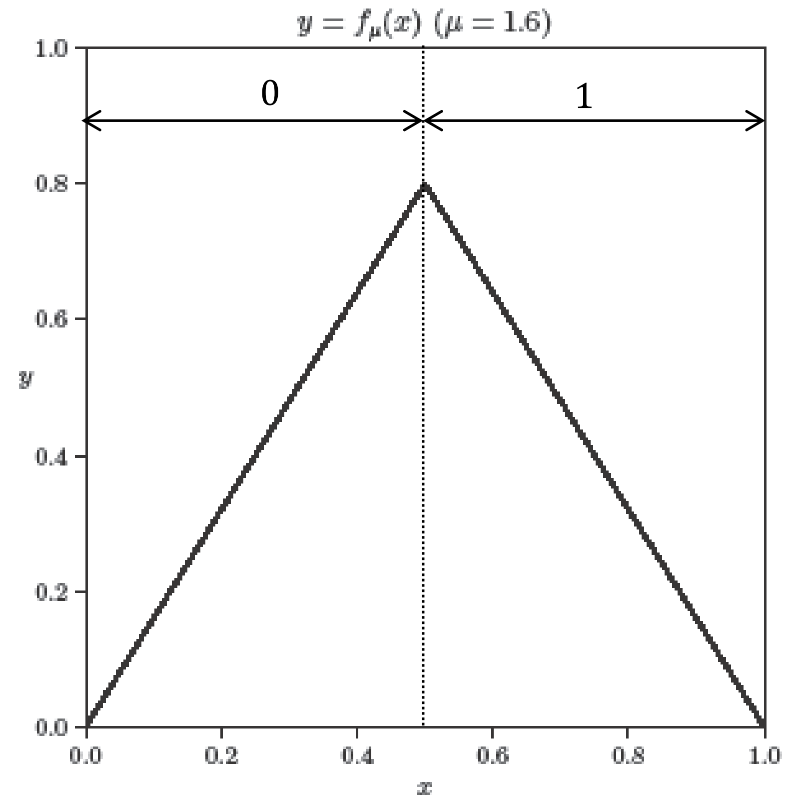
Tent code

$\gamma^n(x) = b_1 b_2 \cdots b_n$ for $x \in [0,1)$ where

$$b_1 = \begin{cases} 0 & \text{if } x < \frac{1}{2} \\ 1 & \text{otherwise} \end{cases}$$

and

$$b_{i+1} = \begin{cases} b_i & \text{if } x_i < \frac{1}{2} \\ \overline{b_i} & \text{if } x_i > \frac{1}{2} \\ 1 & \text{if } x_i = \frac{1}{2} \end{cases}$$



$y = f(x)$

Prop.

- $x = \sum_{i=1}^{\infty} \frac{1}{\mu_i} b_i$ (decodable)
- If $x \le x'$ then $\gamma^n(x) \preccurlyeq \gamma^n(x')$ (order preserving)
- $\gamma^n(x) = \gamma^n(x+0)$ (right continuous)
- If $b_i = b_{i+1}$ then $x_i \le \frac{1}{2}$. If $b_i \ne b_{i+1}$ then $x_i \ge \frac{1}{2}$ (left-right decision)

Tent code

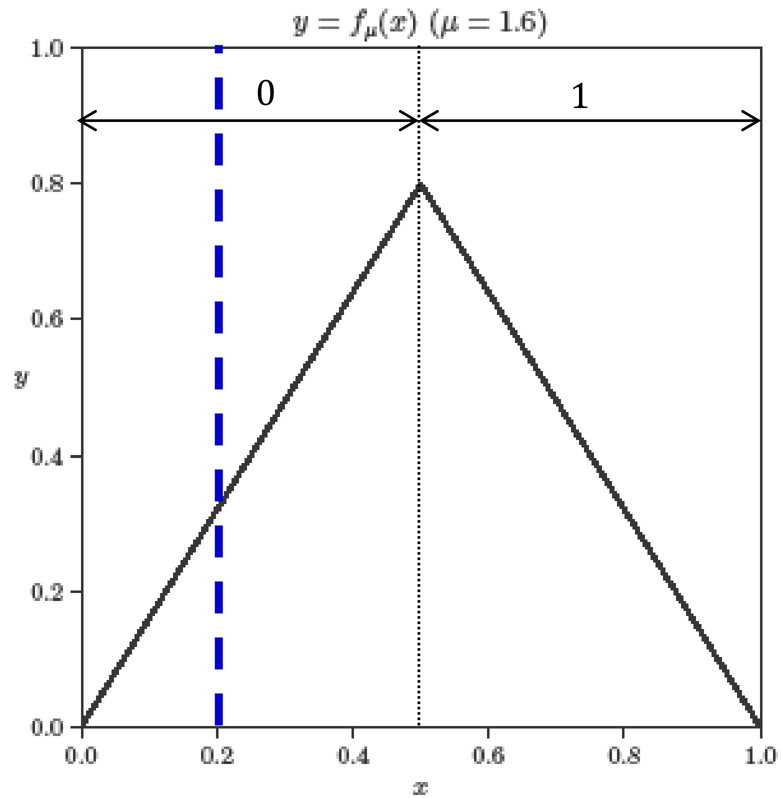
$\gamma^n(x) = b_1 b_2 \cdots b_n$ for $x \in [0,1)$ where

$$b_1 = \begin{cases} 0 & \text{if } x < \frac{1}{2} \\ 1 & \text{otherwise} \end{cases}$$

and

$$b_{i+1} = \begin{cases} b_i & \text{if } x_i < \frac{1}{2} \\ \overline{b_i} & \text{if } x_i > \frac{1}{2} \\ 1 & \text{if } x_i = \frac{1}{2} \end{cases}$$

$\gamma^1(0.2) = 0$



$y = f(x)$

Prop.

- $x = \sum_{i=1}^{\infty} \frac{1}{\mu_i} b_i$ (decodable)
- If $x \leq x'$ then $\gamma^n(x) \preccurlyeq \gamma^n\ (x')$ (order preserving)
- $\gamma^n(x) = \gamma^n(x+0)$ (right continuous)
- If $b_i = b_{i+1}$ then $x_i \leq \frac{1}{2}$. If $b_i \neq b_{i+1}$ then $x_i \geq \frac{1}{2}$ (left-right decision)

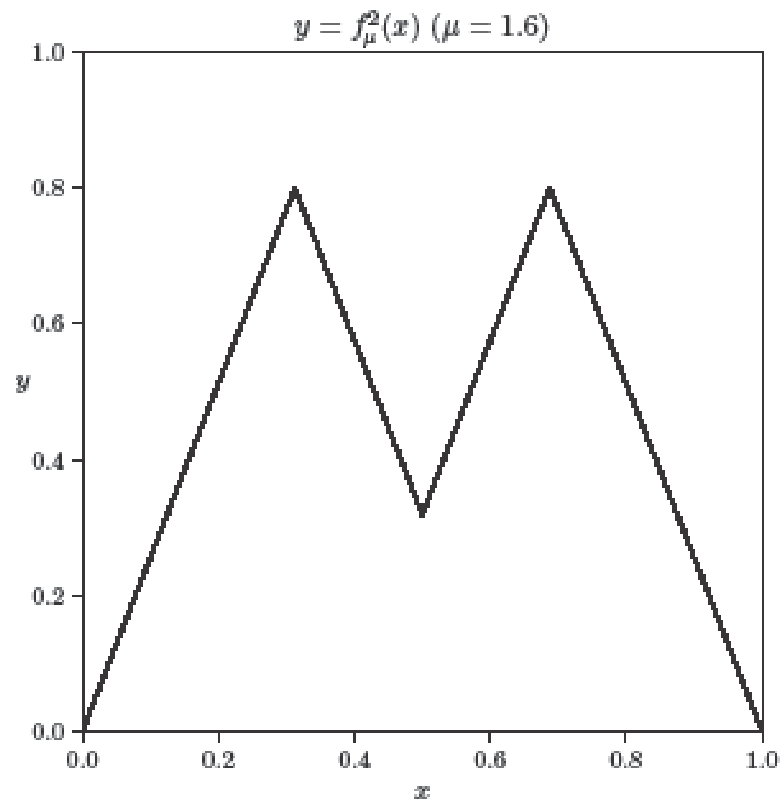
Tent code

$\gamma^n(x) = b_1 b_2 \cdots b_n$ for $x \in [0,1)$ where

$$b_1 = \begin{cases} 0 & \text{if } x < \frac{1}{2} \\ 1 & \text{otherwise} \end{cases}$$

and

$$b_{i+1} = \begin{cases} b_i & \text{if } x_i < \frac{1}{2} \\ \overline{b_i} & \text{if } x_i > \frac{1}{2} \\ 1 & \text{if } x_i = \frac{1}{2} \end{cases}$$



$y = f^2(x)$

Prop.

- $x = \sum_{i=1}^{\infty} \frac{1}{\mu_i} b_i$ (decodable)
- If $x \leq x'$ then $\gamma^n(x) \preccurlyeq \gamma^n\ (x')$ (order preserving)
- $\gamma^n(x) = \gamma^n(x+0)$ (right continuous)
- If $b_i = b_{i+1}$ then $x_i \leq \frac{1}{2}$. If $b_i \neq b_{i+1}$ then $x_i \geq \frac{1}{2}$ (left-right decision)

Tent code

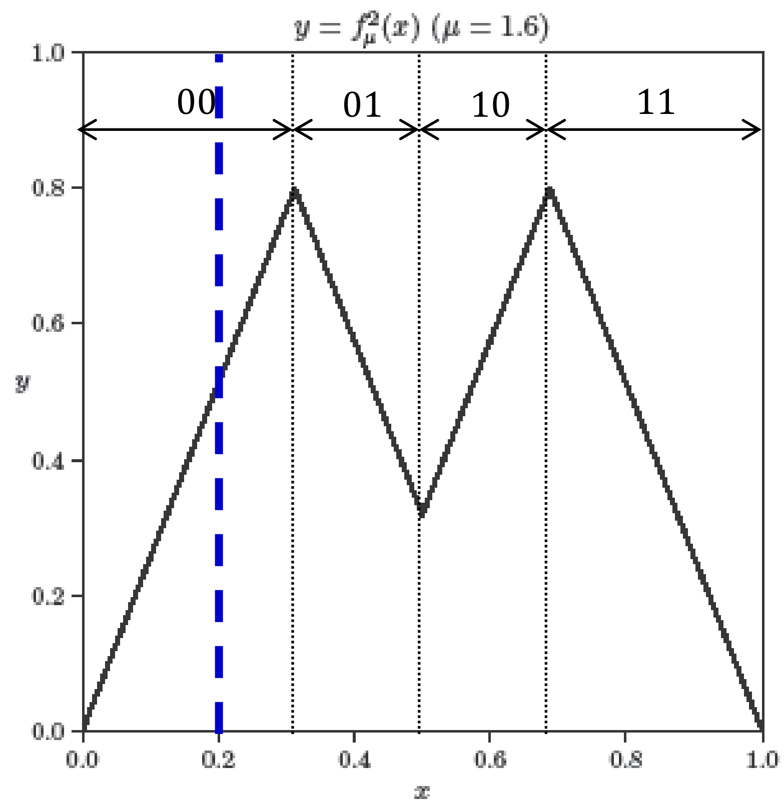
$\gamma^n(x) = b_1 b_2 \cdots b_n$ for $x \in [0,1)$ where

$$b_1 = \begin{cases} 0 & \text{if } x < \frac{1}{2} \\ 1 & \text{otherwise} \end{cases}$$

and

$$b_{i+1} = \begin{cases} b_i & \text{if } x_i < \frac{1}{2} \\ \overline{b_i} & \text{if } x_i > \frac{1}{2} \\ 1 & \text{if } x_i = \frac{1}{2} \end{cases}$$

$$\gamma^2(0.2) = 00$$



$y = f^2(x)$

Prop.

- $x = \sum_{i=1}^{\infty} \frac{1}{\mu_i} b_i$ (decodable)
- If $x \leq x'$ then $\gamma^n(x) \preccurlyeq \gamma^n(x')$ (order preserving)
- $\gamma^n(x) = \gamma^n(x+0)$ (right continuous)
- If $b_i = b_{i+1}$ then $x_i \leq \frac{1}{2}$. If $b_i \neq b_{i+1}$ then $x_i \geq \frac{1}{2}$ (left-right decision)

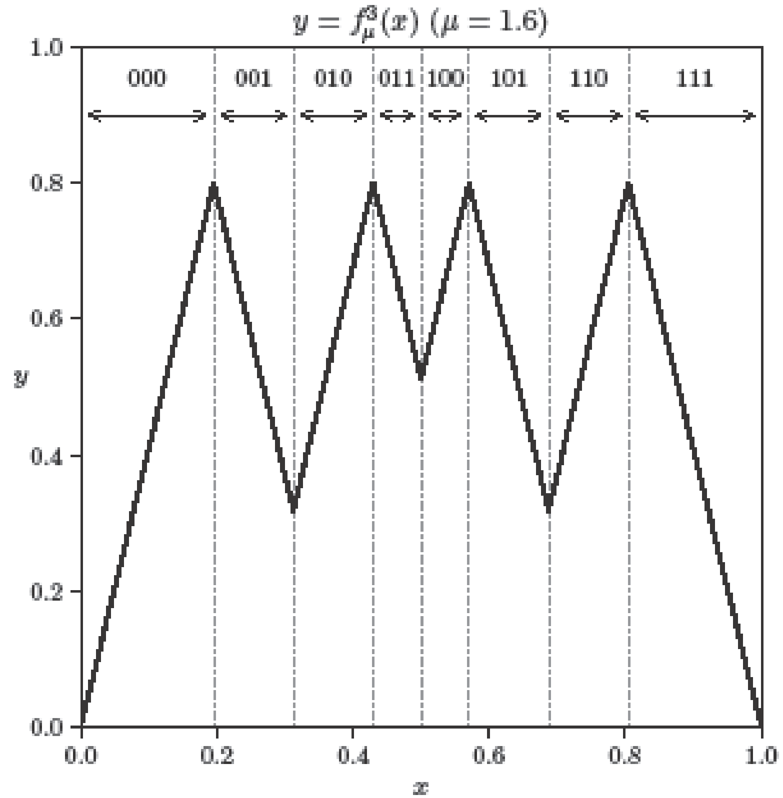
Tent code

$\gamma^n(x) = b_1 b_2 \cdots b_n$ for $x \in [0,1)$ where

$$b_1 = \begin{cases} 0 & \text{if } x < \frac{1}{2} \\ 1 & \text{otherwise} \end{cases}$$

and

$$b_{i+1} = \begin{cases} b_i & \text{if } x_i < \frac{1}{2} \\ \overline{b_i} & \text{if } x_i > \frac{1}{2} \\ 1 & \text{if } x_i = \frac{1}{2} \end{cases}$$



$y = f^3(x)$

Prop.

- $x = \sum_{i=1}^{\infty} \frac{1}{\mu_i} b_i$ (decodable)
- If $x \le x'$ then $\gamma^n(x) \preccurlyeq \gamma^n\,(x')$ (order preserving)
- $\gamma^n(x) = \gamma^n(x+0)$ (right continuous)
- If $b_i = b_{i+1}$ then $x_i \le \frac{1}{2}$. If $b_i \ne b_{i+1}$ then $x_i \ge \frac{1}{2}$ (left-right decision)

Tent code

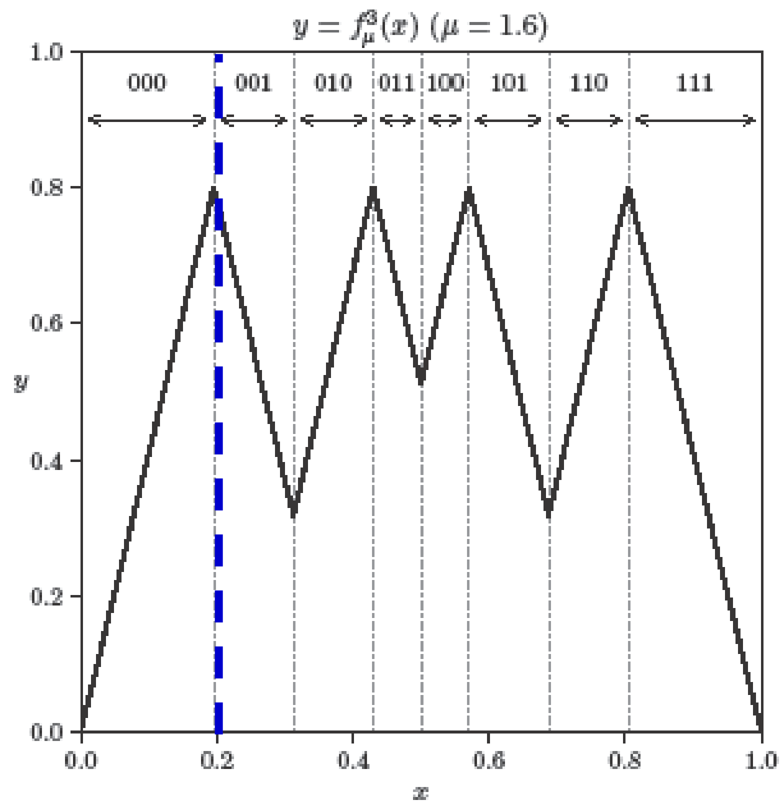
$\gamma^n(x) = b_1 b_2 \cdots b_n$ for $x \in [0,1)$ where

$$b_1 = \begin{cases} 0 & \text{if } x < \frac{1}{2} \\ 1 & \text{otherwise} \end{cases}$$

and

$$b_{i+1} = \begin{cases} b_i & \text{if } x_i < \frac{1}{2} \\ \overline{b_i} & \text{if } x_i > \frac{1}{2} \\ 1 & \text{if } x_i = \frac{1}{2} \end{cases}$$

$\gamma^3(0.2) = 001$



$y = f^3(x)$

Prop.

- $x = \sum_{i=1}^{\infty} \frac{1}{\mu_i} b_i$ (decodable)
- If $x \leq x'$ then $\gamma^n(x) \preccurlyeq \gamma^n\ (x')$ (order preserving)
- $\gamma^n(x) = \gamma^n(x+0)$ (right continuous)
- If $b_i = b_{i+1}$ then $x_i \leq \frac{1}{2}$. If $b_i \neq b_{i+1}$ then $x_i \geq \frac{1}{2}$ (left-right decision)

Tent code

$\gamma^n(x) = b_1 b_2 \cdots b_n$ for $x \in [0,1)$ where

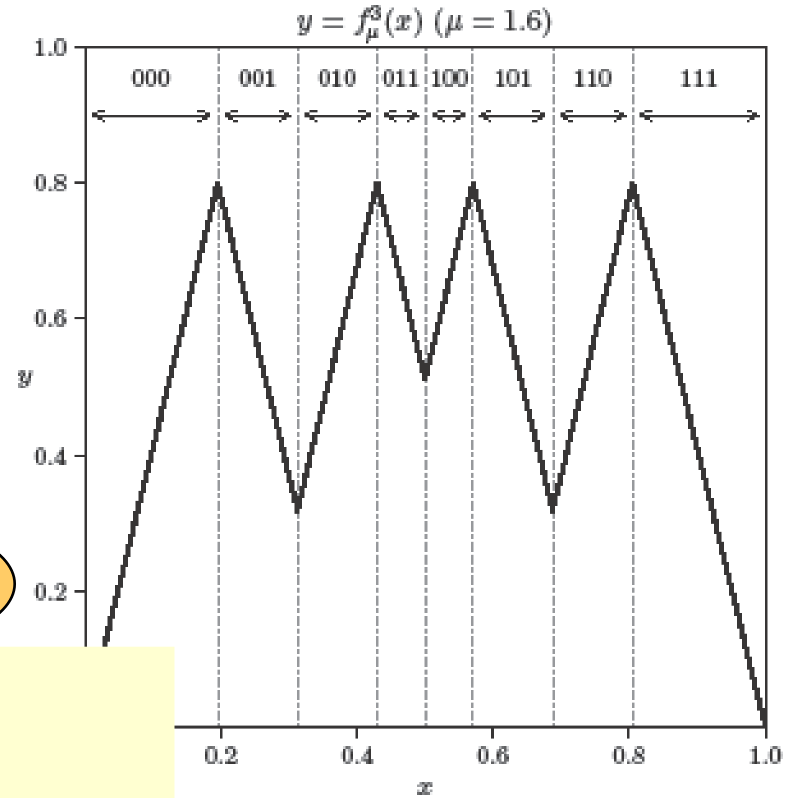
$$b_1 = \begin{cases} 0 & \text{if } x < \frac{1}{2} \\ 1 & \text{otherwise} \end{cases}$$

and

$$b_{i+1} = \begin{cases} b_i & \text{if } x_i < \frac{1}{2} \\ \overline{b_i} & \text{if } x_i > \frac{1}{2} \\ 1 & \text{if } x_i = \frac{1}{2} \end{cases}$$

$\mathcal{L}_n \subset \{0,1\}^n$

- Let
  $$\mathcal{L}_n = \{\gamma^n(x) \mid x \in (0,1)\}$$
  i.e., all possible tent codes of length n.
- We say $\boldsymbol{b} \in \{0,1\}^n$ is **valid** if $\boldsymbol{b} \in \mathcal{L}_n$.



$y = f^3(x)$

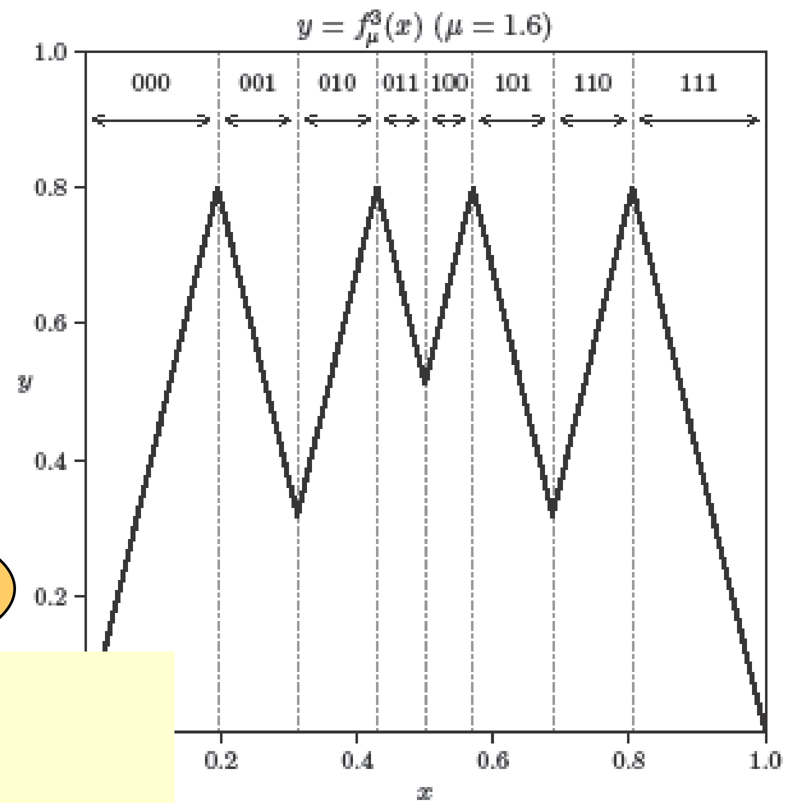
Tent code

$\gamma^n(x) = b_1 b_2 \cdots b_n$ for $x \in [0,1)$ where

$$b_1 = \begin{cases} 0 & \text{if } x < \frac{1}{2} \\ 1 & \text{otherwise} \end{cases}$$

and

$$b_{i+1} = \begin{cases} b_i & \text{if } x_i < \frac{1}{2} \\ \overline{b_i} & \text{if } x_i > \frac{1}{2} \\ 1 & \text{if } x_i = \frac{1}{2} \end{cases}$$



$y = f^3(x)$

$\mathcal{L}_n \subset \{0,1\}^n$

- Let
$$\mathcal{L}_n = \{\gamma^n(x) \mid x \in (0,1)\}$$
i.e., all possible tent codes of length n.
- We say $\boldsymbol{b} \in \{0,1\}^n$ is **valid** if $\boldsymbol{b} \in \mathcal{L}_n$.

⇒ Our main concern is the **computational complexity** to decide whether $\boldsymbol{b} \in \{0,1\}^n$ is ***valid*** or not.

Target of this work

Let $X \in [0,1)$ u.a.r., and consider $\gamma^n(X)$.

Target.

Generate $B_1 \cdots B_n = \gamma^n(X)$.

A naïve calculation requires $\Omega(n)$ space

by a standard argument of the numerical computation.

Question.

Is there $\mathbf{o}(n)$ space algorithm?

Such as

- $\mathrm{O}(\sqrt{n})$
- $\mathrm{O}(\log n)$

Main result

For convenience, let $\mathcal{D}_n$ denote the probability distribution which $\gamma^n(X)$ follows for u.a.r $X \in [0,1)$; thus

- $\mathcal{D}_n$ is a prob. distr. over $\mathcal{L}_n \subset \{0,1\}^n$, but
- $\mathcal{D}_n$ is *not* the uniform distribution over $\mathcal{L}_n$.

Question.

Is there $\mathbf{o}(\boldsymbol{n})$ space algorithm for sampling from $\mathcal{D}_n$?

Yes, we can!

Thm. 2.3.

Let $\mu \in (1,2)$ be a rational given by an irreducible fraction $\mu = c/d$.

Then, there exists an algorithm to generate *valid* $\boldsymbol{B} \sim \mathcal{D}_n$ in $\mathrm{O}\left(\frac{\log^2 n \log^3 d}{\log^4 \mu}\right)$ space in expectation.

3. Idea for a space efficient algorithm

Two strategies for sampling from $\mathcal{D}_n$.

A. Naïvely calculate $\gamma^n(X)$.

- calculation requires $\Omega(n)$ space.

B. Directly sample from $\mathcal{L}_n$, according to $\mathcal{D}_n$.

- $|\mathcal{L}_n| = \Omega(\mu^n)$, meaning that *identification* of $\boldsymbol{b} \in \mathcal{L}_n$ requires $\Omega(\log_2 \mu^n) = \Omega(n \log_2 \mu) = \Omega(n)$ space for any μ constant to n.

We employ a hybrid strategy; realize str. B by *emulating* str. A.

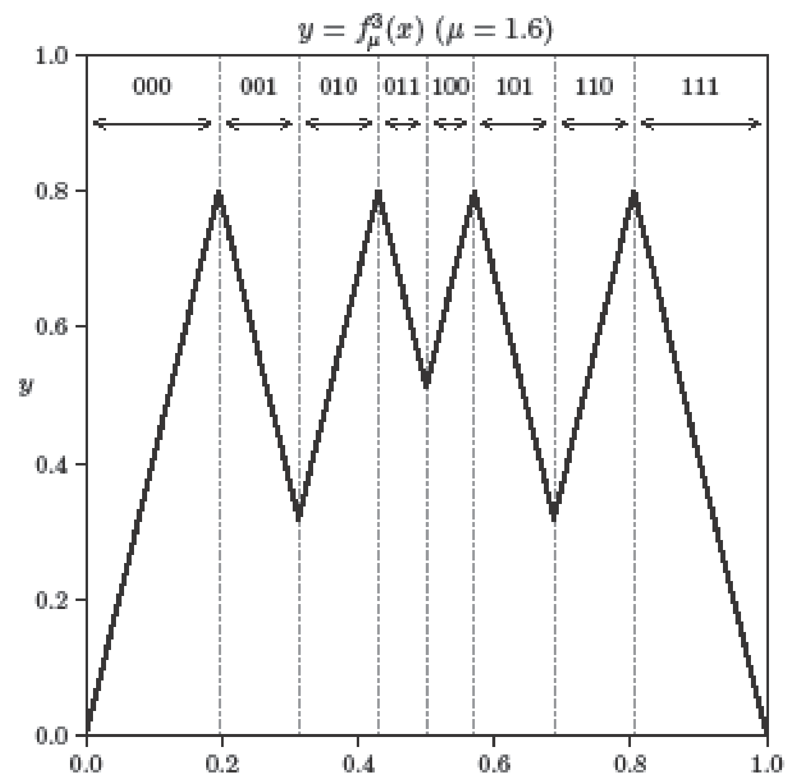
For this purpose, we want

1. a space efficient **representation** of $\boldsymbol{b} \in \mathcal{L}_n$ (for str. B).
2. a space efficient **simulation** of calculating $\gamma^n(X)$ (for str. A)

1. Equivalence class for a representation

Observation

- Iterated tent map consists of many **line-segments**.
- The line-segments correspond to $\mathcal{L}_n$ one-to-one.
- #line-segments ($= |\mathcal{L}_n|$) grows exponential to n.
- **However, some line-segments look the "same".**



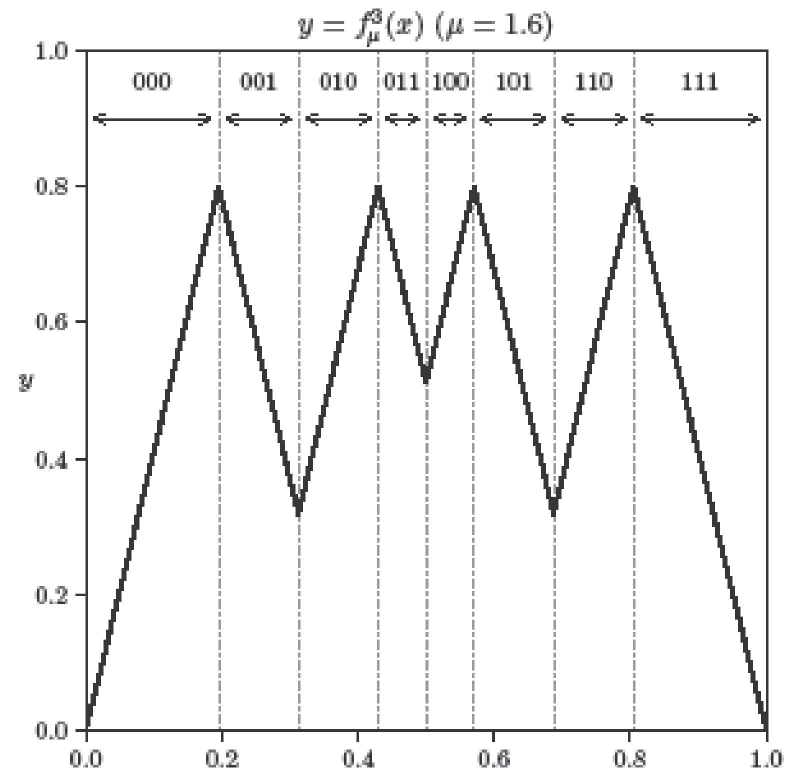
1. Equivalence class for a representation

Observation

- Iterated tent map consists of many **line-segments**.
- The line-segments correspond to $\mathcal{L}_n$ one-to-one.
- #line-segments ($= |\mathcal{L}_n|$) grows exponential to n.
- **However, some line-segments look the "same".**

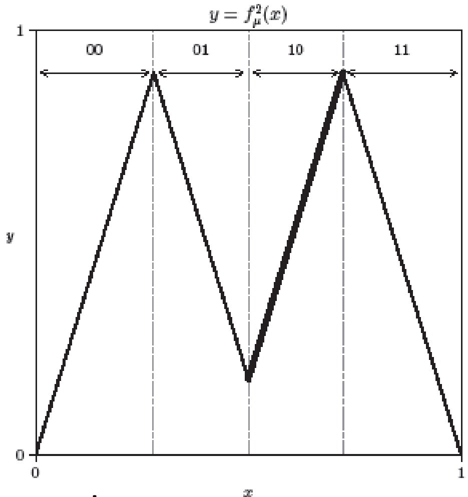
- We define the **segment-type** of the segment corresponding to $\boldsymbol{b} \in \mathcal{L}_n$ by
  $T(\boldsymbol{b}) = \{f^n(x) \mid \gamma^n(x) = \boldsymbol{b}\}$

- Let
  $\mathcal{T}_n = \{T(\boldsymbol{b}) | b \in \mathcal{L}_n\}$
  denote the all set of segment-types.



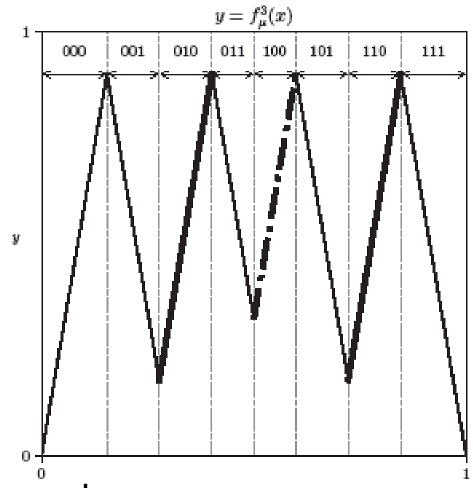
1. Equivalence class for a representation

Consider the n times iterated maps.



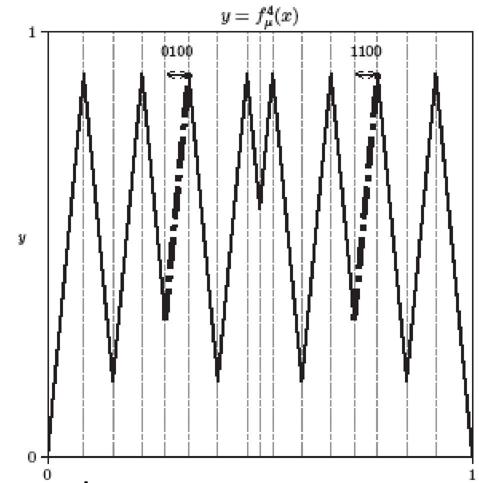
2nd iterated map

- 4 segments
- 4 segment-types



3rd iterated map

- 8 segments
- 6 segment-types



4th iterated map

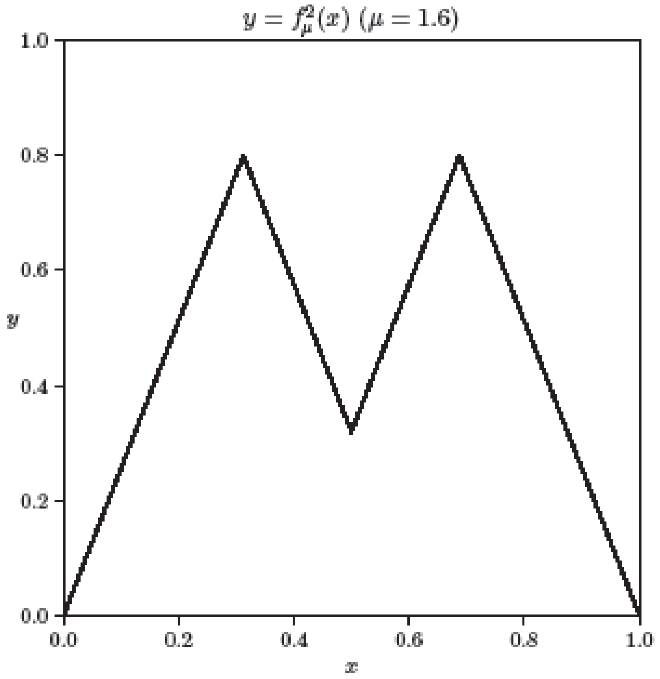
- 16 segments
- 8 segment-types

In general, we prove that n times iterated map consists of

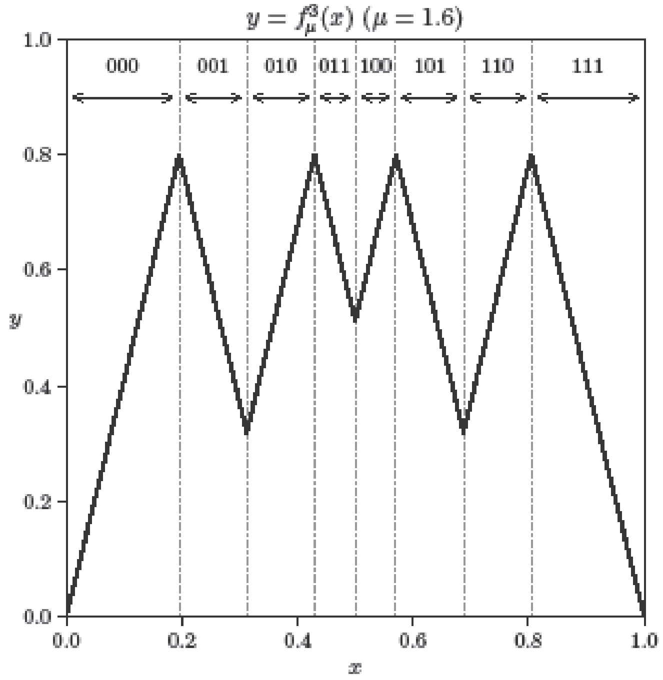
- $|\mathcal{L}_n| \geq \mu^n$ segments
- at most $2n$ segment-types

Thm. 3.1.

An intuition --- compressing lemma



$f^2(x)$

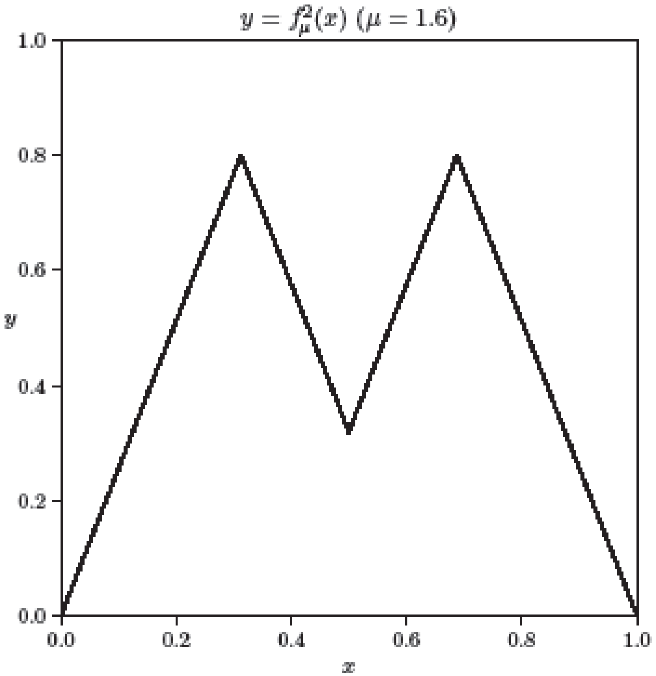


$f^3(x)$

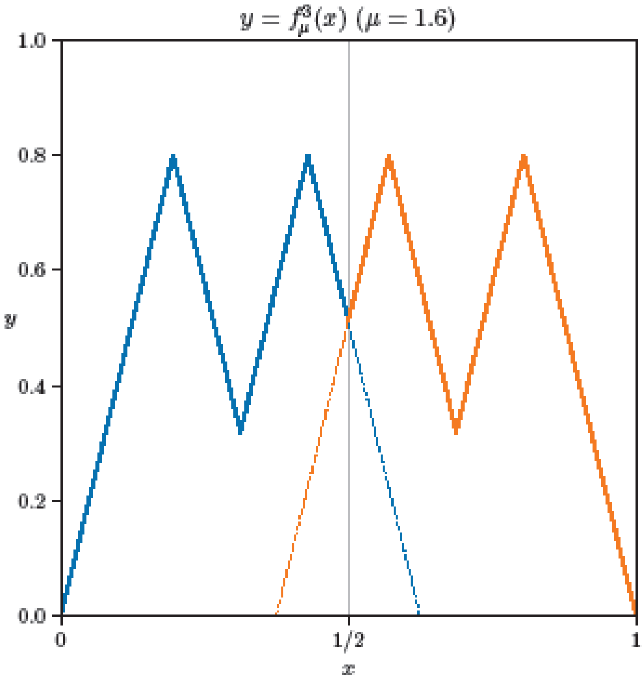
<u>Observation (cf. Lem. 3.2.)</u>

f^{n+1} consists of two f^n, each of which is compressed in $1/\mu$ in x-axis direction and cutoff at $1/2$.

An intuition --- compressing lemma



$f^2(x)$



$f^3(x)$

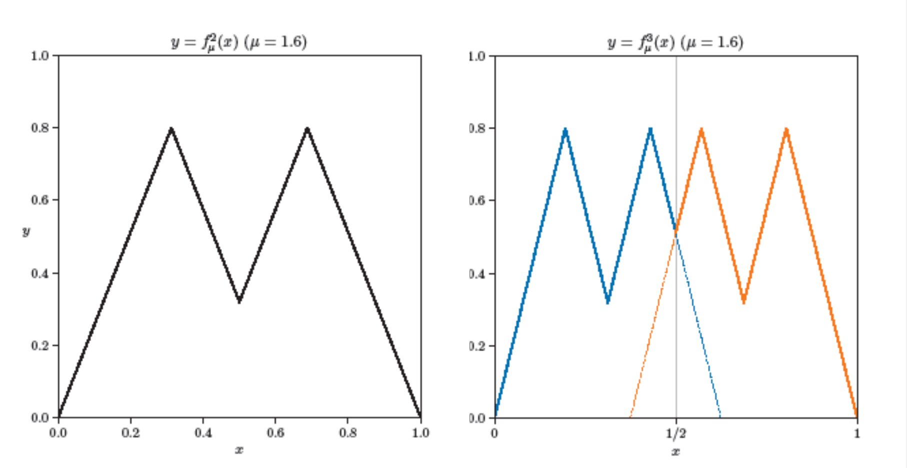
Observation (cf. Lem. 3.2.)

f^{n+1} consists of two f^n, each of which is compressed in $1/\mu$ in x-axis direction and cutoff at $1/2$.

Formal description of compressing lemma

Observation

f^{n+1} consists of two f^n, compressed in $1/\mu$ in x-axis direction and cutoff at $1/2$.



$f^2(x)$ $f^3(x)$

Lem 3.2. (compressing lemma)

Let $\tilde{f}(x) = \begin{cases} f(x) & x \leq \frac{1}{2} \\ 1 - f(x) & x \geq \frac{1}{2} \end{cases}$

then $f^{n+1}(x) = f^n\left(\tilde{f}(x)\right) = \begin{cases} f^n(\mu x) & x \leq \frac{1}{2} \\ f^n(1 - \mu(1 - x)) & x \geq \frac{1}{2} \end{cases}$

- For $x \leq \frac{1}{2}$, Lem. 3.2. implies blue line.
- For $x \geq \frac{1}{2}$, let $x = 1 - t$ ($t \leq 1/2$) then

$$\tilde{f}(x) = 1 - \mu(1 - x) = 1 - \mu\big(1 - (1 - t)\big) = 1 - \mu t.$$

This means orange line.

1. Equivalence class for a representation

Explicit explanation of $\mathcal{T}_n$

Thm. 3.1.

Let $\boldsymbol{c_i} = \gamma^i\left(\frac{1}{2}\right)$, and $\bar{\boldsymbol{c}}_{\boldsymbol{i}}$ is the bitwise complement of $\boldsymbol{c_i}$.

Let $I_i = T(\boldsymbol{c_i})$ and $\bar{I}_i = T(\bar{\boldsymbol{c}}_{\boldsymbol{i}})$ for $i = 1,2, \ldots$.

Then,

$$\mathcal{T}_n = \{I_1, I_2, \ldots, I_{n^*}\} \cup \{\bar{I}_1, \bar{I}_2, \ldots, \bar{I}_{n^*}\}$$

holds for any $n \geq 1$, w/ some appropriate n^* ($n^* \leq n$).

In precise, $n_* = \min(\{i \in \{1,2,\ldots,n-1\} \,|\, I_{i+1} \in \mathcal{T}_I\} \cup \{n\})$.

Thm. 3.1. immediately implies $|\mathcal{T}_n| = 2n^*$ $(\leq 2n)$.

$\Rightarrow$ We obtain an equivalent class on $\mathcal{L}_n$ of size $O(n)$.

An example of the set of segment-types

$\mathcal{T}_5$ for $\mu = 1.6$

$\boxed{\bar{I}_1 = [0,0.8)}$ $\boxed{I_1 = (0,0.8]}$

$\boxed{\bar{I}_2 = (0.32,0.8]}$ $\boxed{I_2 = [0.32,0.8)}$

$\boxed{\bar{I}_3 = (0.512,0.8]}$ $\boxed{I_3 = [0.512,0.8)}$

$\boxed{\bar{I}_4 = [0.32,0.7808)}$ $\boxed{I_4 = (0.32,0.7808]}$

$\boxed{\bar{I}_5 = (0.35072,0.8]}$ $\boxed{I_5 = [0.35072,0.8)}$

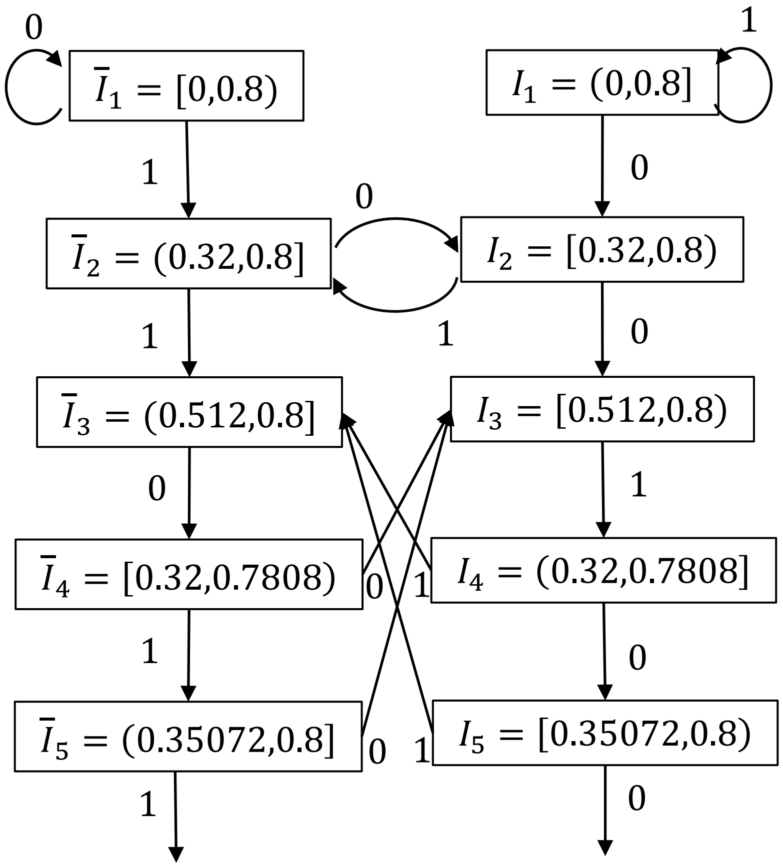
2. Space efficient simulation for a calculation of $\gamma^n(X)$

$\mathcal{T}_5$ for $\mu = 1.6$

$\bar{I}_1 = [0,0.8)$	$I_1 = (0,0.8]$
$\bar{I}_2 = (0.32,0.8]$	$I_2 = [0.32,0.8)$
$\bar{I}_3 = (0.512,0.8]$	$I_3 = [0.512,0.8)$
$\bar{I}_4 = [0.32,0.7808)$	$I_4 = (0.32,0.7808]$
$\bar{I}_5 = (0.35072,0.8]$	$I_5 = [0.35072,0.8)$

2. Space efficient simulation for a calculation of $\gamma^n(X)$

State transition over $\mathcal{T}_5$ for $\mu = 1.6$



2. Space efficient simulation for a calculation of $\gamma^n(X)$

Lem. 3.3.

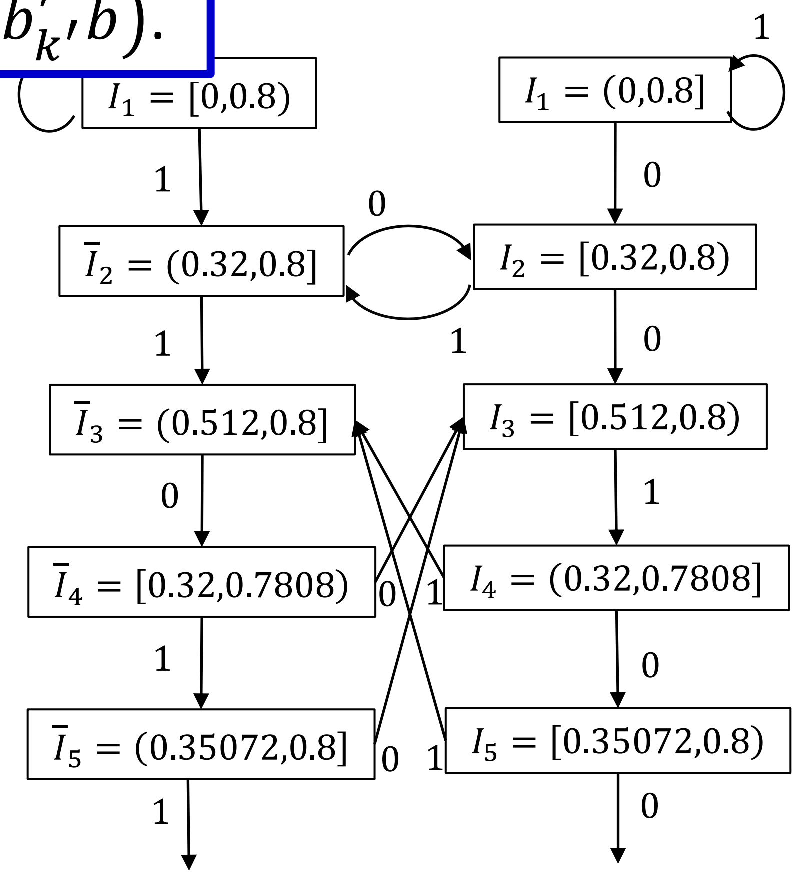
Suppose $T(b_1 \cdots b_k) = T(b'_1 \cdots b'_{k'})$.

Then, $b_1 \cdots b_k b$ is valid iff $b'_1 \cdots b'_{k'} b$ is valid.

Furthermore, $T(b_1 \cdots b_k b) = T(b'_1 \cdots b'_{k'} b)$.

te transition over

for $\mu = 1.6$



2. Space efficient simulation for a calculation of $\gamma^n(X)$

te transition over

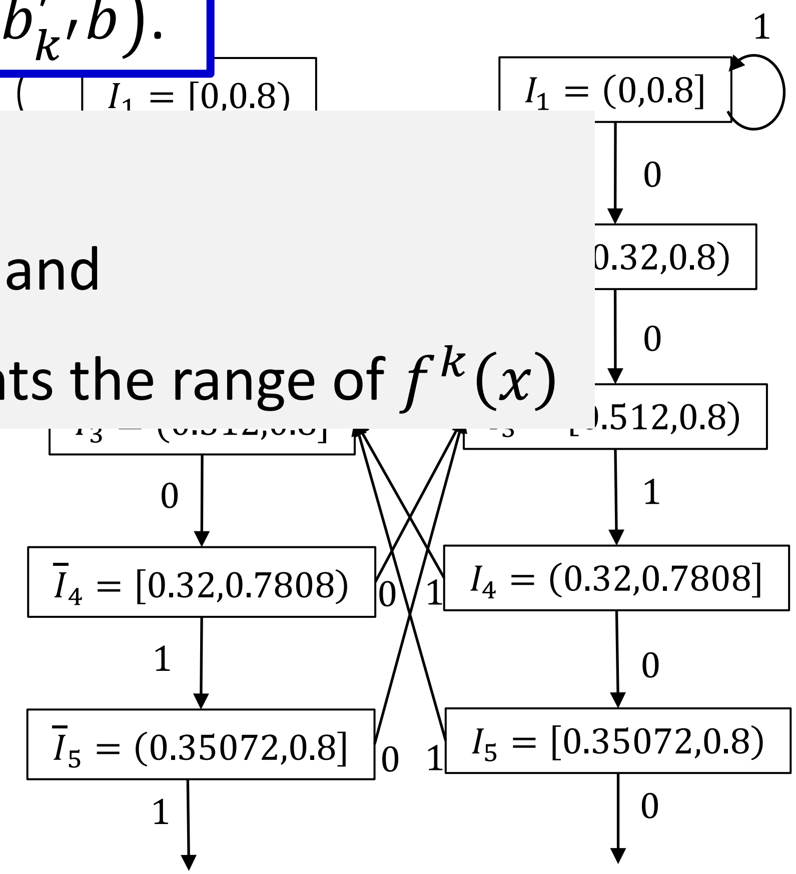
for $\mu = 1.6$

Lem. 3.3.

Suppose $T(b_1 \cdots b_k) = T(b_1' \cdots b_{k'}')$.

Then, $b_1 \cdots b_k b$ is valid iff $b_1' \cdots b_{k'}' b$ is valid.

Furthermore, $T(b_1 \cdots b_k b) = T(b_1' \cdots b_{k'}' b)$.



An intuitive "proof".

- $k + 1^{\text{st}}$ bit depends on $f^k(x) < \frac{1}{2}$, and
- Segment-type $T(b_1 \cdots b_k)$ represents the range of $f^k(x)$

2. Space efficient simulation for a calculation of $\gamma^n(X)$

Lem. 3.3.

Suppose $T(b_1 \cdots b_k) = T\left(b_1' \cdots b_{k'}'\right)$.

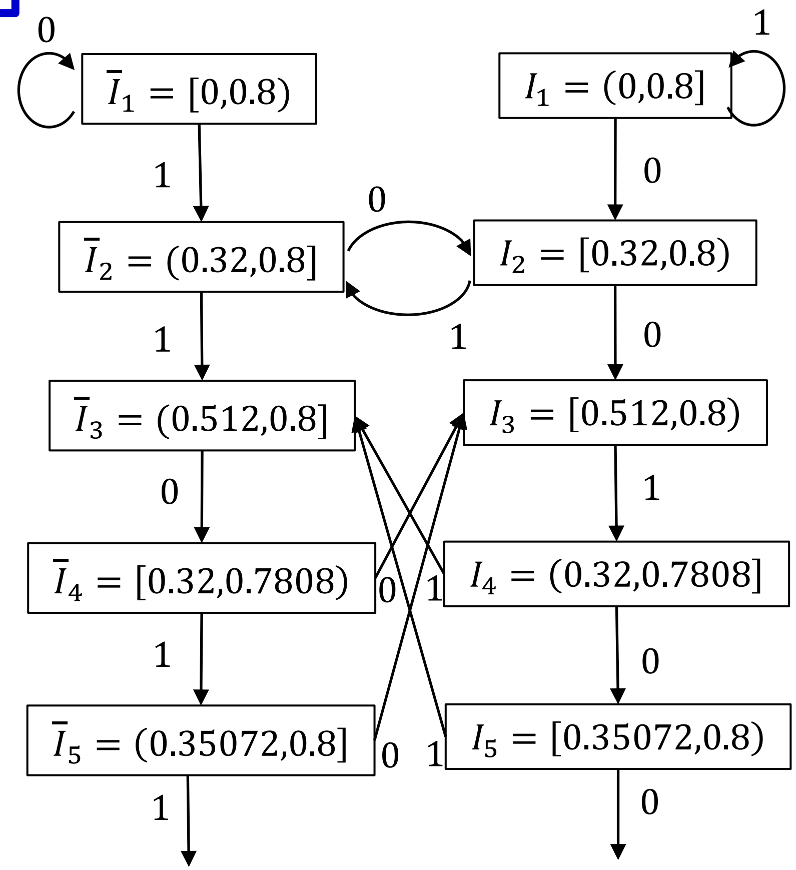
Then, $b_1 \cdots b_k b$ is valid iff $b_1' \cdots b_{k'}' b$ is valid.

Furthermore, $T(b_1 \cdots b_k b) = T\left(b_1' \cdots b_{k'}' b\right)$.

State transition over $\mathcal{T}_5$ for $\mu = 1.6$

Lem 3.3 implies **state transitions** over the equivalence classes $\mathcal{T}_n$.

This provides an automaton for $\mathcal{L}_n$.



Automaton

Lem. 3.3.

Suppose $T(b_1 \cdots b_k) = T\left(b_1' \cdots b_{k'}'\right)$.

Then, $b_1 \cdots b_k b$ is valid iff $b_1' \cdots b_{k'}' b$ is valid.

Furthermore, $T(b_1 \cdots b_k b) = T\left(b_1' \cdots b_{k'}' b\right)$.

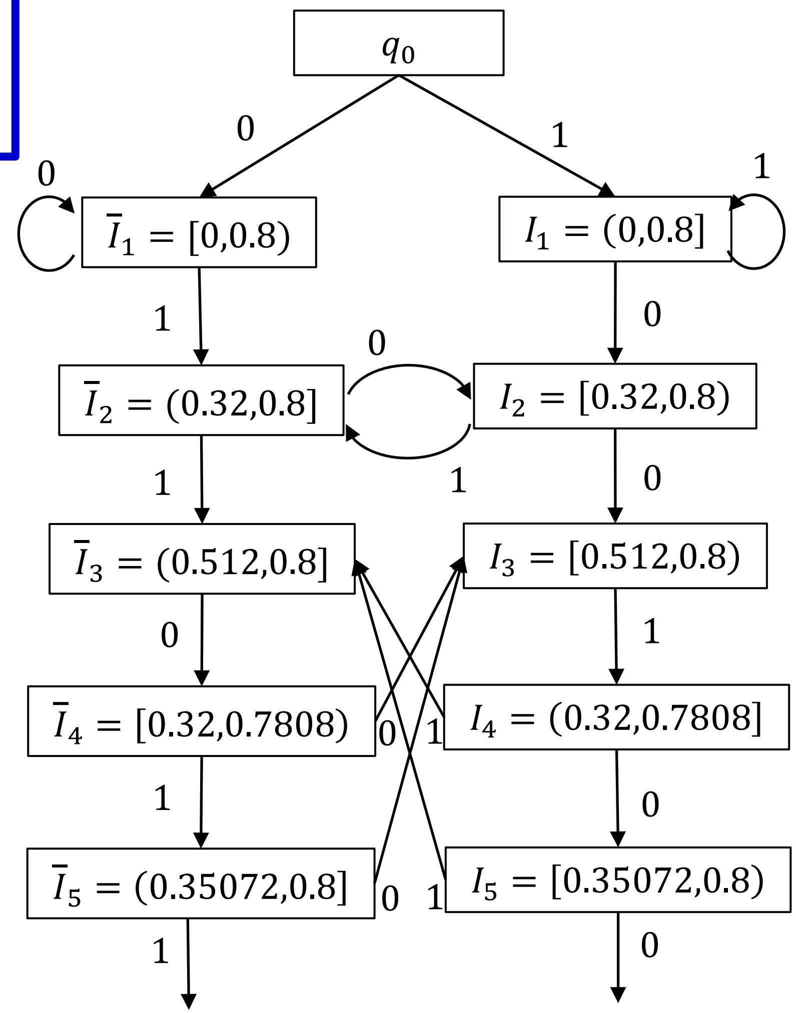
Lem 3.3 implies **state transitions** over the equivalence classes $\mathcal{T}_n$.

This provides an automaton for $\mathcal{L}_n$.

The automaton

- consists of $2n + 2$ states
  incl. q_0 and "reject" state.
- and recognizes $\mathcal{L}_n$ ***exactly***.

Automaton over $\mathcal{T}_5$ for $\mu = 1.6$



Markov model (probabilistic automaton)

Furthermore, the state transit model preserves the uniform measure.

Lem.

Let $B_1 \cdots B_n = \gamma^n(X)$ for u.a.r. $X \in (0,1)$. Then,

$$\Pr[B_n = 0 \mid \boldsymbol{B_{n-1}} = \boldsymbol{b}] = \frac{|T(\boldsymbol{b}0)|}{|T(\boldsymbol{b}0)| + |T(\boldsymbol{b}1)|}$$

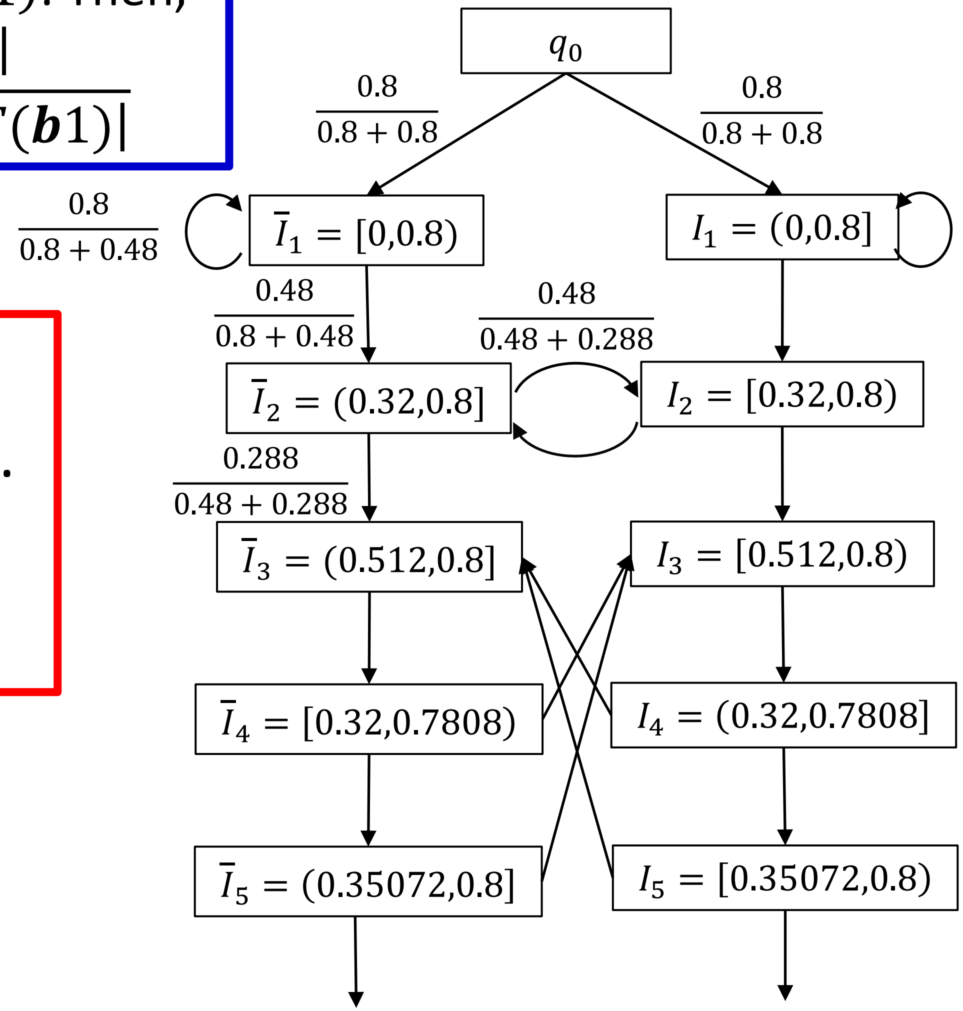
Thm. 3.5.

Suppose $\boldsymbol{B} = B_1 \cdots B_n$ is a bit seq. provided by the Markov model.

Then $\boldsymbol{B} \sim \mathcal{D}_n$.

Thus, we obtain an algorithm to generate $\boldsymbol{B} \sim \mathcal{D}_n$.

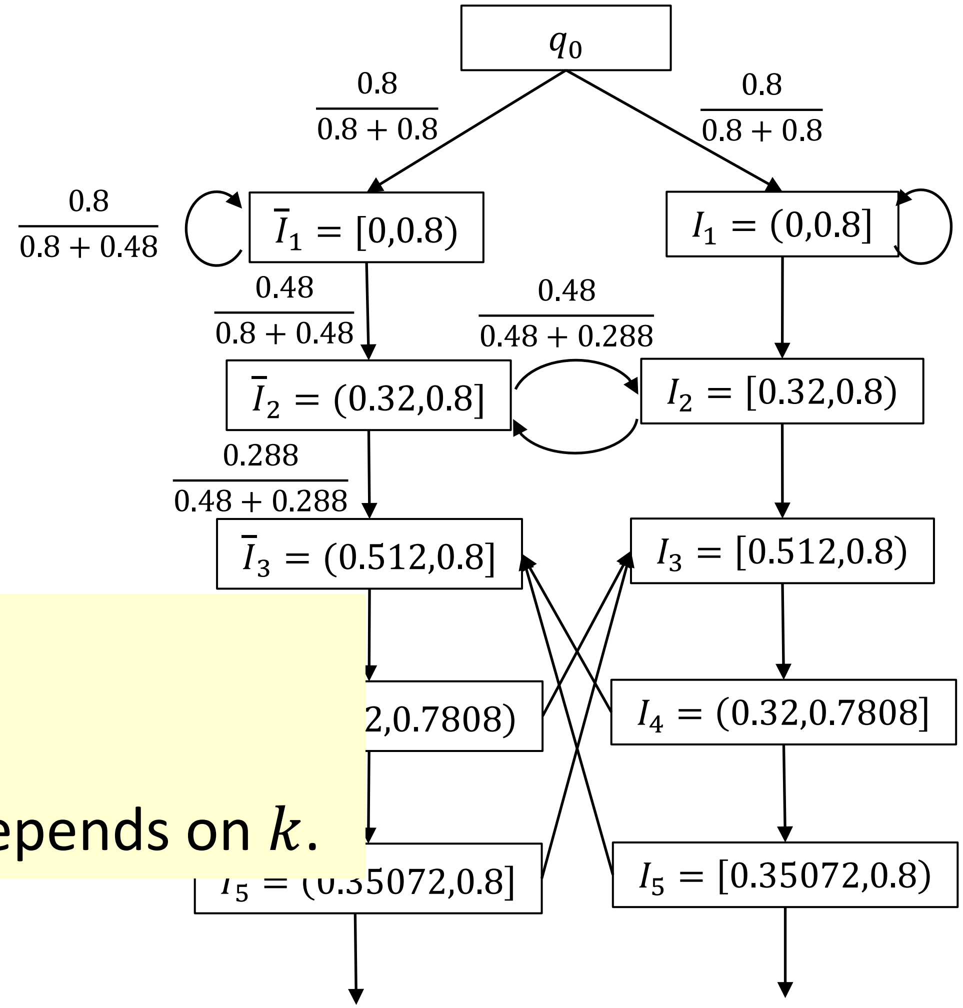
Markov model over $\mathcal{T}_5$ for $\mu = 1.6$



Space efficient algorithm to generate $B \sim \mathcal{D}_n$

Alg. (construct on demand)

1. Construct the Markov model up to level $k = \lceil \log n \rceil$.
2. For $i = 1$ to n
3. Generate B_i following the Markov model over $\mathcal{T}_k$.
4. If the current state is level k
5. then extend the model to level $k+1$.



Prop.

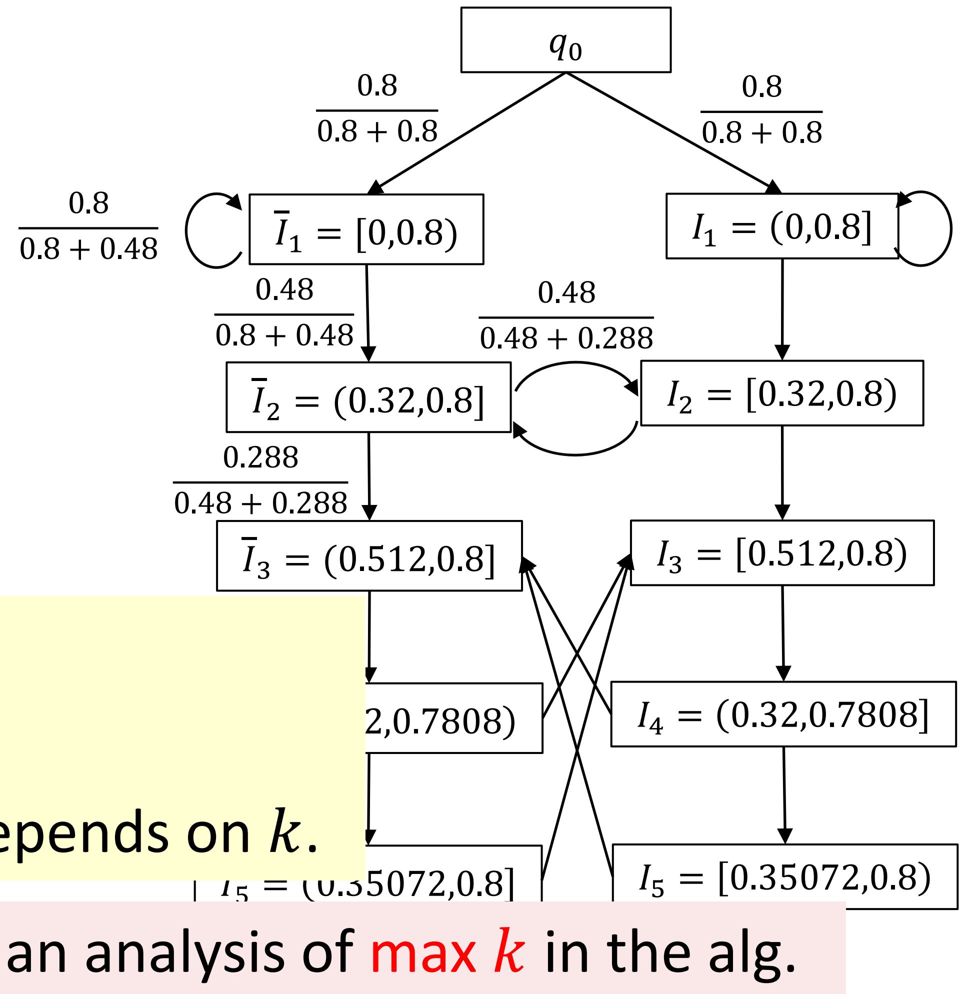
Alg. exactly generates $\boldsymbol{B} \sim \mathcal{D}_n$.

The space complexity mainly depends on k.

Space efficient algorithm to generate $B \sim \mathcal{D}_n$

Alg. (construct on demand)

1. Construct the Markov model up to level $k = \lceil \log n \rceil$.
2. For $i = 1$ to n
3. Generate B_i following the Markov model over $\mathcal{T}_k$.
4. If the current state is level k
5. then extend the model to level $k + 1$.



Prop.

Alg. exactly generates $\boldsymbol{B} \sim \mathcal{D}_n$.

The space complexity mainly depends on k.

⇨ The remaining issue is an analysis of max k in the alg.

4. Analysis of max k

Expected level

Let $K \in \{1, \dots, n\}$ be a random variable denoting the maximum level that $\gamma^n(X)$ reaches.

Lem. 4.1'. (rational μ)

Let $\mu = \frac{c}{d} \in (1,2)$ where $\gcd(c, d) = 1$.

Then, $\mathrm{E}[K] = O\left(\log_\mu n \log_\mu d\right)$

Cf. Prop. (real μ)

For any $\mu \in (1,2)$

$$\mathrm{E}[K] \le \max\left\{32 \log_\mu n \log_2 \log_\mu n \,, 4 \log_\mu \frac{2}{\mu - 1}\right\}$$

Expected level

Let $K \in \{1, \dots, n\}$ be a random variable
denoting the maximum level that $\gamma^n(X)$ reaches.

Lem.

The expected space complexity of Alg. is $\mathrm{O}(\mathrm{E}[K^2])$

Lem. 4.1. (rational μ)

Let $\mu = \frac{c}{d} \in (1,2)$ where $\gcd(c,d) = 1$.

Then, $\mathrm{E}[K^2] = \mathrm{O}\left(\frac{\log^2 n \log^2 d}{\log^4 \mu}\right)$

Thm. 2.3.

Let $\mu \in (1,2)$ be a rational given by an irreducible fraction $\mu = c/d$.

Then, there exists an algorithm to generate *valid* $\boldsymbol{B} \sim \mathcal{D}_n$

in $\mathrm{O}\left(\frac{\log^2 n \log^3 d}{\log^4 \mu}\right)$ space in expectation.

Proof sketch of Lem 4.1.

> Lem. 4.1. (rational μ)
>
> Let $\mu = \frac{c}{d} \in (1,2)$ where $\gcd(c, d) = 1$.
>
> Then, $\mathrm{E}[K^2] = \mathrm{O}\left(\frac{\log^2 n \log^2 d}{\log^4 \mu}\right)$

Let $l_* = 8\lceil \log_\mu d \rceil \lceil \log_\mu n \rceil$. Then,

$$\begin{aligned}
E[Z] &= \sum_{k=1}^{n} k^2 \Pr[K = k] \\
&= \sum_{k=1}^{2l_*-1} k^2 \Pr[K = k] + \sum_{k=2l_*}^{n} k \Pr[K = k] \\
&\leq (2l_* - 1)^2 \Pr[K \leq 2l_* - 1] + n^2 \Pr[K \geq 2l_*] \qquad (*)
\end{aligned}$$

We can prove that $\Pr[k \geq 2l_*] \leq \frac{1}{n^2}$ holds (see Lem 4.2), and hence

$$\begin{aligned}
(*) &\leq (2l_* - 1)^2 * 1 + n^2 \frac{1}{n^2} \\
&= (2l_* - 1)^2 + 1 \\
&\leq \left(16\lceil \log_\mu d \rceil \lceil \log_\mu n \rceil - 1\right)^2 + 1 \\
&= \mathrm{O}\left(\left(\log_\mu d \log_\mu n\right)^2\right) \\
&= \mathrm{O}\left(\frac{\log^2 n \log^2 d}{\log^4 \mu}\right)
\end{aligned}$$

> Lem. 4.2.
>
> Let $l_* = 8\lceil \log_\mu d \rceil \lceil \log_\mu n \rceil$.
>
> Then, $\Pr[k \geq 2l_*] \leq \frac{1}{n^2}$

Sketch of Proof of Lem 4.2.

Lem. 4.2.

Let $l_* = 8\lceil \log_\mu d \rceil \lceil \log_\mu n \rceil$. Then, $\Pr[k \geq 2l_*] \leq \frac{1}{n^2}$.

Proof of Lem. 4.2 requires more than 6 pages (see arXiv).

The following two lemmas show the outline.

Lem. 4.3.

If Z_t visits I_{2j} (resp. $\bar{I}_{2j}$) for the first time

then $Z_{t-i} = I_{2j-i}$ (resp. $Z_{t-i} = \bar{I}_{2j-i}$) for $i = 1,2, \ldots, j$.

Lem. 4.4.

$\exists l \leq 8\lceil \log_\mu d \rceil \lceil \log_\mu n \rceil$ such that

$$\Pr[L(Z_t) = 2l \,|L(Z_{t-l} = l)] \leq \frac{1}{n^3}$$

Main result (again)

For convenience, let $\mathcal{D}_n$ denote the probability distribution which $\gamma^n(X)$ follows for u.a.r $X \in [0,1)$; thus

- $\mathcal{D}_n$ is a prob. distr. over $\mathcal{L}_n \subset \{0,1\}^n$, but
- $\mathcal{D}_n$ is *not* the uniform distribution over $\mathcal{L}_n$.

Question.

Is there $\mathbf{o}(\boldsymbol{n})$ space algorithm for sampling from $\mathcal{D}_n$?

Yes, we can!

Thm. 2.3.

Let $\mu \in (1,2)$ be a rational given by an irreducible fraction $\mu = c/d$.

Then, there exists an algorithm to generate *valid* $\boldsymbol{B} \sim \mathcal{D}_n$ in $\mathrm{O}\left(\frac{\log^2 n \log^3 d}{\log^4 \mu}\right)$ space in expectation.

5. Concluding Remarks

Concluding Remarks

Result summary

- We gave an algorithm to generate $\boldsymbol{B} \sim \mathcal{D}_n$, which works in $\mathrm{O}(\log^2 n)$ expected space.
  - β-expansion is essentially the same.

Further discussion

- This result implies the computational complexity to decide "whether $\boldsymbol{b} \in \{0,1\}^n$ is valid" is in $\mathrm{O}(\log^2 n)$ space, *in average*.
- We can extend the result from an average to a *smoothed analysis*.
  - See our arXiv paper about it.

Future work

- ☐ Extension to logistic map.
- ☐ Extension to 2D chaotic map, e.g., Baker's map.

Concluding Remarks

Result summary

- We gave an algorithm to generate $\boldsymbol{B} \sim \mathcal{D}_n$, which works in $\mathrm{O}(\log^2 n)$ expected space.
  - β-expansion is essentially the same.

Further discussion

- This result implies the computational complexity to decide "whether $\boldsymbol{b} \in \{0,1\}^n$ is valid" is in $\mathrm{O}(\log^2 n)$ space, *in average*.
- We can extend the result from an average to a *smoothed analysis*.
  - See our arXiv paper about it.

Future work

- ☐ Extension to logistic map.
- ☐ Extension to 2D chaotic map, e.g., Baker's map.

Fin.

The end

Thank you for the attention.