

カオスの計算量

岡田真明, *来嶋秀治

[1] Naoaki Okada and Shuji Kijima, The space complexity of generating tent codes, arXiv:2310.14185, 2023.

[2] Naoaki Okada and Shuji Kijima, A smoothed analysis of the space complexity of computing a chaotic sequence, arXiv:2405.00327, 2024.

プロローグ

線形計画

$$\text{Max. } c_1x_1 + \cdots + c_nx_n$$

$$\text{S.t. } a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1$$

$$\vdots$$

$$a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m$$

$$x_1, \dots, x_n \geq 0$$

定理 [Khachiyan 1979; Fulkerson Prize 1982]

線形計画は多項式時間で解ける.



演習

定理 [Spielman and Teng 2004; Gödel Prize 2008]

単体法はsmoothed analysisの意味で多項式時間.

本講義は、区分線形関数の計算量に関する新しい研究を紹介

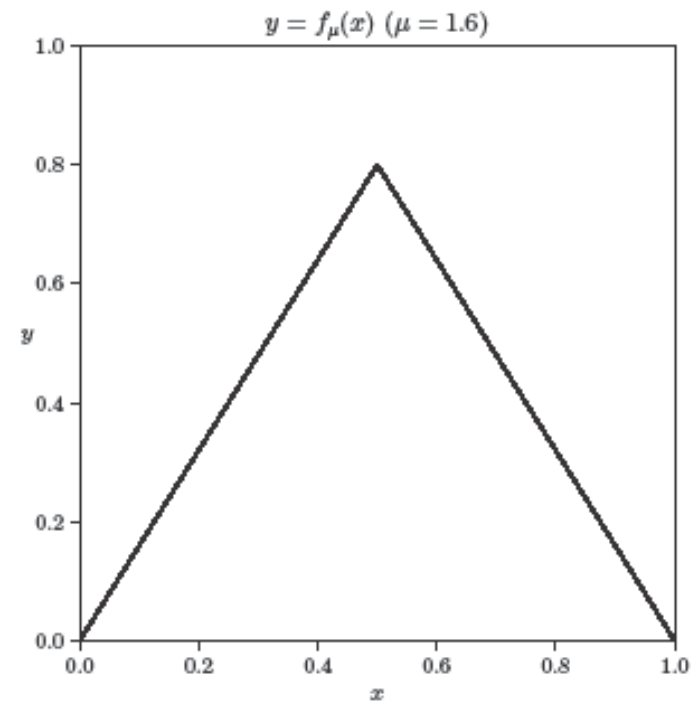
1.1. テント写像とカオス

テント写像

- **テント写像** $f: [0,1] \rightarrow [0,1]$

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

ただし $1 < \mu < 2$ はパラメータ.



$$y = f(x)$$

テント写像

- **テント写像** $f: [0,1] \rightarrow [0,1]$

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

ただし $1 < \mu < 2$ はパラメータ.

- **軌道** $x_0, x_1, x_2, \dots$

$$x_n = f(x_{n-1}) = f^n(x)$$

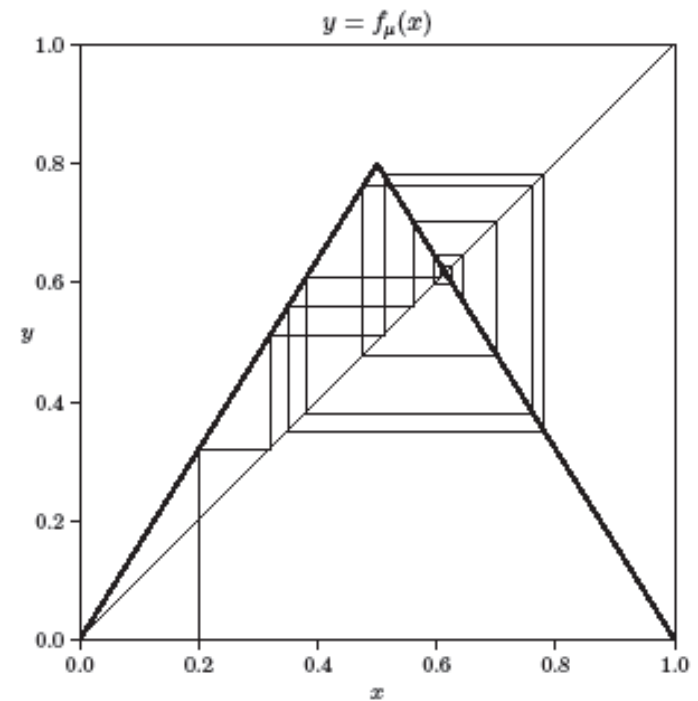
ただし $x_0 = x \in [0,1)$ とする.

⇒ **軌道の挙動はとても「複雑」**

本研究では n が与えられた時に

「 $x_n \leq \frac{1}{2}$ か, 否か」

の**計算量**について考える.

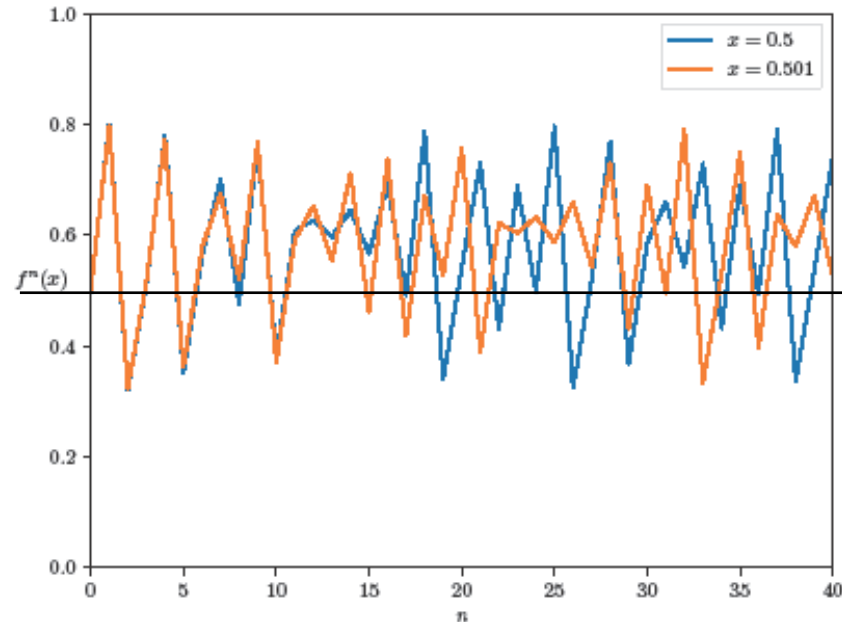


蜘蛛の巣図 (cobweb)

カオス

- 軌道 $x_0, x_1, x_2, \dots$ は**カオス**
 - ✓ 初期値鋭敏性
- テント写像にはいろいろな研究
 - ✓ 疑似乱数、信号（AD変換）
- **計算量**についての研究は皆無？

「入力 n と x に対して $x_n \leq \frac{1}{2}$ の判定」 (**NP困難?** : 未解決).



この話では、関連問題の**領域計算量**論じる.

カオス理論

□ トピック

- ◆ フラクタル
- ◆ セルオートマトン
 - 自己組織化/人工生命
- ◆ アトラクタ/力学系
 - バタフライ効果
 - 分岐
- ◆ 複雑系/複雑ネットワーク

□ 応用

- ◆ 気象予測, 海流や潮汐の変動, 地震学
- ◆ カオス通信, カオス回路
- ◆ 神経回路, 生体システム

計算の対象

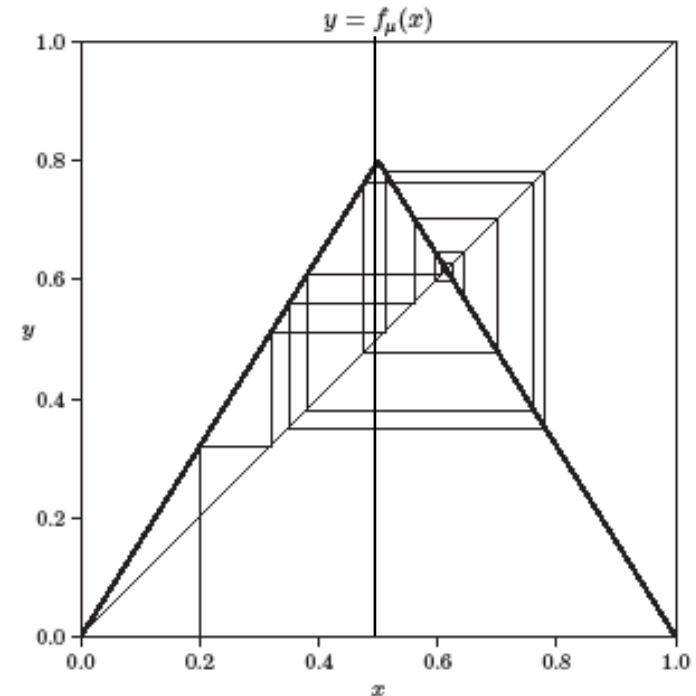
1.2. テント符号

テント符号

テント符号 $\gamma^n(x) = b_1 b_2 \cdots b_n$ ($x \in [0,1)$)

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

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



cobweb

命題

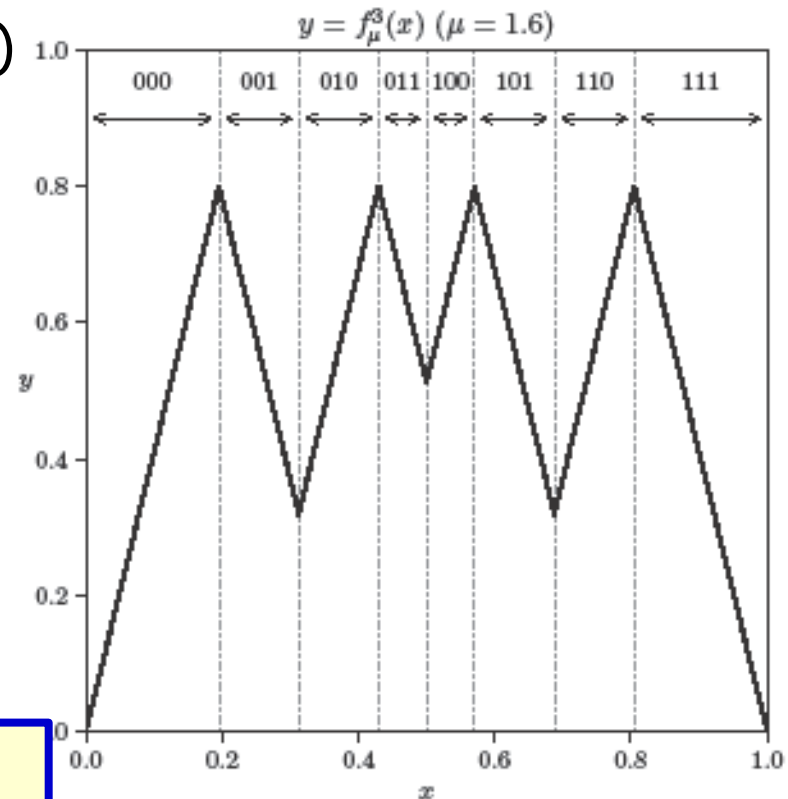
- $x = \sum_{i=1}^{\infty} \frac{1}{\mu_i} b_i$ (復号可能性)
- $x \leq x'$ ならば $\gamma^n(x) \leq \gamma^n(x')$ (順序保存)
- $\gamma^n(x) = \gamma^n(x + 0)$ (右連続)
- $b_i = b_{i+1}$ ならば $x_i \leq \frac{1}{2}$, $b_i \neq b_{i+1}$ ならば $x_i \geq \frac{1}{2}$

テント符号

テント符号 $\gamma^n(x) = b_1 b_2 \cdots b_n$ ($x \in [0,1)$)

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

$$b_{i+1} = \begin{cases} b_i & x_i < \frac{1}{2} \\ \bar{b}_i & x_i > \frac{1}{2} \\ 1 & x_i = \frac{1}{2} \end{cases}$$



$$y = f^3(x)$$

- 長さ n のテント言語 $\mathcal{L}_n \subset \{0,1\}^n$
 $\mathcal{L}_n = \mathcal{L}_n(\mu) = \{\gamma^n(x) \mid x \in (0,1)\}$
 i.e., 長さ n のテント符号全体の集合.
- テント言語 $\mathcal{L} \subset \{0,1\}^*$
 $\mathcal{L} = \mathcal{L}(\mu) = \bigcup_{n=1}^{\infty} \mathcal{L}_n(\mu)$
- $\mathbf{b} \in \mathcal{L}$ のとき, $\mathbf{b}$ は **valid** という.

本研究の目標：

「 $\mathbf{b} \in \{0,1\}^n$ が **valid** か否か」
の計算量

テント符号の計算量

定義通りの計算は $\Theta(n)$ 時間, 領域

問い

テント符号を $o(n)$ 領域で計算可能か？

たとえば

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

1.3. BAD EXAMPLE

普通のアルゴリズム $\mathcal{A}$

Input $x \in [0,1]$

Output $\gamma^n(x)$ の近似

$\kappa \leftarrow$ 適切な桁数

$z \leftarrow \langle x \rangle_\kappa$

$b \leftarrow 0$

For $i = 1$ to n

 If $b = 0$

 If $z < 1/2$ then $b \leftarrow 0$, else $b \leftarrow 1$

 Else

 If $z \geq 1/2$ then $b \leftarrow 0$, else $b \leftarrow 1$

 Return b

$z \leftarrow \langle f(z) \rangle_\kappa$

$\langle x \rangle_\kappa$: x を κ 桁に丸めたもの
e.g., float

デント符号 $\gamma^n(x) = b_1 b_2 \cdots b_n$ ($x \in [0,1)$)

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

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

命題

普通のアルゴリズムは $\mathbf{b} \notin \mathcal{L}$ を出力しうる.

命題の証明

$1.62 \geq \frac{1+\sqrt{5}}{2} \simeq 1.61803$: 黄金比
 ➤ 黄金比は $\mu^2 - \mu - 1 = 0$ の根

- $\mu = 1.62$ とする.
- $\langle z \rangle_8 = \frac{\lfloor 2^8 z \rfloor}{2^8}$: 有効桁数8ビットで計算すると
 - $\mathcal{A}\left(\frac{1}{2}\right) = 100\ 011\ 011\ 011\ 0\mathbf{0} \notin \mathcal{L}(1.62)$
- $\langle z \rangle = \frac{\lfloor 1000z \rfloor}{1000}$: 有効桁数3桁で計算すると
 - $\mathcal{A}\left(\frac{1}{2}\right) = 100\ 011\ 011\ 011\ 01\mathbf{0} \notin \mathcal{L}(1.62)$

ちなみに, 真値は

$$\gamma_\mu^{15}\left(\frac{1}{2}\right) = 100\ 011\ 011\ 011\ 0\mathbf{11} \dots$$

本研究の動機（私のやりたいこと）

- **カオスの応用例**：気象予測、海流や潮汐の変動、地震学
 - 数値シミュレーションの結果は正しいのか？

by chat GPT

**つまり、丸め誤差は「物理」的には
起こりえない軌道（キメラ）を出力しうる。**

- **解決策**：計算機パワーを上げて、精度をよくする！
- **アルゴリズム屋(=私)の視点**：
 - 「精度を上げる！」の前に、ほかに計算方法ないの？
⇒（テント言語という、ちっぽけな例だけど）**あるよ！**

本講義のねらい

- 数値計算の計算量解析技術を学ぶ^{*1}
- 言語とオートマトンを学ぶ^{*2}
- 非自明なアルゴリズムの設計技法について学ぶ
- アルゴリズムの確率的解析を学ぶ
- 新規研究課題の開拓について学ぶ

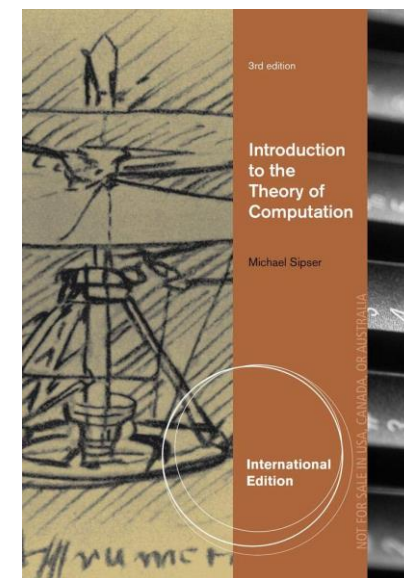
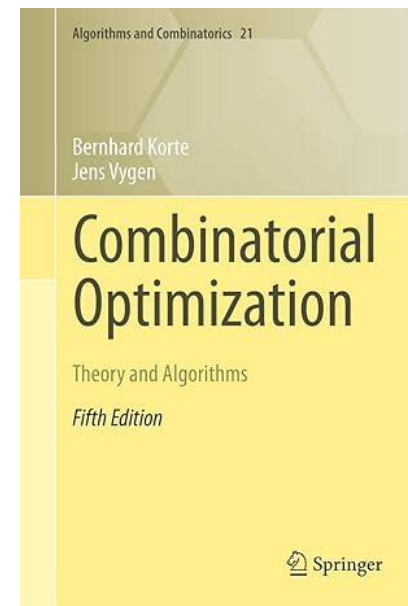
[参考図書]

*1 Bernhard Korte and Jens Vygen, Combinatorial Optimization: Theory and Algorithms, 6th ed., Springer, 2018.

線形計画の多項式時間解法（楕円体法）

*2 Michael Sipser, Introduction to the theory of computation, 3rd ed., Cengage Learning, 2012.

言語とオートマトン



1.4. 問題と定理

計算機科学としての問題

問題1 (Recognition)

入力: ビット列 $\mathbf{b} \in \{0,1\}^n$.

質問: $\mathbf{b} \in \mathcal{L}$?

問題2 (判定問題)

入力: ビット列 $\mathbf{b}_n \in \{0,1\}^n$ と実数 $x \in [0,1)$.

質問: $\mathbf{b}_n = \gamma^n(x)$?

問題3 (計算問題)

入力: 実数 $x \in [0,1)$ と正整数 n .

質問: $\gamma^n(x)$ を求めよ.

問題1への回答: Average case analysis

問題1 (Recognition)

入力: ビット列 $\mathbf{b} \in \{0,1\}^n$.

質問: $\mathbf{b} \in \mathcal{L}$?

定理 1 (Recognition; 平均時解析)

$\mu = \frac{c}{d} \in (1,2)$ は既約分数とする.

ビット列 $\mathbf{b} \in \{0,1\}^n$ が与えられたとき, $\mathbf{b} \in \mathcal{L}$ を判定可能.

入力 $\mathbf{b}$ が $\mathcal{D}_n$ に従うとき, 期待領域計算量は $O\left(\frac{\log^2 n \log d}{\log^2 \mu}\right)$.

ただし, $\mathcal{D}_n: X \in [0,1]$ を一様として, $\gamma^n(X)$ の従う分布.

μ が実数の場合も同様の事実が得られる (後述) .

問題2への回答: Smoothed analysis

問題2 (判定問題)

入力: ビット列 $\mathbf{b}_n \in \{0,1\}^n$ と実数 $x \in [0,1)$.

質問: $\mathbf{b}_n = \gamma^n(x)$?

近似解法

$$\begin{aligned}\mathcal{L}_n(x, \epsilon) &= \{\gamma^n(x') \mid x - \epsilon \leq x' \leq x + \epsilon\} \\ &= \{\mathbf{b}_n \in \mathcal{L}_n \mid \gamma^n(x - \epsilon) \preceq \mathbf{b}_n \preceq \gamma^n(x + \epsilon)\}\end{aligned}$$

定理 2 (判定問題; 平滑化解析)

$\mu = \frac{c}{d} \in (1,2)$ は既約分数とし, $0 < \epsilon < 1/4$ とする.

ビット列 $\mathbf{b}_n \in \{0,1\}^n$ と実数 $x \in [0,1)$ が与えられたとき,

- $\mathbf{b}_n \in \mathcal{L}_n(x, \epsilon) \Rightarrow$ 受理
- $\mathbf{b}_n \notin \mathcal{L}_n(x, 2\epsilon) \Rightarrow$ 拒否

を実現可能. 入力 $\mathbf{b}_n$ が $\mathcal{D}_n(x, \epsilon)$ に従うとき,

期待領域計算量は $O\left(\frac{\log^3 d (\log^2 n + \log^2 \epsilon^{-1})}{\log^4 \mu}\right)$.

ただし, $\mathcal{D}_n(x, \epsilon): X \in [x - \epsilon, x + \epsilon]$ を一様として, $\gamma^n(X)$ の従う分布.

問題3への回答：定数領域近似

問題3 (計算問題)

入力: 実数 $x \in [0,1)$ と正整数 n .

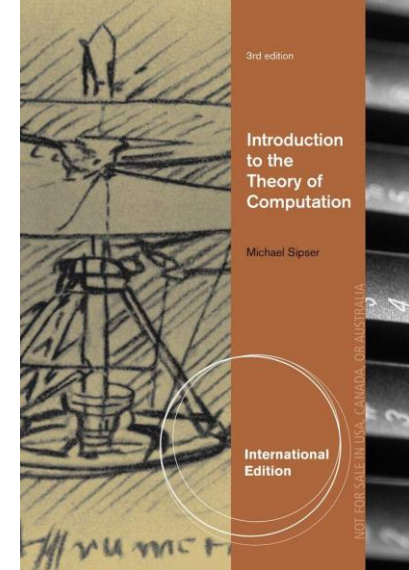
質問: $\gamma^n(x)$ を求めよ.

定理 3 (計算問題)

$\mu = \frac{c}{d} \in (1,2)$ は既約分数とし, $0 < \epsilon < 1/4$ とする.

実数 $x \in [0,1)$ と正整数 n が与えられたとき,

$\mathbf{b}_n \in \mathcal{L}_n(x, \epsilon)$ を $O\left(\frac{\lg^2 \epsilon^{-1} \lg d}{\lg^2 \mu} + \lg n\right)$ 計算領域で出力可能.



2.1. 計算と言語とオートマトン

計算機科学の歴史 (NP以前)

1874, Cantor, $\aleph^n \neq 2^\infty$, 対角線論法

1900, Hilbert, 23問題: 2. 算術の無矛盾性

1931, Gödel, 不完全性定理

1936, Turing, Turing機械 + 停止問題

1936, Church, ラムダ計算

1945, von Neumann, ノイマン型コンピュータ(ENIAC)

1956, Kleene, regular language = finite automaton認識

1956, Chomsky, Chomsky階層

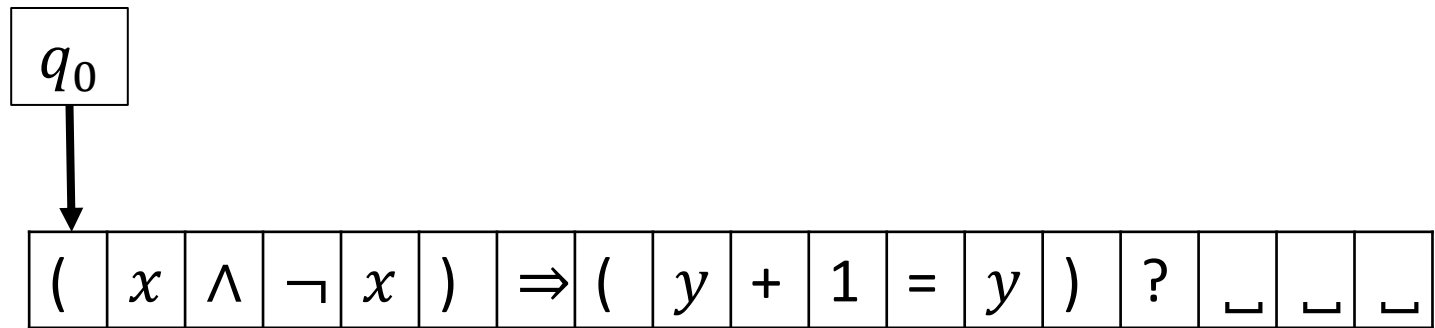
1971, Cook, NP完全の提案

} 証明=計算

} 言語と計算

} 計算量

計算機科学における計算: Turing machine



Turing machine

- headerとtapeで構成された機械
 - 決められた規則に従って動作する
- headerは有限個の演算規則集 (有限オートマトン)
- tapeはメモリ
 - 文字を読んだり書いたり(書き換えたり) できる. 長さに上限がない
- 文字は有限種類
- 最終的に, **accept(正しい)** or **reject(間違い)**を判断して**停止**
 - 判断できない計算問題が存在する (Turingの停止問題)

言語の認識

- Σ : 文字の集合(alphabet)
- Σ^k : 長さ k の文字列の集合. $\Sigma^* = \bigcup_{k=0}^{\infty} \Sigma^k$
- $\mathcal{L} \subseteq \Sigma^*$: 言語(language)
- $w \in \mathcal{L}$: 語(word)
- $w \in \mathcal{L}$ をacceptし, $w \notin \mathcal{L}$ をrejectできることを $\mathcal{L}$ のrecognitionという.

定理 (Kleene 1956)

正規言語であることの必要十分条件は**有限オートマトン**でrecognizeできる言語

$\Sigma = \{0,1\}$ とする.

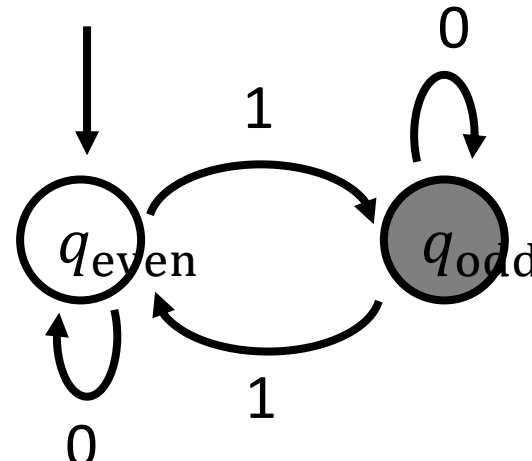
□ 正規言語の例

- $\{w \mid w \text{の最初と最後は同じ文字}\} = 0\Sigma^*0 \cup 1\Sigma^*1 \cup 0 \cup 1$
- $\{w \mid w \text{の長さは3の倍数}\} = (\Sigma\Sigma\Sigma)^*$
- $\{w \mid w \text{は1を偶数個もつ}\}$

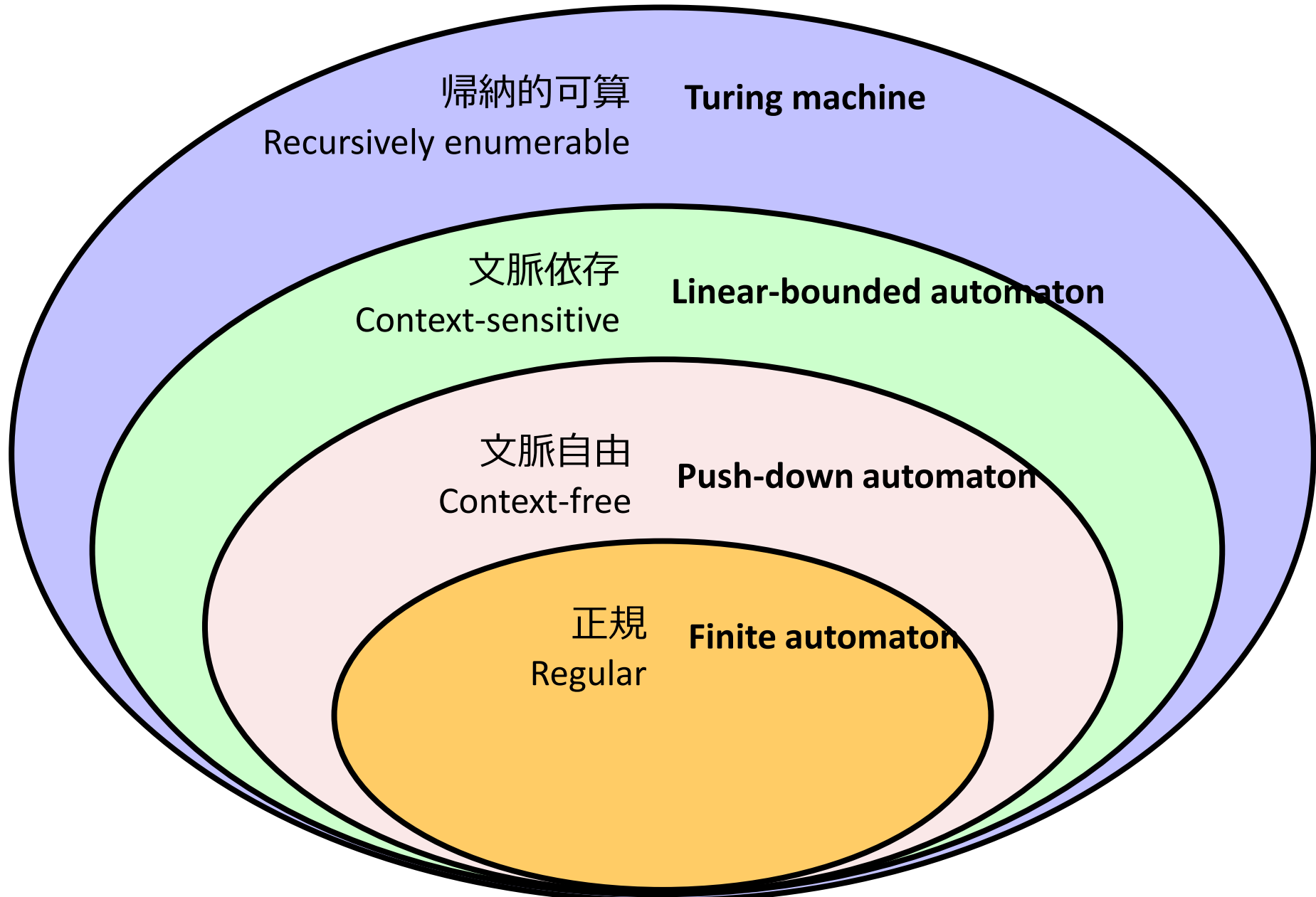
□ 正規言語でない例

- $\{0^n 1^n \mid n \geq 0\}$
- $\{w \mid w \text{は0と1を同数もつ}\}$

有限オートマトンは
大きな数を数えられない



Chomsky hierarchy



決定問題(decision problem)

例1. グラフ3彩色

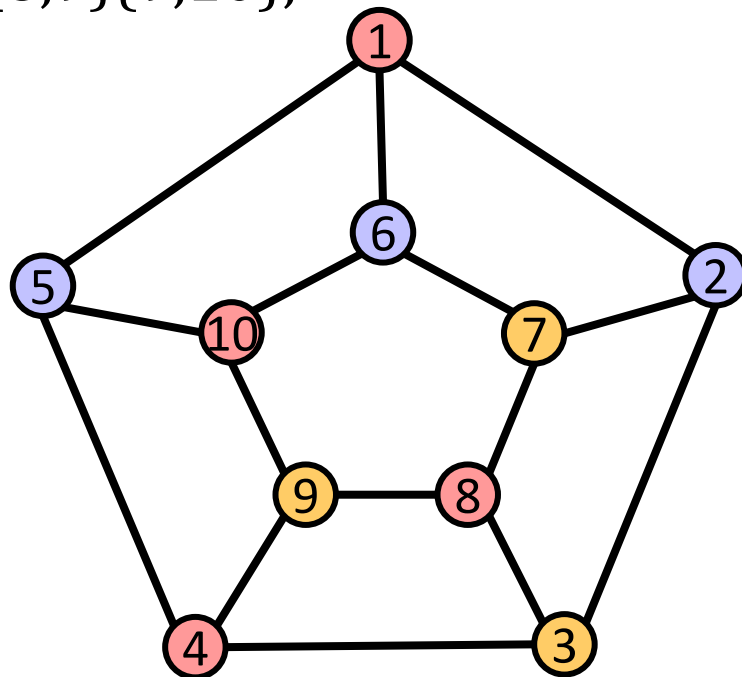
入力: $G = (V, E)$

問題: G は3色で塗り分けられるか？

$\mathcal{L} \subseteq \Sigma^* = \{0, \dots, 9, \{, \}, \dots, :, ;\}$: グラフ3彩色言語

$w = 10: \{1,2\}\{1,5\}\{1,6\}\{2,3\}\{2,7\}\{3,4\}\{3,8\}\{4,5\}\{4,9\}\{5,10\}$
 $\{6,7\}\{6,10\}\{7,8\}\{8,9\}\{9,10\};$

$w \in \mathcal{L}$



テント言語の認識

2.2. 自明なオートマトン

$\mathcal{L}$ のRecognition

Recognition

入力: $\mathbf{b} \in \{0,1\}^n$

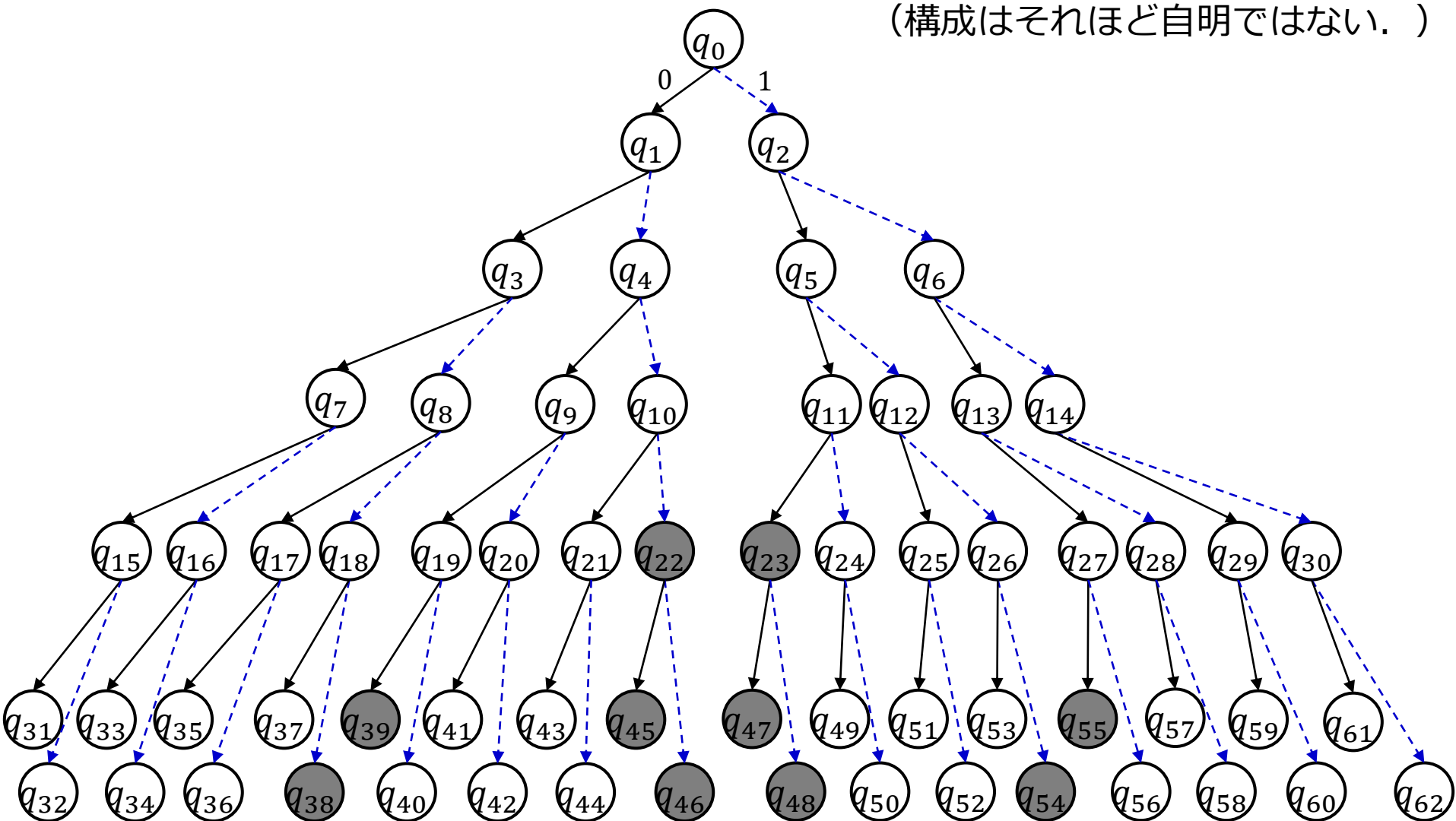
質問: $\mathbf{b} \in \mathcal{L}$?

例題 $\mathcal{L}(1.6)$

1. $\mathbf{b} = 100100$
2. $\mathbf{b} = 111000111000$
3. $\mathbf{b} = 1100110011001100$
4. $\mathbf{b} = 11010101010101010$

テント言語 $\mathcal{L}_{\leq 5}(1.6)$ の「自明な」オートマトン

(構成はそれほど自明ではない。)



サイズが大きい！

テント言語の認識

2.3. 基本アイデア

テント言語上の同値関係

観察

- n 回反復テント写像は多くの**折れ線**で構成される.
- 各線分は $\mathcal{L}_n$ と一対一対応. ($\Rightarrow$ 演習問題)
- 線分の数 ($= |\mathcal{L}_n|$) は n に関して指数的に増加する.
- **しかし, いくつかの折れ線は「同じ」ように見える.**

セクション

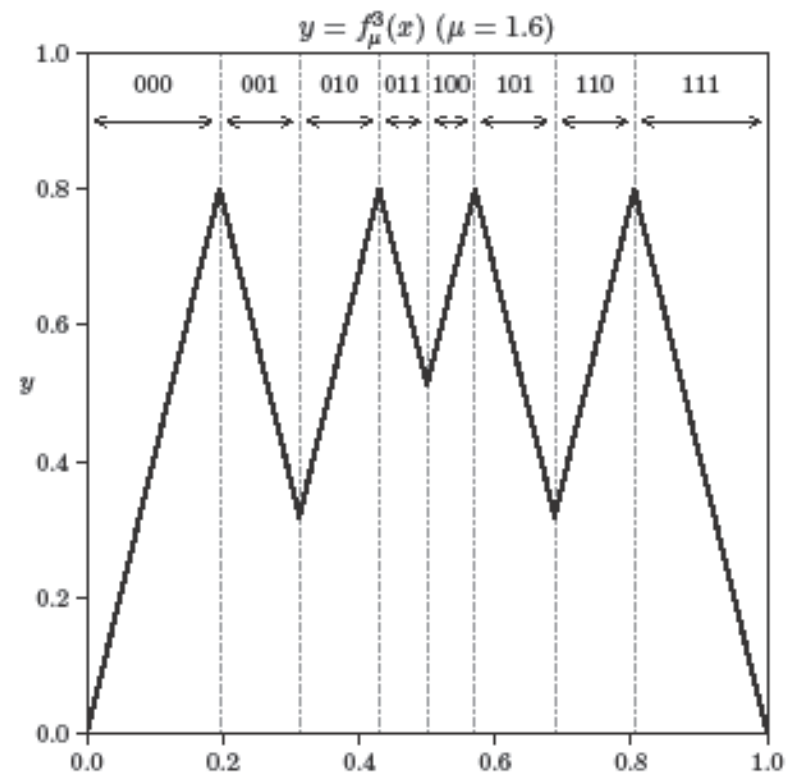
$$S(\mathbf{b}) = \{x \mid \gamma(x) = \mathbf{b}\}$$

セクションタイプ

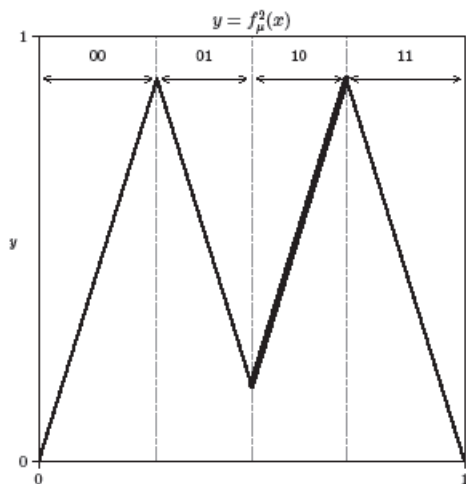
$$T(\mathbf{b}) = \{f^n(x) \mid \gamma^n(x) = \mathbf{b}\}$$

- $\mathcal{T}_n = \{T(\mathbf{b}) \mid \mathbf{b} \in \mathcal{L}_n\}$
- $\mathcal{T} = \bigcup_{n=1}^{\infty} \mathcal{T}_n$

$$\mathbf{b} \sim \mathbf{b}' \Leftrightarrow T(\mathbf{b}) = T(\mathbf{b}')$$

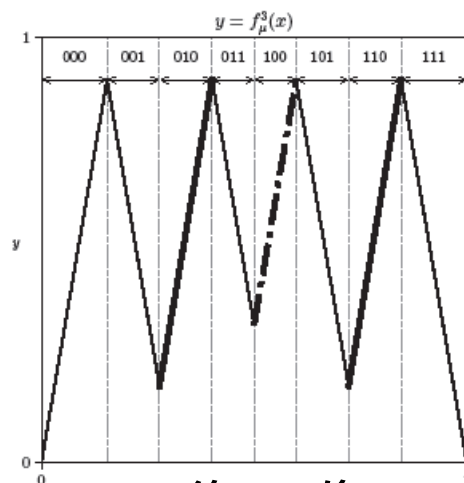


テント言語上の同値関係



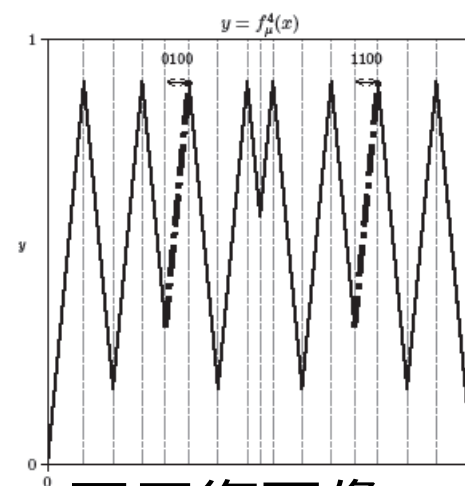
2回反復写像

- $|\mathcal{L}_n| = 4$
- $|\mathcal{T}_n| = 4$



3回反復写像

- $|\mathcal{L}_n| = 8$
- $|\mathcal{T}_n| = 6$



4回反復写像

- $|\mathcal{L}_n| = 16$
- $|\mathcal{T}_n| = 8$

一般に, n 回反復すると

- $|\mathcal{L}_n| \geq \mu^n$
- $|\mathcal{T}_n| \leq 2n$



命題 2.1.

テント言語上の同値関係

実は $\bar{c}_i$ は c_i のbit反転 (演習)

命題 2.1

$c_i = \gamma^i \left(\frac{1}{2} \right)$ とし, $\bar{c}_i = \gamma^i \left(\frac{1}{2} - 0 \right)$ とする.

$I_i = T(c_i)$ と $\bar{I}_i = T(\bar{c}_i)$ ($i = 1, 2, \dots$) を定める.

このとき, 任意の $n \geq 1$ について

$$\mathcal{T}_n = \bigcup_{i=1}^{n^*} \{I_i, \bar{I}_i\}$$

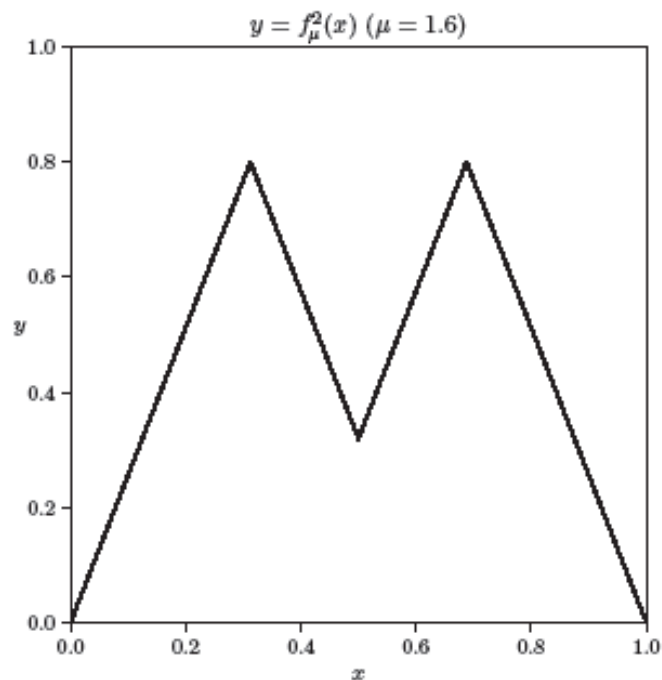
ただし n^* ($n^* \leq n$) は適切なパラメータとする.

詳細には $n_* = \min(\{i \in \{1, 2, \dots, n-1\} \mid I_{i+1} \in \mathcal{T}_i\} \cup \{n\})$.

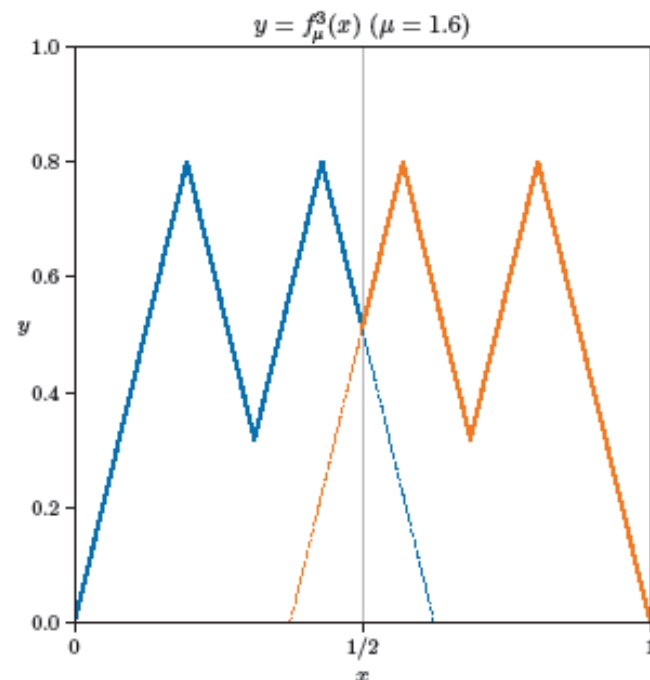
命題2.1の示唆

- $|\mathcal{T}_n| \leq 2n$ (n 回反復時のセクションタイプは高々 $2n$)
- $\mathcal{T}_{n-1} \subseteq \mathcal{T}_n$ (異なる反復回数間でセクションタイプは共有される)

命題2.1の直感



$f^2(x)$



$f^3(x)$

観察

- $f^{n+1}(x) \left(x \leq \frac{1}{2} \right)$: f^n を左に $1/\mu$ 倍に押し縮める (1/2で打切り) .
- $f^{n+1}(x) \left(x \geq \frac{1}{2} \right)$: f^n を右に $1/\mu$ 倍に押し縮める (1/2で打切り) .

観察

- $f^{n+1}(x) \left(x \leq \frac{1}{2} \right)$: f^n を左に $1/\mu$ 倍に押し縮める (1/2で打ち切り) .
- $f^{n+1}(x) \left(x \geq \frac{1}{2} \right)$: f^n を右に $1/\mu$ 倍に押し縮める (1/2で打ち切り) .

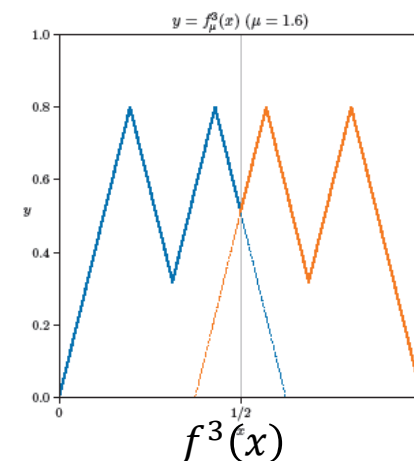
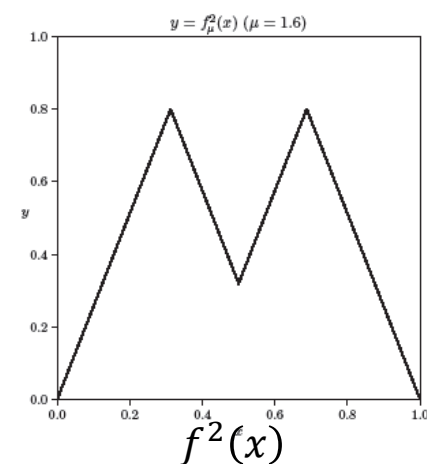
Compression lemma

補題 2.2.

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

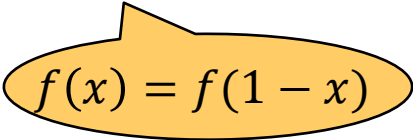
$$f^{n+1}(x) = f^n(\tilde{f}(x)) = \begin{cases} f^n(\mu x) & x \leq \frac{1}{2} \\ f^n(1 - \mu(1 - x)) & x \geq \frac{1}{2} \end{cases}$$

- $x \leq \frac{1}{2}$ のとき: $f^3(x) = f^2(\mu x)$ (青い折れ線)
- $x \geq \frac{1}{2}$ のとき: $t = 1 - x$ とおくと
 $f^3(1 - t) = f^2(1 - \mu t)$ (オレンジの折れ線)



補題 2.2の証明

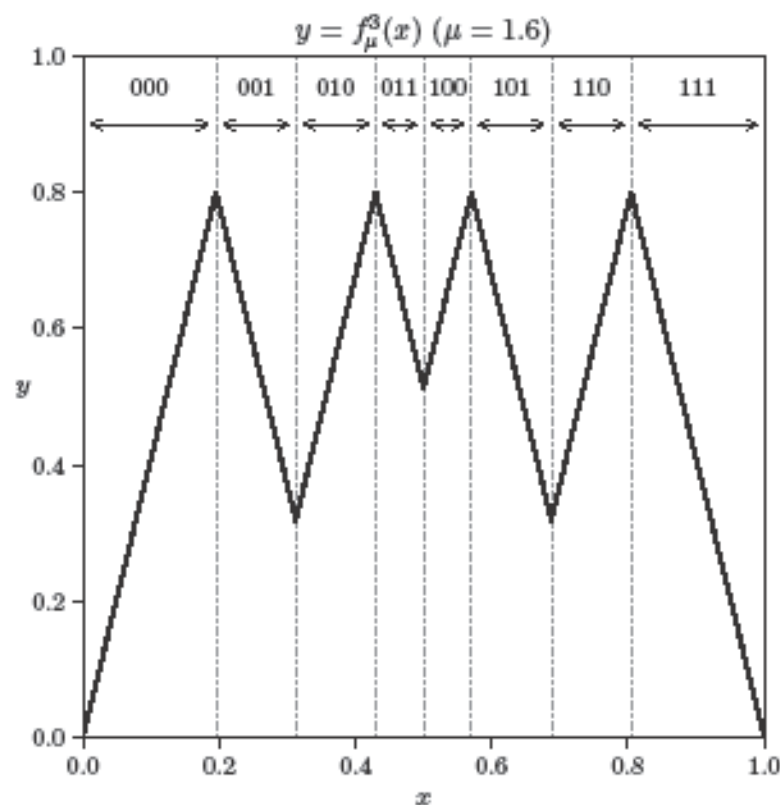
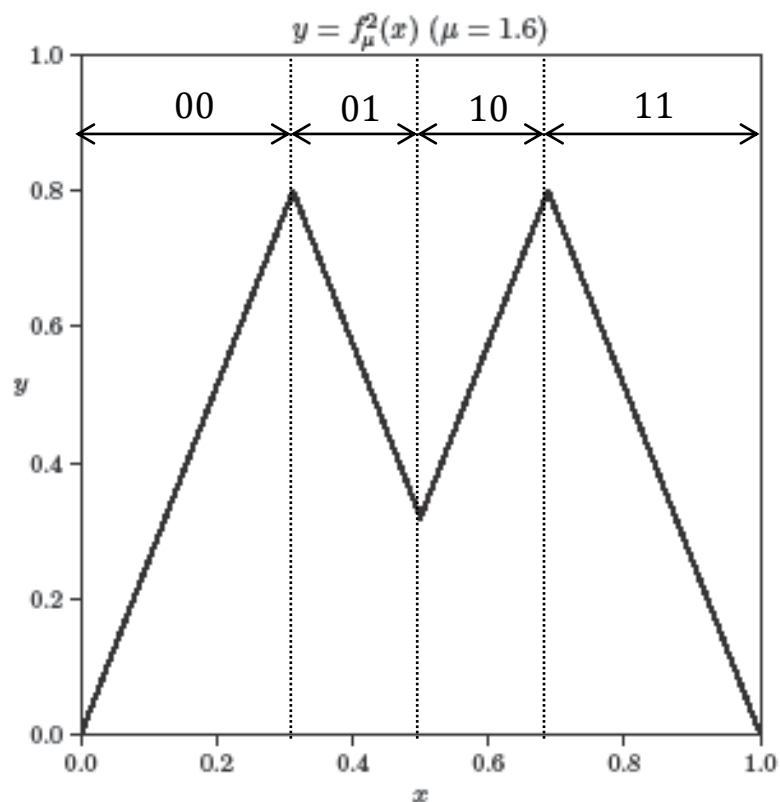
- ✓ $x \leq \frac{1}{2}$ のとき $f^{n+1}(x) = f^n(f(x)) = f^n(\tilde{f}(x))$.
- ✓ $x \geq \frac{1}{2}$ のとき $f^{n+1}(x) = f^n(f(x)) = f^n(1 - f(x)) = f^n(\tilde{f}(x))$


$$f(x) = f(1 - x)$$

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

補題 2.3

$\tilde{f}(S_n(\mathbf{b}_n)) \subseteq S_{n-1}(b_2 \cdots b_n)$. $\mathbf{b}_n \neq \gamma^n \left(\frac{1}{2} \pm 0\right)$ の時は等号成立.



図を見る限り明らか（っぽい）。

一応、補題2.3の証明

補題2.2から
ほぼ自明だが

□ $\tilde{x} = \tilde{f}(x)$ とする.

□ $\gamma^n(x) = b_1 \cdots b_n$

□ $\gamma^{n-1}(\tilde{x}) = d_1 \cdots d_{n-1}$

□ $b_{i+1} = d_i$ を示す.

- $x_{i+1} = \tilde{x}_i$ ($i = 2, 3, \dots$)
 - よって $i \geq 2$ の場合は自明

• $b_2 = d_1$ を示す.

- $x < 1/2$ の場合: $b_1 = 0, \tilde{x} = x_1$
 - ✓ $f(x) < 1/2$ の場合: $b_2 = 0; d_1 = 0$
 - ✓ $f(x) \geq 1/2$ の場合: $b_2 = 1; d_1 = 1$
- $x \geq 1/2$ の場合: $b_1 = 1, \tilde{x} = 1 - x_1$
 - ✓ $f(x) \leq 1/2$ の場合: $b_2 = 1; d_1 = 1$
 - ✓ $f(x) > 1/2$ の場合: $b_2 = 0; d_1 = 0$

テント符号 $\gamma^n(x) = b_1 b_2 \cdots b_n$ ($x \in [0, 1)$)

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

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

命題2.1の証明 (エッセンス)

証明

- $\mathcal{T}_1 = \{T(1), T(0)\}$ より $n = 1$ はOK.
- $\mathcal{T}_n \subseteq \mathcal{T}_{n-1} \cup \{T(\mathbf{d}_n), T(\mathbf{d}'_n)\}$ を示す.
- $T(\mathbf{b}_n) = T(b_2 \cdots b_n)$ を示す.

$$T(\mathbf{b}_n) = \{f^n(x) \mid x \in S_n(\mathbf{b}_n)\}$$

$$= \{f^{n-1}(\tilde{f}(x)) \mid x \in S_n(\mathbf{b}_n)\}$$

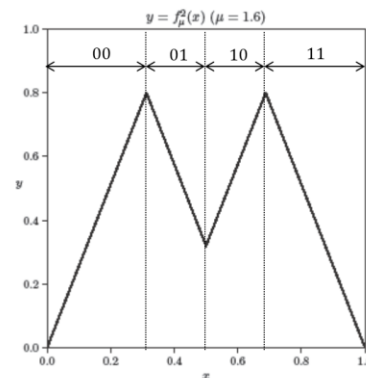
$$= \{f^{n-1}(y) \mid y \in \tilde{f}(S_n(\mathbf{b}_n))\}$$

$$= \{f^{n-1}(y) \mid y \in S_{n-1}(b_2 \cdots b_n)\}$$

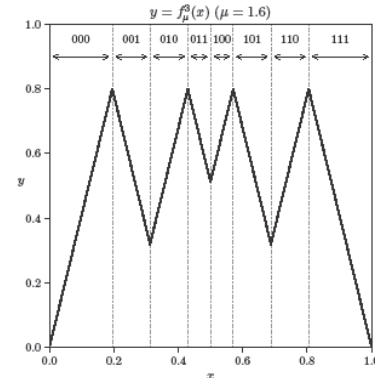
$$= T(b_2 \cdots b_n)$$

補題2.2

補題2.3



$f^2(x)$



$f^3(x)$

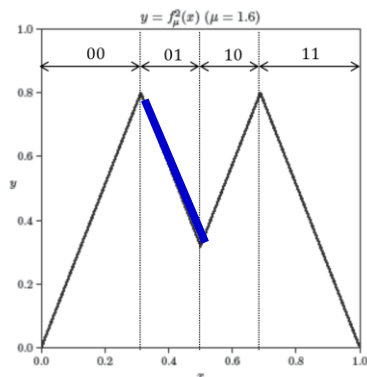
テント言語の認識

2.4. 非自明なオートマトン

テント言語の同値類

01 ~ 001 ~ 101 ~ 0001
 ~ 0101 ~ 1101 on $\mathcal{L}(1.6)$

$f^2(x)$



$\mathcal{T}_5 (\mu = 1.6)$

$$\bar{I}_1 = [0, 0.8)$$

$$I_1 = (0, 0.8]$$

$$\bar{I}_2 = (0.32, 0.8]$$

$$I_2 = [0.32, 0.8)$$

$$\bar{I}_3 = (0.512, 0.8]$$

$$I_3 = [0.512, 0.8)$$

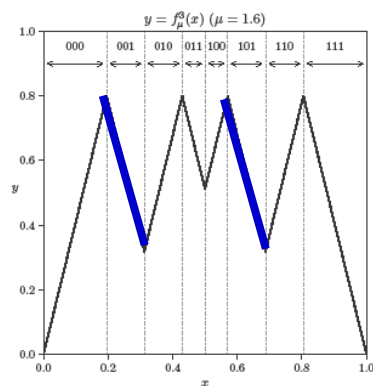
$$\bar{I}_4 = [0.32, 0.7808)$$

$$I_4 = (0.32, 0.7808]$$

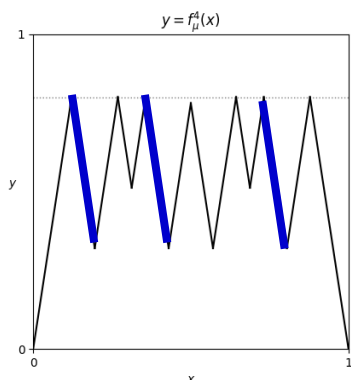
$$\bar{I}_5 = (0.35072, 0.8]$$

$$I_5 = [0.35072, 0.8)$$

$f^3(x)$



$f^4(x)$



写像の反復と同値類の遷移

補題 2.4

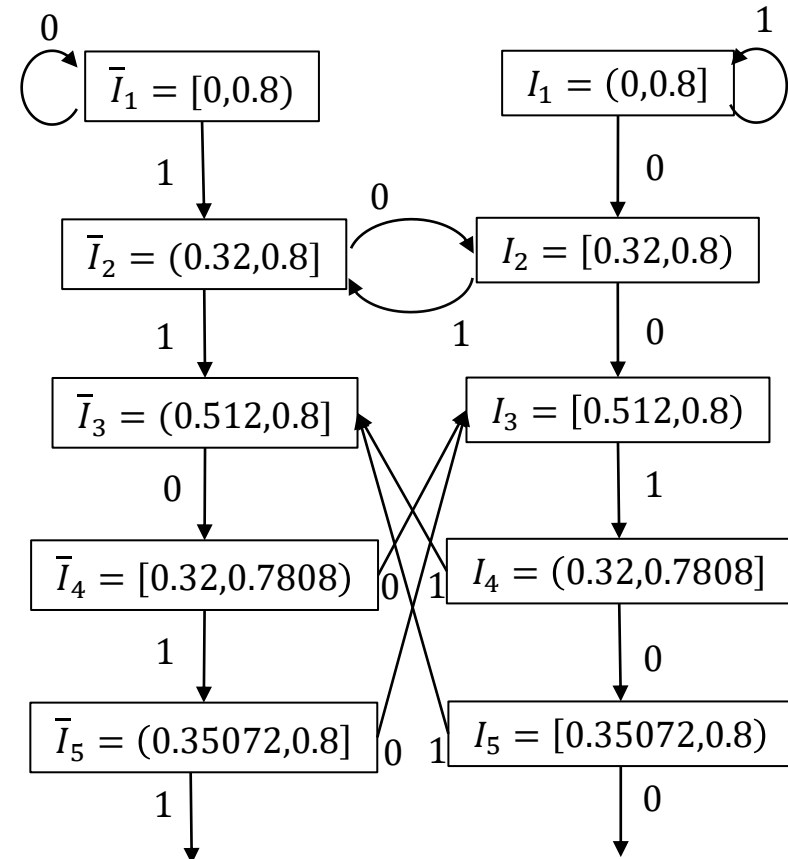
- $T(b_1 \cdots b_k) = T(b'_1 \cdots b'_k)$ とする.
 $b \in \{0,1\}$ に対して,
 $b_1 \cdots b_k b \in \mathcal{L} \Leftrightarrow b'_1 \cdots b'_k b \in \mathcal{L}$.
- さらに $T(b_1 \cdots b_k b) = T(b'_1 \cdots b'_k, b)$.

“証明の直観”.

- $b_{k+1} \in \{0,1\}$ は $f^k(x) < \frac{1}{2}$ で決まる.
- タイプ $T(b_1 \cdots b_k)$ は $f^k(x)$ の値域

$\mathcal{T}_5$ 上の状態遷移

($\mu = 1.6$)



テント言語のオートマトン

Recognition

入力: $\mathbf{b} \in \{0,1\}^n$

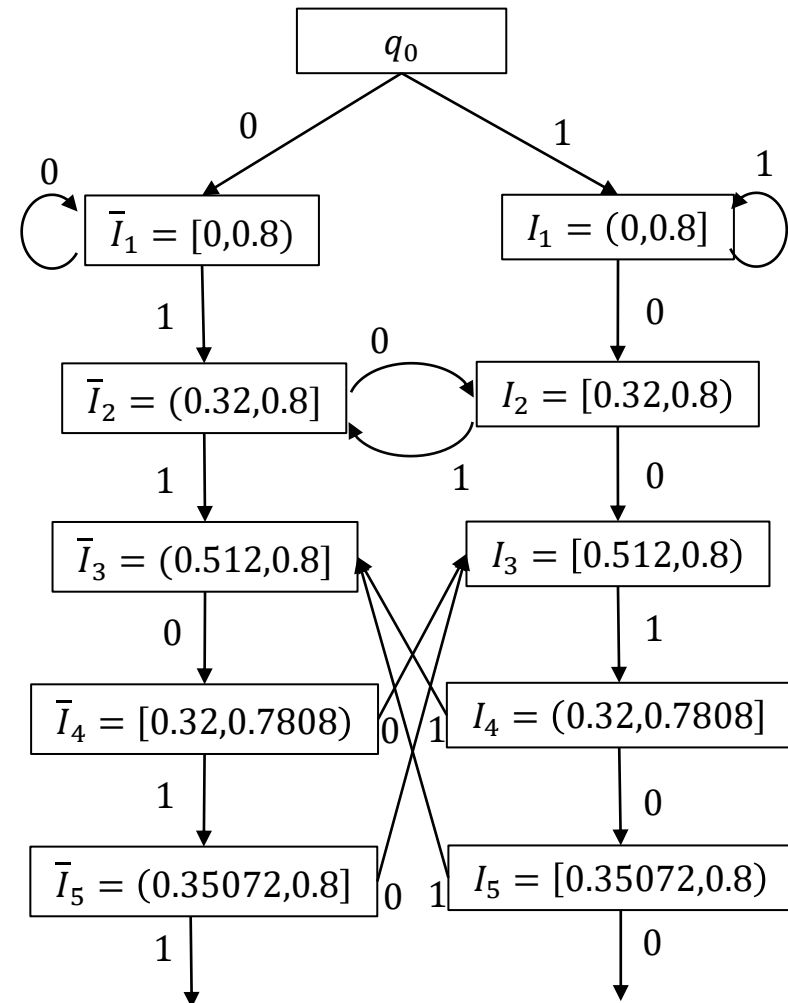
質問: $\mathbf{b} \in \mathcal{L}$?

- 状態数は $2n + 2$
 - $\mathcal{T}_n \cup \{q_0, q_\perp\}$
- $\mathcal{L}_n$ を **正しく** 認識.
 - $\mathbf{b} \in \mathcal{L}$ なら accept
 - $\mathbf{b} \notin \mathcal{L}$ なら reject
- セクションタイプ $J \in \mathcal{T}$ の段を **レベル** といい $L(J)$ で表す.
 i.e., $[L(J) = l] \Leftrightarrow [J = I_l \text{ or } \bar{I}_l]$
- オートマトンは「左右対称」.
 また $\text{cl}(I_l) = \text{cl}(\bar{I}_l)$.

(演習)

$\mathcal{T}_5$ 上の状態遷移

($\mu = 1.6$)



具体的な状態遷移

補題2.5

$T^n(x) = [v, u)$ のとき

$$T^{n+1}(x) = \begin{cases} \begin{cases} [f(v), f(.5)) & f^n(x) < .5 \\ (f(v), f(.5)] & f^n(x) \geq .5 \end{cases} & v < .5 < u \\ [f(v), f(u)) & u \leq .5 \\ (f(u), f(v)] & v \geq .5 \end{cases}$$

$T^n(x) = (v, u]$ のとき

$$T^{n+1}(x) = \begin{cases} \begin{cases} (f(v), f(.5)] & f^n(x) \leq .5 \\ [f(v), f(.5)) & f^n(x) > .5 \end{cases} & v < .5 < u \\ (f(u), f(v)] & u \leq .5 \\ [f(v), f(u)) & v \geq .5 \end{cases}$$

2.5. 計算量

テント言語のオートマトン

Recognition

入力: $\mathbf{b} \in \{0,1\}^n$

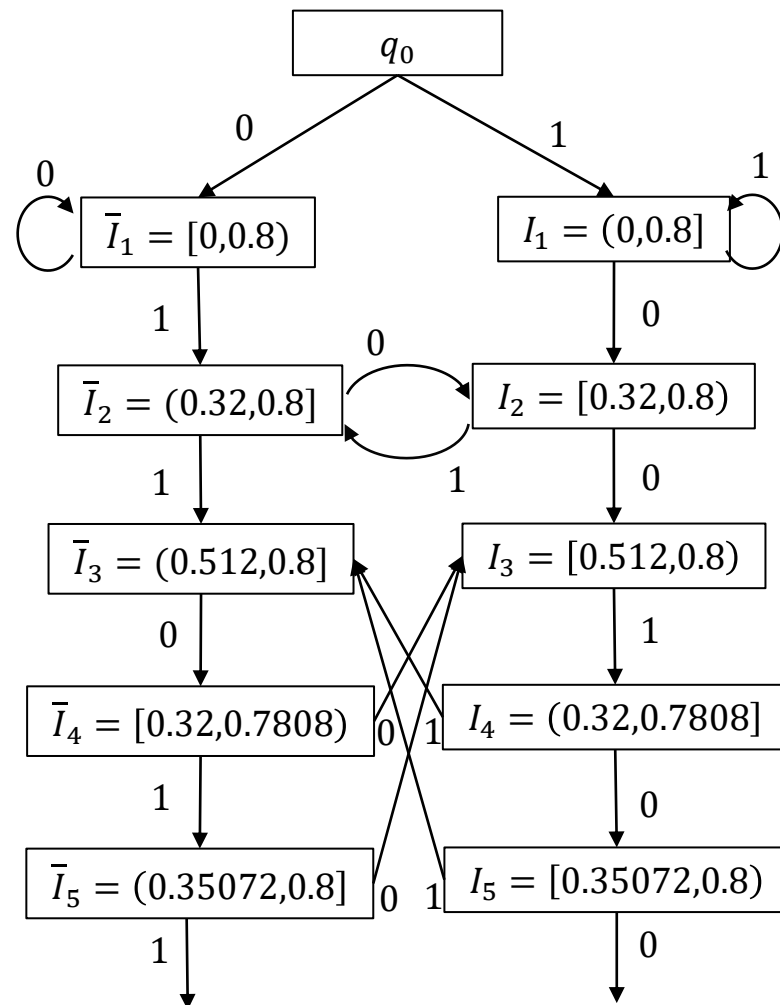
質問: $\mathbf{b} \in \mathcal{L}$?

例題 $\mathcal{L}(1.6)$

1. $\mathbf{b} = 100100$
2. $\mathbf{b} = 111000111000$
3. $\mathbf{b} = 1100110011001100$
4. $\mathbf{b} = 11010101010101010$

$\mathcal{T}_5$ 上の状態遷移

($\mu = 1.6$)



テント言語のオートマトン

Recognition

入力: $\mathbf{b} \in \{0,1\}^n$

質問: $\mathbf{b} \in \mathcal{L}$?

例題 $\mathcal{L}(1.6)$

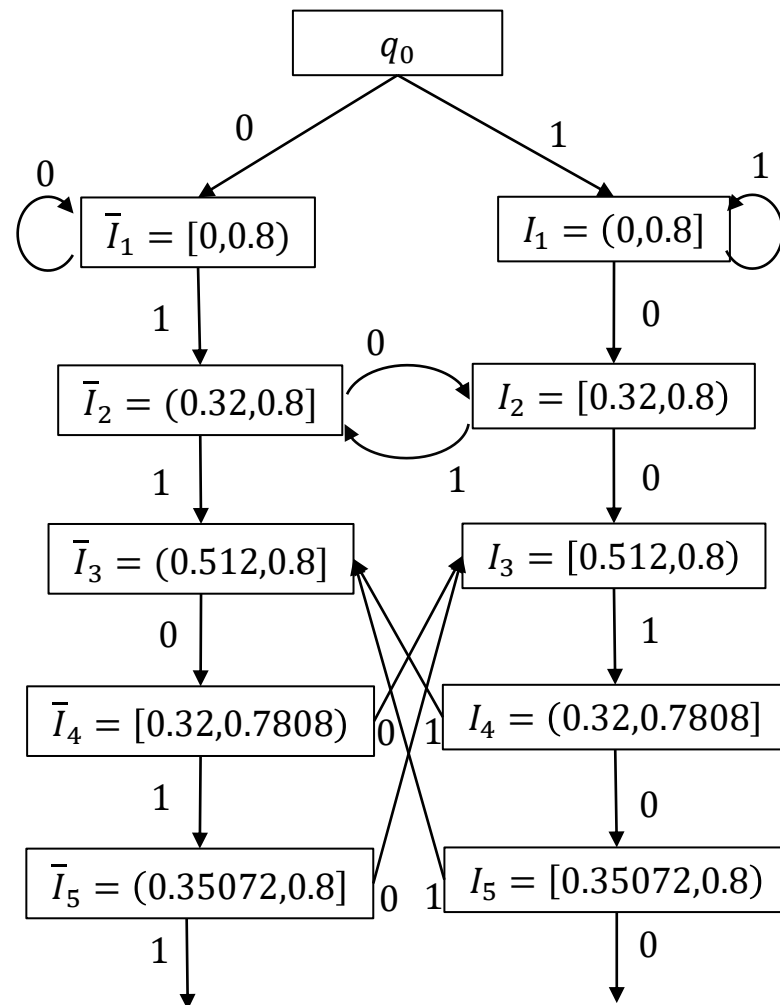
1. $\mathbf{b} = 100100$ 5段
2. $\mathbf{b} = 111000111000$ 3段
3. $\mathbf{b} = 1100110011001100$ 4段
4. $\mathbf{b} = 11010101010101010$ 2段

入力が n bit だからと言って,
 n 段まで必要ない場合もある.

➡ 遅延更新 (Deferred update)

$\mathcal{T}_5$ 上の状態遷移

($\mu = 1.6$)



テント言語のオートマトン

Recognition

入力: $\mathbf{b} \in \{0,1\}^n$

質問: $\mathbf{b} \in \mathcal{L}$?

命題 2.6.

$\mu = c/d$ は既約分数とする.

判定問題の空間計算量は
 $O(k^2 \log d)$.

ただし, k は入力 $\mathbf{b}$ が要する最大レベル.

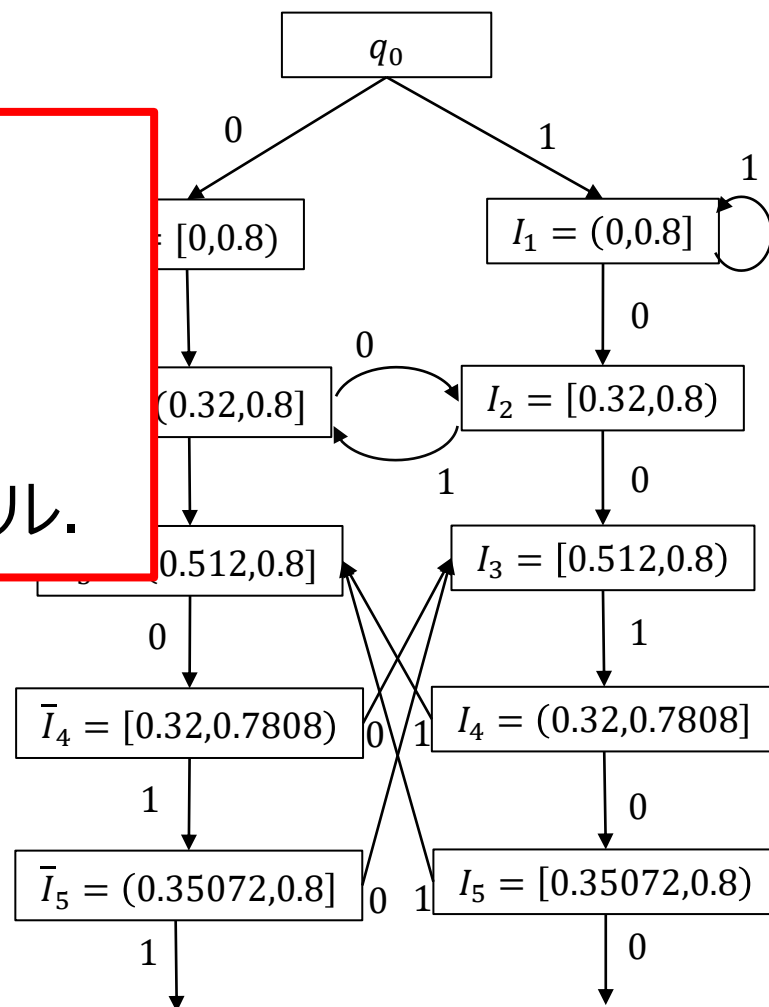
証明

セクションタイプ I_k は

$O(k \log d)$ 領域で表現可能.

$\mathcal{T}_5$ 上の状態遷移

($\mu = 1.6$)



補題2.7.

$\frac{a}{b} \in (0,1)$ は既約分数とする. $f^k\left(\frac{a}{b}\right) = \frac{c_k}{d_k}$ (既約) とすると

$$\lg d_k \leq k \lg d + \lg b$$

証明: 帰納法

- $k = 0$ の場合は自明.

- $f^k\left(\frac{a}{b}\right) \leq 1/2$ の場合

$$f^{k+1}\left(\frac{a}{b}\right) = \mu f^k\left(\frac{a}{b}\right) = \frac{c}{d} \frac{c_k}{d_k}$$

よって $\lg d_{k+1} \leq \lg d + \lg d_k \leq (k+1) \lg d + \lg b$.

- $f^k\left(\frac{a}{b}\right) > 1/2$ の場合

$$f^{k+1}\left(\frac{a}{b}\right) = \mu \left(1 - f^k\left(\frac{a}{b}\right)\right) = \frac{c}{d} \left(1 - \frac{c_k}{d_k}\right) = \frac{c d_k - c_k d}{d d_k}$$

同様に $\lg d_{k+1} \leq (k+1) \lg d + \lg b$. よって題意を得る.

$$f^k\left(\frac{a}{b}\right) = \frac{c_k}{d_k} \in (0,1) \text{より}$$

$$\lg c_k \leq \lg d_k$$

すなわち $f^k\left(\frac{a}{b}\right)$ は

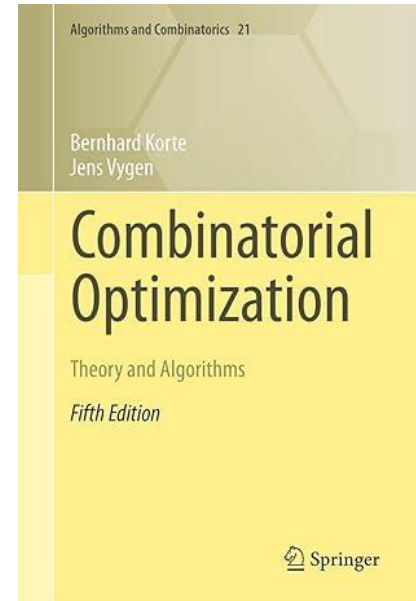
$2(k \lg d + \lg b + 1)$ bit
で表現可能

「計算量」(決定性 Turing machine)

通常(形容詞のない場合)は
worst case time complexityを指す

□ 計算量 = 演算回数(有限回に限る)

- 読み込み, 書き出し, 代入, 比較: $O(\text{桁数})$
- 四則演算(+, -, ×, /) $O(\text{桁数})$
- 論理演算($\neg, \wedge, \vee, \Rightarrow$) $O(1)$ /1演算
- 繰り返し(for, while)は繰り返し中の演算の総数
- 「パラメータ」
 - 固定(定数)なら $O(1)$
 - 可変なら四則演算に準ずる
- 「関数(ライブラリ)」
 - 計算量が解明されていれば, それに準拠
 - オラクル計算量では, 通常の演算数とは別に数える



3.1. マルコフモデル

テント言語のオートマトン

Recognition

入力: $\mathbf{b} \in \{0,1\}^n$

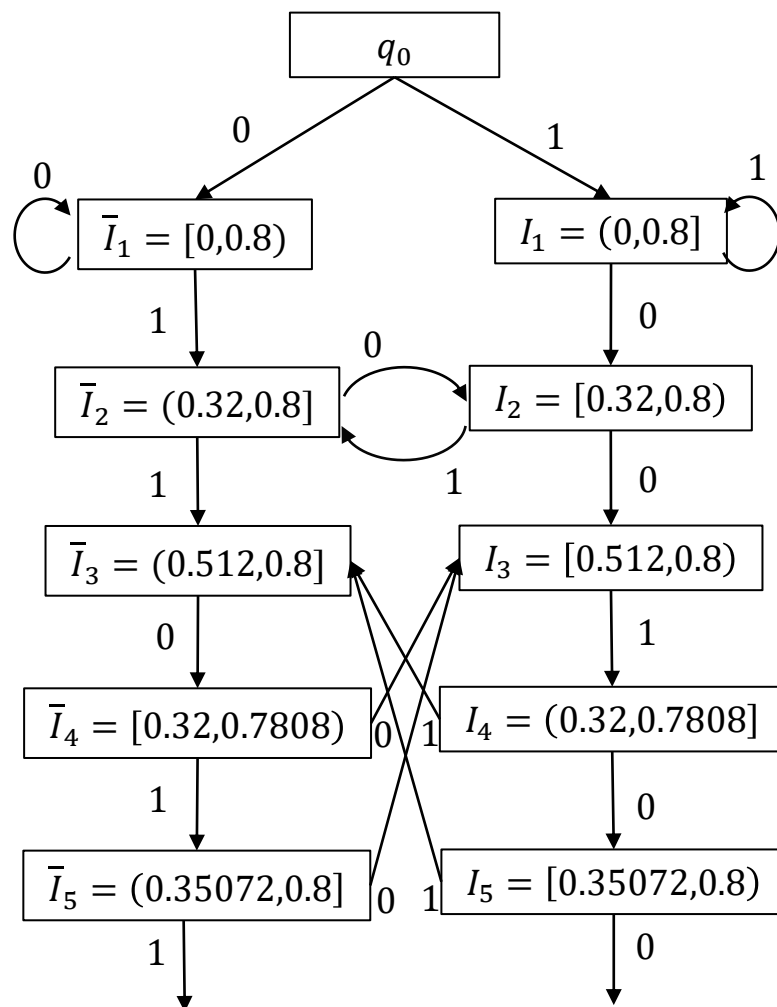
質問: $\mathbf{b} \in \mathcal{L}$?

例題 $\mathcal{L}(1.6)$

1. $\mathbf{b} = 100100$
2. $\mathbf{b} = 111000111000$
3. $\mathbf{b} = 1100110011001100$
4. $\mathbf{b} = 11010101010101010$

$\mathcal{T}_5$ 上の状態遷移

($\mu = 1.6$)



マルコフモデル (確率的オートマトン)

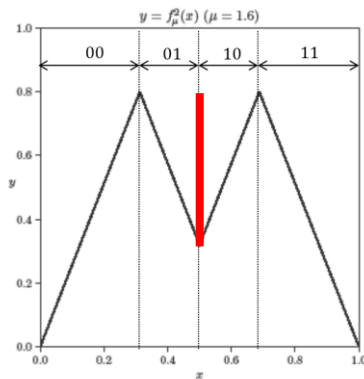
補題 3.1.

$X \in (0,1)$ は一様ランダムとする.

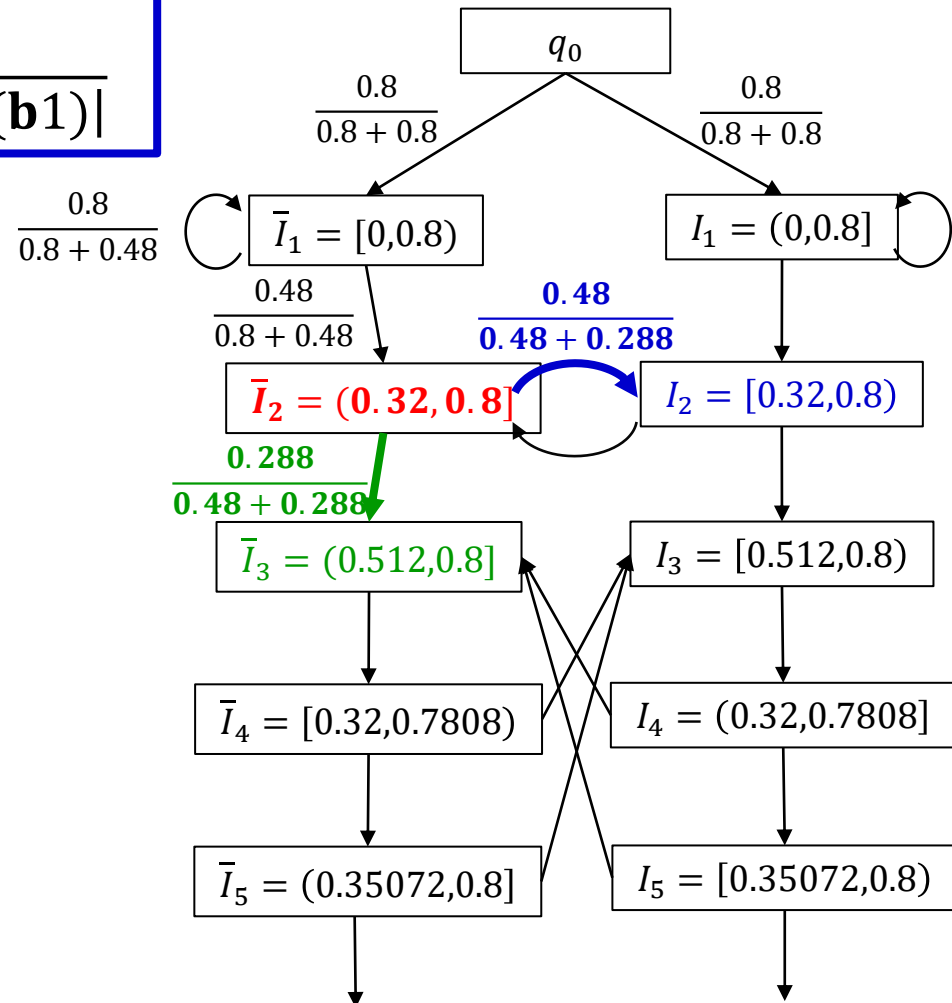
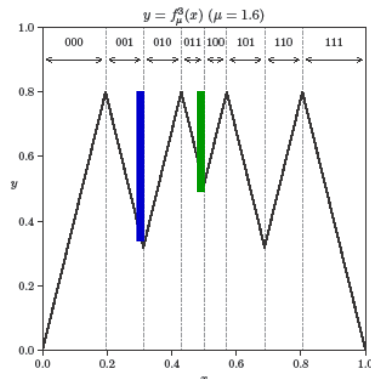
$B_1 \cdots B_n = \gamma^n(X)$ とすると,

$$\Pr[B_i = 0 \mid \mathbf{B}_{i-1} = \mathbf{b}] = \frac{|T(\mathbf{b}0)|}{|T(\mathbf{b}0)| + |T(\mathbf{b}1)|}$$

$f^2(x)$



$f^3(x)$



主張

$f^n(X)$ は $T(\gamma^n(X))$ 上に一様に分布する

証明: 帰納法

- X は $[0,1)$ 上に一様に分布する ($n = 0$ の場合はOK) .
- X_{n-1} が $T(\gamma^{n-1}(X)) = \left[v, \frac{1}{2}\right)$ 上に一様に分布している場合に,
 X_n が $\left[f(v), f\left(\frac{1}{2}\right)\right)$ 上で一様に分布することを示す (他の場合も同様) .

$$\begin{aligned}
 \Pr\left[f^n(X) < k \mid X_{n-1} \in \left[v, \frac{1}{2}\right)\right] &= \Pr\left[f(X_{n-1}) < k \mid X_{n-1} \in \left[v, \frac{1}{2}\right)\right] \\
 &= \Pr\left[\mu X_{n-1} < k \mid X_{n-1} \in \left[v, \frac{1}{2}\right)\right] \\
 &= \Pr\left[X_{n-1} < \frac{k}{\mu} \mid X_{n-1} \in \left[v, \frac{1}{2}\right)\right] \\
 &= \frac{\left|\left[v, \frac{k}{\mu}\right]\right|}{\left|\left[v, \frac{1}{2}\right]\right|} = \frac{|\left[\mu v, k\right]|}{\left|\left[\mu v, \frac{\mu}{2}\right]\right|} = \frac{|\left[f(v), k\right]|}{\left|\left[f(v), f\left(\frac{1}{2}\right)\right]\right|}
 \end{aligned}$$

➤ よって X_n は $\left[f(v), f\left(\frac{1}{2}\right)\right)$ 上で一様に分布する.

マルコフモデル (確率的オートマトン)

補題 3.1.

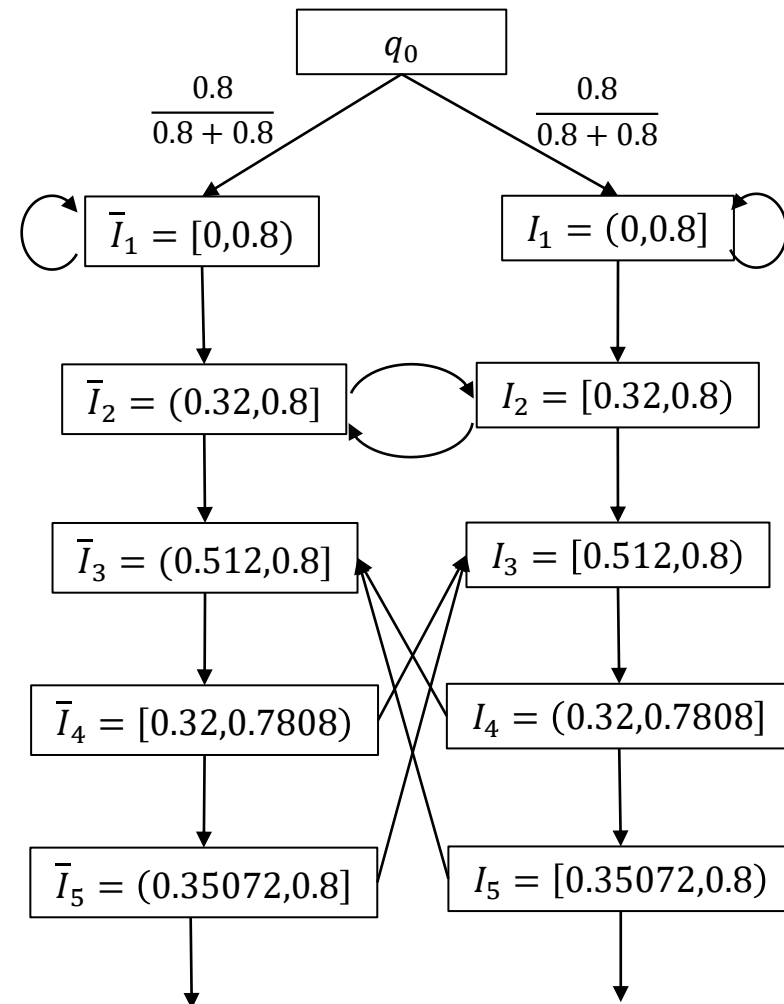
$X \in (0,1)$ は一様ランダムとする.

$B_1 \cdots B_n = \gamma^n(X)$ とすると,

$$\Pr[B_i = 0 \mid \mathbf{B}_{i-1} = \mathbf{b}] = \frac{|T(\mathbf{b}0)|}{\mu|T(\mathbf{b})|}$$

Remark

- $|T(\mathbf{b}0)| + |T(\mathbf{b}1)| = \mu|T(\mathbf{b})|$ (演習)
- $p(J, J') = p(\bar{J}, \bar{J}')$ (演習)
ただし, $J = I_l$ のとき $\bar{J} = \bar{I}_l$ を表すものとする.



3.2. 平均計算量解析

最大レベルの解析

- $Z_0, Z_1, Z_2, \dots: Z_0 = q_0$ とするマルコフ連鎖
- $K_n = \max\{L(Z_t) | 0 \leq t \leq n\}$

例えば $q = \frac{1}{n}$ を代入すると,
$$\Pr[K_n \geq \lceil 2 \log_\mu n \rceil] \leq \frac{1}{n}$$

i.e., 高い確率で $K_n = O(\log_\mu n)$

補題 3.2.

$k_q = \lceil \log_\mu n + \log_\mu q^{-1} \rceil$ とおくと, $\Pr[K_n \geq k_q] \leq q$.

証明のアウトライン

主張 1.

$k \geq 2$ は任意とする.

A_t : Z_t が時刻 t で初めてレベル k に到達するイベントとすると,

$$\Pr[A_t] \leq \frac{|I_k|}{\mu^k}.$$

主張 2.

$$\frac{|I_{k_q}|}{\mu^{k_q}} \leq \frac{q}{n}.$$

$$A_t = \bigwedge_{s < t} [L(Z_s) < k] \wedge [L(Z_t) = k]$$

主張1の証明

- $|I_i| = |\bar{I}_i|$ ($i = 1, 2, 3, \dots$)

- とくに $|I_1| = \frac{\mu}{2}$

- レベルが上がるのは $I_i \rightarrow I_{i+1}$ or $\bar{I}_i \rightarrow \bar{I}_{i+1}$

- 確率 $p(I_i, I_{i+1}) = \frac{|I_{i+1}|}{\mu |I_i|} = p(\bar{I}_i, \bar{I}_{i+1})$

- レベル k に至るまでに, 各 $i = 1, 2, \dots, k-1$ について
少なくとも1回 $I_i \rightarrow I_{i+1}$ or $\bar{I}_i \rightarrow \bar{I}_{i+1}$ の推移を要する. よって

$$\begin{aligned} \Pr[A_t] &\leq \prod_{i=1}^{k-1} p(I_i, I_{i+1}) \\ &= \prod_{i=1}^{k-1} \frac{|I_{i+1}|}{\mu |I_i|} \\ &= \frac{|I_k|}{\mu^{k-1} |I_1|} \\ &= \frac{2|I_k|}{\mu^k} \end{aligned}$$

主張 1.

$k \geq 2$ は任意とする.

A_t : Z_t が時刻 t で初めてレベル k に到達する

$$\Pr[A_t] \leq \frac{|I_k|}{\mu^k}.$$

主張2の証明

主張 2.

$$\frac{|I_{k_q}|}{\mu^{k_q}} \leq \frac{q}{n}.$$

- $k_q = \lceil \log_{\mu} n + \log_{\mu} q^{-1} \rceil$ (補題3.2の前提)
- 背理法: $\frac{|I_{k_q}|}{\mu^{k_q}} > \frac{q}{n}$ と仮定
- $|I_{k_q}| > \frac{q}{n} \mu^{k_q} \geq \frac{q}{n} \mu^{\log_{\mu} n + \log_{\mu} q^{-1}} \geq \frac{q}{n} n q^{-1} = 1$
- $|I_{k_q}| \leq 1$ に矛盾.

補題3.2の証明

- A_t^* : Z_t が時刻 t で初めてレベル k_q に到達するイベント
- $\Pr[K_n \geq k_q] = \Pr[V_{t=0}^n A_t^*]$

$$\leq \sum_{t=0}^n \Pr[A_t^*]$$

$$\leq n \frac{|I_{k_q}|}{\mu^{k_q}}$$

$$\leq n \frac{q}{n}$$

$$= q$$

主張 1.

$$\Pr[A_t^*] \leq \frac{|I_{k_q}|}{\mu^{k_q}}.$$

主張 2.

$$\frac{|I_{k_q}|}{\mu^{k_q}} \leq \frac{p}{n}.$$

問題1への回答: Average case analysis

問題1 (Recognition)

入力: ビット列 $\mathbf{b} \in \{0,1\}^n$.

質問: $\mathbf{b} \in \mathcal{L}$?

定理 1 (Recognition; 平均時解析)

$\mu = \frac{c}{d} \in (1,2)$ は既約分数とする.

ビット列 $\mathbf{b} \in \{0,1\}^n$ が与えられたとき, $\mathbf{b} \in \mathcal{L}$ を判定可能.

入力 $\mathbf{b}$ が $\mathcal{D}_n$ に従うとき, 期待領域計算量は $O\left(\frac{\log^2 n \log d}{\log^2 \mu}\right)$.

ただし, $\mathcal{D}_n: X \in [0,1]$ を一様として, $\gamma^n(X)$ の従う分布.

μ が実数の場合も同様の事実が得られる (後述) .

μ 有理数は補題2.6でしか使っていない

定理 1の証明

定理 1

入力 $\mathbf{b}$ が $\mathcal{D}_n$ に従うとき, 期待領域計算量は $O\left(\frac{\log^2 n \log d}{\log^2 \mu}\right)$.

証明

補題3.2から以下の主張を示す (次のページ) .

主張 (次のページで示す)

$$E[K_n^2] = O\left(\frac{\log^2 n}{\log^2 \mu}\right)$$

補題 3.2.

$k_q = \lceil \log_\mu n + \log_\mu q^{-1} \rceil$ とおくと,
 $\Pr[K_n \geq k_q] \leq q$.

主張と命題2.6から定理は明らか. $\square$

命題2.6

$\mu = c/d$ は既約分数とする.
判定問題の空間計算量は $O(k^2 \log d)$.
ただし, k は入力 $\mathbf{b}$ が要する最大レベル.

主張の証明

主張

$$E[K_n^2] = O\left(\frac{\log^2 n}{\log^2 \mu}\right)$$

- $k_* = \lceil 3 \log_\mu n \rceil$ とする.

➤ 補題3.2 ($q = \frac{1}{n^2}$ 代入) より $\Pr[K_n \geq k_*] \leq \frac{1}{n^2}$

$$\begin{aligned} & \bullet \quad E[K_n^2] = \sum_{i=1}^n k^2 \Pr[K_n = k] \\ &= \sum_{k=1}^{k_*-1} k^2 \Pr[K_n = k] + \sum_{l=k_*}^n l^2 \Pr[K_n = l] \\ &\leq (k_* - 1)^2 \Pr[K_n \leq k_* - 1] + n^2 \Pr[K_n \geq k_*] \\ &\leq (k_* - 1)^2 * 1 + n^2 \frac{1}{n^2} \\ &= (k_* - 1)^2 + 1 \\ &\leq (\lceil 3 \log_\mu n \rceil - 1)^2 + 1 \\ &= O\left((\log_\mu n)^2\right) \\ &= O\left(\frac{\log^2 n}{\log^2 \mu}\right) \end{aligned}$$

補題 3.2.

$k_q = \lceil \log_\mu n + \log_\mu q^{-1} \rceil$ とおくと,
 $\Pr[K_n \geq k_q] \leq q.$

3.3. 定数アルゴリズム

問題3への回答：定数領域近似

問題3 (計算問題)

入力: 実数 $x \in [0,1)$ と正整数 n .

質問: $\gamma^n(x)$ を求めよ.

定理 3 (計算問題)

$\mu = \frac{c}{d} \in (1,2)$ は既約分数とし, $0 < \epsilon < 1/4$ とする.

実数 $x \in [0,1)$ と正整数 n が与えられたとき,

$\mathbf{b}_n \in \mathcal{L}_n(x, \epsilon)$ を $O\left(\frac{\lg^2 \epsilon^{-1} \lg d}{\lg^2 \mu} + \lg n\right)$ 計算領域で出力可能.

問題3への回答：定数領域近似

問題3 (計算問題)

入力: 実数 $x \in [0,1)$.

質問: $\gamma^\infty(x)$ を求めよ.

定理 3 (計算問題)

$\mu = \frac{c}{d} \in (1,2)$ は既約分数とし, $0 < \epsilon < 1/4$ とする.

実数 $x \in [0,1)$ と正整数 n が与えられたとき,

$\mathbf{b} \in \mathcal{L}(x, \epsilon)$ を $O\left(\frac{\lg^2 \epsilon^{-1} \lg d}{\lg^2 \mu}\right)$ 計算領域で出力可能.

n に対して定数

無限長の入力テープを κ bitだけ読む.

アルゴリズム

Input 実数 $x \in [0,1]$
 Output ビット列 $b_1 b_2 \dots \in \mathcal{L}(x, \epsilon)$
 $\kappa \leftarrow \lceil -3 \lg \epsilon / \lg \mu \rceil$
 $z \leftarrow \langle x \rangle_\kappa$
 オートマトンをレベル 2κ まで構築
 For $i = 1$ to κ
 b_{i-1} と z から b_i を計算
 オートマトンの状態を遷移
 $z \leftarrow \langle f(z) \rangle_\kappa$
 For $i = \kappa$ to ∞
 $T(b_1 \dots b_{i-1} 0)$ と $T(b_1 \dots b_{i-1} 1)$ を比べ
 レベルが低い方のビットを選択

今日は省略

補題 A

任意の l について, $I_l, \dots, I_{l+1}$ のうちの少なくとも一つは backward edge (レベルが下がる遷移) が存在.

主張(次ページで示す)

アルゴリズムは $\mathbf{b} \in \mathcal{L}(x, \epsilon)$ を出力

定理3は主張から明らか.

証明

- $\mathbf{b} \in \mathcal{L}$ は補題Aより明らか.
- $\gamma(x - \epsilon) \leq \mathbf{b} \leq \gamma(x + \epsilon)$ を示す.
 - $\mathbf{b} = b_1 b_2 b_3 \dots$ とする.
 - $x^- = x - \frac{\epsilon}{2}$, $x^{--} = x - \epsilon$ として,
 - $\gamma^\kappa(x^{--}) < b_1 \dots b_\kappa$ を示して下界を示す. (上界も同様)
 - $\gamma^\kappa(x^{--}) < \gamma^\kappa(x^-)$
 - ✓ $|f^\kappa(x^{--}) - f^\kappa(x^-)| > 1$ とテント符号の順序保存の性質より.
 - $\gamma^\kappa(x^-) \leq b_1 \dots b_\kappa$
 - ✓ $\gamma^1(x) \leq \gamma^1(z)$ は明らか.
 - ✓ $\gamma^i(x) = \gamma^i(z)$ である限り, z_i は x_i より「内側」にいることを示す:

■ 主張 $|x_i^- - z_i| \geq \frac{\epsilon}{2}$ (帰納法で示す)

$$\begin{aligned}
 |x_{i+1}^- - z_{i+1}| &= |f(x_i^-) - \langle f(z_i) \rangle_\kappa| \\
 &\geq |f(x_i^-) - f(z_i)| - |f(z_i) - \langle f(z_i) \rangle_\kappa| \\
 &= \mu |x_i^- - z_i| - |f(z_i) - \langle f(z_i) \rangle_\kappa| \\
 &\geq \mu \frac{\epsilon}{2} - \frac{1}{2^\kappa} \geq \mu \frac{\epsilon}{2} - \frac{1}{2^{-3 \lg \epsilon / \lg \mu}} \geq \frac{\epsilon}{2}
 \end{aligned}$$

つまり $x_i^- - z_i$ の距離は一定以上を保っている (「順序」も保存). □

アルゴリズム (有限長バージョン)

Input 実数 $x \in [0,1]$, 自然数 n
 Output ビット列 $b_1 b_2 \cdots b_n \in \mathcal{L}_n(x, \epsilon)$
 $\kappa \leftarrow \lceil -3 \lg \epsilon / \lg \mu \rceil$
 $z \leftarrow \langle x \rangle_\kappa$
 オートマトンをレベル 2κ まで構築
 For $i = 1$ to κ
 b_{i-1} と z から b_i を計算
 オートマトンの状態を遷移
 $z \leftarrow \langle f(z) \rangle_\kappa$
 For $i = \kappa$ to n
 $T(b_1 \cdots b_{i-1} 0)$ と $T(b_1 \cdots b_{i-1} 1)$ を比べ
 レベルが低い方のビットを選択

このカウンタに $\lg n$ bit 必要

補題 A

任意の l について, $I_l, \dots, I_{l+1}$ のうちの少なくとも一つは
 backward edge (レベルが下がる遷移) が存在.

主張

アルゴリズムは $\mathbf{b}_n \in \mathcal{L}_n(x, \epsilon)$ を出力

3.4. 平滑化解析

問題2への回答: Smoothed analysis

問題2 (判定問題)

入力: ビット列 $\mathbf{b}_n \in \{0,1\}^n$ と実数 $x \in [0,1)$.

質問: $\mathbf{b}_n = \gamma^n(x)$?

近似解法

$$\begin{aligned}\mathcal{L}_n(x, \epsilon) &= \{\gamma^n(x') \mid x - \epsilon \leq x' \leq x + \epsilon\} \\ &= \{\mathbf{b}_n \in \mathcal{L}_n \mid \gamma^n(x - \epsilon) \preceq \mathbf{b}_n \preceq \gamma^n(x + \epsilon)\}\end{aligned}$$

定理 2 (判定問題; 平滑化解析)

$\mu = \frac{c}{d} \in (1,2)$ は既約分数とし, $0 < \epsilon < 1/4$ とする.

ビット列 $\mathbf{b}_n \in \{0,1\}^n$ と実数 $x \in [0,1)$ が与えられたとき,

- $\mathbf{b}_n \in \mathcal{L}_n(x, \epsilon) \Rightarrow$ 受理
- $\mathbf{b}_n \notin \mathcal{L}_n(x, 2\epsilon) \Rightarrow$ 拒否

を実現可能. 入力 $\mathbf{b}_n$ が $\mathcal{D}_n(x, \epsilon)$ に従うとき,

期待領域計算量は $O\left(\frac{\log^3 d (\log^2 n + \log^2 \epsilon^{-1})}{\log^4 \mu}\right)$.

ただし, $\mathcal{D}_n(x, \epsilon): X \in [x - \epsilon, x + \epsilon]$ を一様として, $\gamma^n(X)$ の従う分布.

アルゴリズム

Input ビット列 $\mathbf{b}_n = b_1 b_2 \cdots b_n \in \{0,1\}^n$, 実数 $x \in [0,1]$

Output $\mathbf{b}_n \in \mathcal{L}_n(x, \epsilon) \Rightarrow \mathbf{YES}$, $\mathbf{b}_n \notin \mathcal{L}_n(x, 2\epsilon) \Rightarrow \mathbf{NO}$

$\kappa \leftarrow \lceil -3 \lg \epsilon / \lg \mu \rceil$

$z^- \leftarrow \left\langle x - \frac{3}{2}\epsilon \right\rangle_\kappa$

$z^+ \leftarrow \left\langle x + \frac{3}{2}\epsilon \right\rangle_\kappa$

オートマトンをレベル κ まで構築

For $i = 1$ to n

b_{i-1} と z^+ (resp. z^-) から b_i^+ (resp. b_i^-) を計算

If $\mathbf{b}_i^- \leq \mathbf{b}_i \leq \mathbf{b}_i^+$ を満たしていない $\Rightarrow$ Return **NO**

オートマトンの状態を遷移

$z^- \leftarrow \langle f(z^-) \rangle_\kappa$

$z^+ \leftarrow \langle f(z^+) \rangle_\kappa$

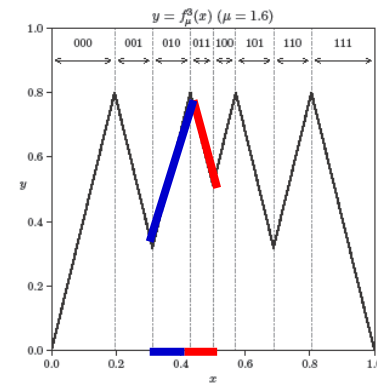
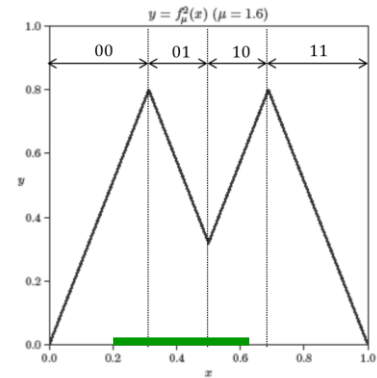
If 現在の状態がオートマトンの最大レベルに到達

次のレベルを構築

Return **YES**

定理2の証明

- 正当性は定数領域計算の証明と同様（省略）
- 計算量は平均時解析と同様!?
- 何が問題か？
 - ✓ 反復が浅いとき、
マルコフ連鎖の推移確率が正しくない。



右図の例

$x = 0.4, \epsilon = 0.2$ の場合 ($X \in [0.2, 0.6]$ u.a.r.)

- $\Pr[b_3 = 1 | \mathbf{b} = 00] = 1 \neq \frac{|T(001)|}{|T(000)| + |T(001)|}$ NG
- $\Pr[b_3 = 0 | \mathbf{b} = 01] = \frac{|T(010)|}{|T(010)| + |T(011)|}$ OK
- $\Pr[b_3 = 0 | \mathbf{b} = 10] > \frac{|T(100)|}{|T(100)| + |T(101)|}$ NG

計算量の証明

X は $[x - \epsilon, x + \epsilon]$ 上の一様確率変数とする.

□ i 回の反復で X は y の周りを包含する

(X **covers** around y at the i -th iteration) :

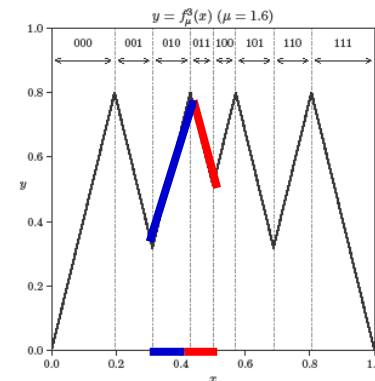
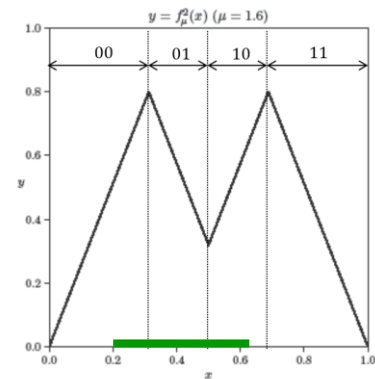
$$S_i(\gamma^i(y)) \subseteq [x - \epsilon, x + \epsilon]$$

□ i 回の反復で X は U を完全包含する

(X **fully covers** $U \subseteq [x - \epsilon, x + \epsilon]$ at the i -th iteration) :

$$\bigcup_{y \in U} S_i(\gamma^i(y)) \subseteq [x - \epsilon, x + \epsilon]$$

$V = \left(x - \left(1 - \frac{1}{n^2}\right)\epsilon, x + \left(1 - \frac{1}{n^2}\right)\epsilon\right)$ とする.



補題3.3.

$l_* = \lceil 2 \log_\mu n + \log_\mu \epsilon^{-1} \rceil$ 回反復の後, X は V を完全包含する.

補題3.4.

$$E[K^2 | X \in V] = O\left(\frac{\log^2 d (\log^2 n + \log^2 \epsilon^{-1})}{\log^4 \mu}\right)$$

定理2の証明

補題3.3.

$l_* = \lceil 2 \log_\mu n + \log_\mu \epsilon^{-1} \rceil$ 回反復の後,
 X は V を完全包含する.

- $l_* = \lceil 2 \log_\mu n + \log_\mu \epsilon^{-1} \rceil$ とすると V は完全包含される.

➤ $X \in V$ の場合は $\Pr[B_n = 0 \mid \mathbf{B}_{n-1} = \mathbf{b}] = \frac{|T(\mathbf{b}0)|}{|T(\mathbf{b}0)| + |T(\mathbf{b}1)|}$ が成り立つ

➤ average case と同様に解析できる.

- $E[K_n^2] = E[K_n^2 \mid X \in V] \Pr[X \in V] + E[K_n^2 \mid X \notin V] \Pr[X \notin V]$

$$\leq E[K_n^2 \mid X \in V] * 1 + \frac{1}{n^2} n^2$$

$$= O\left(\frac{\log^2 d (\log^2 n + \log^2 \epsilon^{-1})}{\log^4 \mu}\right)$$

$V = (x - (1 - \frac{1}{n^2})\epsilon, x + (1 - \frac{1}{n^2})\epsilon)$ より

補題3.4.

$$E[K^2 \mid X \in V] = O\left(\frac{\log^2 d (\log^2 n + \log^2 \epsilon^{-1})}{\log^4 \mu}\right)$$

補題3.3の証明

$$V = \left(x - \left(1 - \frac{1}{n^2} \right) \epsilon, x + \left(1 - \frac{1}{n^2} \right) \epsilon \right)$$

78

補題3.3.

$\lceil 2 \log_{\mu} n + \log_{\mu} \epsilon^{-1} \rceil$ 回反復の後, X は V を完全包含する.

• 背理法で示す:

$\exists y' \notin [x - \epsilon, x + \epsilon], \exists y \in V, \gamma^k(y) = \gamma^k(y')$ とする.

• $y' \notin [x - \epsilon, x + \epsilon]$ と $y \in V$

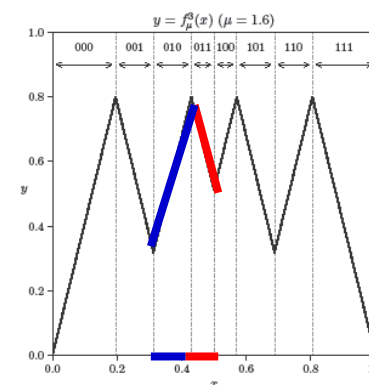
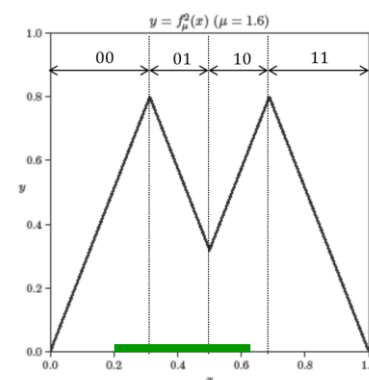
$$\Rightarrow |y - y'| > \frac{\epsilon}{n^2}.$$

• $\gamma^k(y) = \gamma^k(y')$

$$\Rightarrow |f^k(y) - f^k(y')| = \mu^k |y - y'|$$

• $\mu^k |y - y'| \geq \mu^{2 \log_{\mu} n + \log_{\mu} \epsilon^{-1}} |y - y'|$
 $= n^2 \epsilon^{-1} |y - y'| > 1$

• $|f^k(y) - f^k(y')| \leq 1$ に矛盾



補題3.4.

$$E[K^2 | X \in V] = O\left(\frac{\log^2 d (\log^2 n + \log^2 \epsilon^{-1})}{\log^4 \mu}\right)$$

証明の方針

Remark

$\mu \geq \sqrt{2}$ の場合, $\log_{\mu} d \leq 2$ より
 $k_* \leq \lceil 12 \log_{\mu} n + 3 \log_{\mu} \epsilon^{-1} \rceil$

補題3.5. (あとで示す)

$$\begin{aligned} k_* &= \lceil (7 + 3 \log_{\mu} d) \log_{\mu} n + (1 + \log_{\mu} d) \log_{\mu} \epsilon^{-1} \rceil \\ &= O\left(\log_{\mu} d (\log_{\mu} n + \log_{\mu} \epsilon^{-1})\right) = O\left(\frac{\log d (\log n + \log \epsilon^{-1})}{\log^2 \mu}\right) \end{aligned}$$

とおくと $\Pr[K_n \geq k_* | L(Z_t) = l_*] \leq \frac{1}{n^2}$.

を使う.

以下, まず補題3.5 $\Rightarrow$ 補題3.4を示し, その後で補題3.5を示す.

$$\Pr[K_n = k | L(Z_t) = l] \leq \Pr[K_n = k | L(Z_t) = l_*] \text{ for } l \leq l_*$$

補題3.5 $\Rightarrow$ 補題3.4

$$\begin{aligned}
 E[K_n^2 | X \in V] &= \sum_{k=1}^n \sum_{l=1}^{l_*} k^2 \Pr[K_n = k | L(Z_{l_*}) = l] \Pr[L(Z_{l_*}) = l] \\
 &\leq \sum_{k=1}^n k^2 \Pr[K_n = k | L(Z_{l_*}) = l_*] \sum_{l=1}^{l_*} \Pr[L(Z_{l_*}) = l] \\
 &= \sum_{k=1}^{k_*-1} k^2 \Pr[K_n = k | L(Z_{l_*}) = l_*] \\
 &= \sum_{k=1}^{k_*-1} k^2 \Pr[K_n = k | L(Z_{l_*}) = l_*] + \sum_{k=k_*}^n k^2 \Pr[K_n = k | L(Z_{l_*}) = l_*] \\
 &\leq (k_* - 1)^2 \Pr[K_n < k_* | L(Z_{l_*}) = l_*] + n^2 \Pr[K_n \geq k_* | L(Z_{l_*}) = l_*] \\
 &\leq (k_* - 1)^2 * 1 + n^2 \frac{1}{n^2} \\
 &= (k_* - 1)^2 + 1 \\
 &= O(k_*^2)
 \end{aligned}$$



補題3.4.

$$\Pr[K_n \geq k_* | L(Z_{l_*}) = l_*] \leq \frac{1}{n^2}.$$

補題3.5の証明のアウトライン

補題3.5.

$$\begin{aligned} k_* &= \lceil (7 + 3 \log_\mu d) \log_\mu n + (1 + \log_\mu d) \log_\mu \epsilon^{-1} \rceil \\ &= O\left(\log_\mu d (\log_\mu n + \log_\mu \epsilon^{-1})\right) = O\left(\frac{\log d (\log n + \log \epsilon^{-1})}{\log^2 \mu}\right) \end{aligned}$$

とおくと $\Pr[K_n \geq k_* | L(Z_t) = l_*] \leq \frac{1}{n^2}$.

証明のアウトライン

主張 1.

A_t : Z_s がレベル l にいるとき, 時刻 $t > s$ で初めてレベル k ($k > l$) に到達するイベントとすると,

$$\Pr[A_t] \leq \frac{|I_k|}{\mu^{k-l} |I_l|}.$$

主張 2.

$$\frac{|I_{k_*}|}{\mu^{k_*-l} |I_{l_*}|} \leq \frac{1}{n^3}.$$

主張1の証明

主張 1.

A_t : Z_s がレベル l にいるとき, 時刻 $t > s$ で初めてレベル k ($k > l$)に到達するイベントとすると,

$$\Pr[A_t] \leq \frac{|I_k|}{\mu^{k-l}|I_l|}.$$

- $|I_i| = |\bar{I}_i|$ ($i = 1, 2, 3, \dots$)
- レベルが上がるのは $I_i \rightarrow I_{i+1}$ or $\bar{I}_i \rightarrow \bar{I}_{i+1}$

$$\text{確率 } p(I_i, I_{i+1}) = \frac{|I_{i+1}|}{\mu|I_i|} = p(\bar{I}_i, \bar{I}_{i+1})$$

- レベル l に至るまでに, 各 $i = l, l+1, \dots, k-1$ について少なくとも1回 $I_i \rightarrow I_{i+1}$ or $\bar{I}_i \rightarrow \bar{I}_{i+1}$ の推移を要する. よって

$$\begin{aligned} \Pr[A_t] &\leq \prod_{i=l}^{k-1} p(I_i, I_{i+1}) \\ &= \prod_{i=l}^{k-1} \frac{|I_{i+1}|}{\mu|I_i|} \\ &= \frac{|I_k|}{\mu^{k-l}|I_l|} \end{aligned}$$

主張 2.

$$\frac{|I_{k_*}|}{\mu^{k_*-l_*}|I_{l_*}|} \leq \frac{1}{n^3}.$$

主張2の証明

- 背理法： $\frac{|I_{k_*}|}{\mu^{k_*-l_*}|I_{l_*}|} > \frac{1}{n^3}$ と仮定
- $|I_{l_*}| \geq \frac{1}{2d^{l_*}}$
- $k_* - l_* \geq (7 + 3 \log_\mu d) \log_\mu n + (1 + \log_\mu d) \log_\mu \epsilon^{-1} - (3 \log_\mu n + \log_\mu \epsilon^{-1})$
 $= 4 \log_\mu n + (3 \log_\mu n + \log_\mu \epsilon^{-1}) \log_\mu d$
- $|I_{k_*}| > \frac{1}{n^3} \mu^{k_*-l_*} |I_{l_*}| \geq \frac{1}{n^3} \mu^{4 \log_\mu n + (3 \log_\mu n + \log_\mu \epsilon^{-1}) \log_\mu d} \frac{1}{2d^{l_*}}$
 $\geq \frac{1}{n^3} n^4 d^{3 \log_\mu n + \log_\mu \epsilon^{-1}} \frac{1}{2d^{3 \log_\mu n + \log_\mu \epsilon^{-1}}} \geq \frac{n}{2} \geq 1$
- $|I_{l_*}| \leq 1$ に矛盾.

$$k_* = \lceil (7 + 3 \log_\mu d) \log_\mu n + (1 + \log_\mu d) \log_\mu \epsilon^{-1} \rceil$$

$$l_* = \lceil 2 \log_\mu n + \log_\mu \epsilon^{-1} \rceil \leq 3 \log_\mu n + \log_\mu \epsilon^{-1}$$

$$\log_\mu n \geq 1$$

補題3.5の証明

A_t^* : Z_{l_*} がレベル l_* にいるとき, 時刻 $t > l_*$ で初めてレベル k_* に到達するイベントとすると,

$$\begin{aligned} \Pr[K_n \geq k_* | L(Z_S) = l_*] &= \Pr \left[\bigvee_{t=l_*}^n A_t^* \right] \\ &\leq \sum_{t=l_*}^n \Pr[A_t^*] \\ &\leq n \frac{|I_{k_*}|}{\mu^{k_*-l_*} |I_{l_*}|} \\ &\leq n \frac{1}{n^3} \\ &= \frac{1}{n^2} \quad \square \end{aligned}$$

主張 1.

$$\Pr[A_t] \leq \frac{|I_k|}{\mu^{k-l} |I_l|}.$$

主張 2.

$$\frac{|I_{k_*}|}{\mu^{k_*-l_*} |I_{l_*}|} \leq \frac{1}{n^3}.$$

3.5. まとめ

まとめ

1. テント言語 $\mathcal{L}$ を定義
2. $\mathcal{L}_n$ を認識する $O(n)$ 状態のオートマトン
- 3.1. **recognition**の平均時解析
- 3.2. 近似**計算**の定数領域アルゴリズム
- 3.3. 近似**判定**の平滑化解析

今後の課題

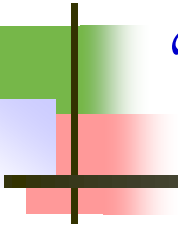
- テント言語の時間計算量 (演習3.1.)
- ロジスティック写像 (演習3.2.)
 - $f_a(x) = ax(1 - x) \quad 0 \leq x \leq 1$
ただし $1 < a < 4$ は定数
- 二次元の区分線形写像 (e.g. Baker's map)

本講義のねらい

- 計算機科学の基礎的な技術を学ぶ
 - 数値計算の計算量解析（の初歩）
 - 言語とオートマトン（の初歩）
 - 非自明アルゴリズムの設計（の例）
 - アルゴリズムの確率的解析（の例）
- 新しい研究課題の開拓事例を見る
- 一緒に研究しませんか？

謝辞

- 共同研究者の岡田真明氏に心より感謝いたします.
- 先行研究「乱択 β 展開」の共同研究者の富田祐作氏にも深く感謝いたします.
- 實松豊先生（九州大学）, 篠原克寿先生（一橋大学）には本研究の入り口となったcompression lemmaのアイデアを教えていただきました. 厚くお礼申し上げます.
- 辻井正人先生（九州大学） にはMarkov extensionの存在を教えていただきました. 感謝いたします.
- 本研究はJSTさがけJPMJPR16E4, JSPS科研費JP21H03396, JP23K21645 の支援を受けました.



The end

Thank you for the attention.