

複雑さの理論 期末練習問題

問 1

次の定義を述べよ.

- (1) リ・ヨークのカオス (2) リアプノフ指数 (3) 時刻 m から n ステップのエントロピー型カオス尺度
(4) 完全守秘性

問 2

パラメータ $a \in [0, 1]$ の 2 進変換

$$x_{n+1} = \begin{cases} 2ax_n & (0 \leq x_n < 0.5) \\ a(2x_n - 1) & (0.5 \leq x_n \leq 1) \end{cases}$$

について, 以下の問いに答えよ.

- (1) 初期値 $x_0 = 0.4$ の軌道のリアプノフ指数を a を用いて表せ.
(2) $a = 1$ のとき, リ・ヨークのカオスであることを示せ.
(3) $a = 1$ のとき, 有理数を初期値とする軌道はカオス軌道となるか調べよ.

問 3

$I = [0, 1]$ の分割を

$$A_1 = [0, 0.25), A_2 = [0.25, 0.5), A_3 = [0.5, 0.75), A_4 = [0.75, 1]$$

とする. 問 2 の 2 進変換について $a = 1$ のとき, 以下の初期値 x_0 の軌道の時刻 $m = 2$ から $n = 10$ ステップのエントロピー型カオス尺度を求めよ. ただし, $\sqrt{2} = 1.41$ とする.

- (1) $x_0 = 0.7$ (2) $x_0 = \frac{\sqrt{2}}{2}$

問 4

暗号系 $\mathcal{C} = (\{a, b\}, \{1, 2, 3, 4\}, \{k_1, k_2, k_3\}, \{E_k\}, \{D_k\})$

$E_k(p)$	a	b	$D_k(c)$	1	2	3	4
k_1	1	3	k_1	a		b	
k_2	2	1	k_2	b	a		
k_3	2	4	k_3		a		b

について, 以下の問いに答えよ.

- (1) 暗号系 \mathcal{C} が暗号系条件を満たすか調べよ.
(2) 以下のとき, 完全守秘性をもつか調べよ.

$$P(a) = \frac{1}{3}, \quad P(b) = \frac{2}{3}$$

$$P(k_1) = \frac{1}{2}, \quad P(k_2) = P(k_3) = \frac{1}{4}$$