

有限分割の Kolmogorov-Sinai エントロピーとカオス尺度

On Kolmogorov-Sinai Entropy in Finite Partitions and Chaos Degree

奥富 秀俊 (Hidetoshi Okutomi)¹, 真尾 朋行 (Tomoyuki Mao)^{1,2}, 梅野 健 (Ken Umeno)²

¹ 東芝情報システム株式会社 (Toshiba Information Systems (Japan) Corporation),

² 京都大学 (Kyoto University)

e-mail : hidetoshi.okutomi@toshiba.co.jp

1 概要

著者らは、カオス尺度を独立したカオスの定量化法として利用できるか否かを探っている．そこで改めて、カオス尺度がどのような量を定量化したものであるかを明確にし、ならびに、既存の定量化法との関係や差分量を明示する研究に取り組んでいる．本稿では、カオス尺度がどのような関係の下での条件付きエントロピーであるかを整理し、また、カオス尺度と Kolmogorov-Sinai エントロピーとの差分量を、有限分割で計測した KS エントロピーの近似関数に対して与える．

2 カオス尺度と分割のエントロピー

(X, \mathcal{F}, μ) を確率空間とする． X の分割 $\mathcal{C} = \{C_1, C_2, \dots, C_M\}$ と $\mathcal{E} = \{E_1, E_2, \dots, E_N\}$ に対して、分割のエントロピーと条件付きエントロピーは以下で定義される．

$$H_\mu(\mathcal{C}) = - \sum_{i=1}^M \mu(C_i) \log \mu(C_i) \quad (1)$$

$$H_\mu(\mathcal{E} | \mathcal{C}) = - \sum_{i=1}^M \sum_{j=1}^N \mu(C_i \cap E_j) \log \frac{\mu(C_i \cap E_j)}{\mu(C_i)} \quad (2)$$

$\tau : X \rightarrow X$ を全射かつ保測の写像とし、時系列データ $\{x_t\}_{t=0}^n$ が τ の反復によって生成されたとする．分割 \mathcal{C} に対する時系列データのカオス尺度は以下で表される [1, 2]．

$$H_{\text{CD}} = - \sum_{i=1}^M \sum_{j=1}^M \mu(C_i \cap \tau^{-1}(C_j)) \log \frac{\mu(C_i \cap \tau^{-1}(C_j))}{\mu(C_i)} \quad (3)$$

条件付きエントロピーの視点では、式 (3) の $\tau^{-1}(C_j)$ が式 (2) の $E_j \in \mathcal{E}$ に対応する．以下において、 $\tau^{-1}(C_j)$ と、 $\tau^{-1}(C_j)$ を元にもつ集合 (による分割) を明示する． \mathcal{C} の要素の逆像をすべて列挙した集合を $\mathcal{C}^{-1} = \{D_1, D_2, \dots, D_N\}$ で表し、さらに、 $\tau(D_k) = C_j$ をみたす D_k を D_t^j ($t = 1, 2, \dots, s(j)$) で表す． $\tau^{-1}(C_j) = \bigcup_{t=1}^{s(j)} D_t^j$ なので、ここで新たな集合 $\overline{\mathcal{C}^{-1}} = \{\bigcup_{t=1}^{s(j)} D_t^j\}_{j=1}^M$ を定義すると、カオス尺度は以下の関係のもとでの条件付きエントロピーであると整理され、分割 \mathcal{C} に対してその τ による像が新たに作る分割のエントロピーの増分と解釈できる [1, 2]．

$$H_{\text{CD}} = H_\mu(\overline{\mathcal{C}^{-1}} | \mathcal{C}) = H_\mu(\overline{\mathcal{C}^{-1}} \vee \mathcal{C}) - H_\mu(\mathcal{C}) \quad (4)$$

また、カオス尺度は、

$$s(i) = - \sum_{j=1}^M \frac{\mu(C_i \cap \tau^{-1}(C_j))}{\mu(C_i)} \log \frac{\mu(C_i \cap \tau^{-1}(C_j))}{\mu(C_i)} \quad (5)$$

$$H_{\text{CD}} = \sum_{i=1}^M \mu(C_i) s(i) \quad (6)$$

と表すことができ、式 (5) の $\mu(C_i \cap \tau^{-1}(C_j))/\mu(C_i)$ は、 C_i の測度が写像 τ によって C_j ($j = 1, 2, \dots, M$) に分配される確率を意味するため、分割区間の測度が写像 τ によって周囲の区間にばら撒かれる様子をエントロピーとして表したものの空間平均という解釈もできる。つまり、初期条件鋭敏性の測度版のようなイメージである。

3 カオス尺度と Kolmogorov-Sinai エントロピーの差分量

(X, \mathcal{F}, μ) を確率空間とする。 X の初期分割 \mathcal{A} と、分割

$$\mathcal{A}_{n-1} \stackrel{\text{def}}{=} \bigvee_{i=0}^{n-1} \tau^{-i}(\mathcal{A}) = \mathcal{A} \vee \tau^{-1}(\mathcal{A}) \vee \tau^{-2}(\mathcal{A}) \vee \dots \vee \tau^{-(n-1)}(\mathcal{A}) \quad (7)$$

に対して、以下の $h_\mu(\tau)$ を Kolmogorov-Sinai エントロピー（以降 KS エントロピーと記す）、あるいは保測変換のエントロピーという [3]。

$$h_\mu(\tau) = \sup_{\mathcal{A}} \lim_{n \rightarrow \infty} \frac{1}{n} H_\mu(\mathcal{A}_{n-1})$$

KS エントロピーには別定義がある [4]。

$$h'_\mu(\tau) = \sup_{\mathcal{A}} \lim_{n \rightarrow \infty} \{H_\mu(\mathcal{A}_n) - H_\mu(\mathcal{A}_{n-1})\} \quad (8)$$

以下の式 (9),(10),(11) の関係から、式 (8) は式 (12) と表せる。

$$\mathcal{A}_{n-1}^{-1} = \tau^{-1}(\mathcal{A}_{n-1}) = \tau^{-1}(\bigvee_{i=0}^{n-1} \tau^{-i}(\mathcal{A})) = \bigvee_{i=1}^n \tau^{-i}(\mathcal{A}) \quad (9)$$

$$\mathcal{A}_n = \bigvee_{i=0}^n \tau^{-i}(\mathcal{A}) = \mathcal{A} \vee \bigvee_{i=1}^n \tau^{-i}(\mathcal{A}) = \mathcal{A} \vee \mathcal{A}_{n-1}^{-1} \quad (10)$$

$$H_\mu(\mathcal{A} \vee \mathcal{A}_{n-1}^{-1}) \rightarrow H_\mu(\mathcal{A}_{n-1}^{-1}) \quad (n \rightarrow \infty) \quad (11)$$

$$h'_\mu(\tau) = \sup_{\mathcal{A}} \lim_{n \rightarrow \infty} \{H_\mu(\mathcal{A}_{n-1}^{-1}) - H_\mu(\mathcal{A}_{n-1})\} \quad (12)$$

ここで \mathcal{A}_{n-1} を任意の分割 \mathcal{C} に置き換えて、KS エントロピーの近似関数を

$$\hat{H}_{\text{KS}} \stackrel{\text{def}}{=} H_\mu(\mathcal{C}^{-1}) - H_\mu(\mathcal{C}) \quad (13)$$

で定義すると、十分に大きい分割数に対して $\hat{H}_{\text{KS}} \sim h'_\mu(\tau)$ が成り立つと想像できる。これより、カオス尺度（式 (3)）と KS エントロピーの近似関数（式 (13)）との差分量が得られる。

$$H_{\text{CD}} - \hat{H}_{\text{KS}} = H_\mu(\overline{\mathcal{C}^{-1}} \vee \mathcal{C}) - H_\mu(\mathcal{C}^{-1}) \quad (14)$$

参考文献

- [1] 奥富 秀俊, 真尾 朋行, 梅野 健, カオス尺度の測度論的視点での再整理, 日本応用数理学会第 21 回研究部会連合発表会, 応用カオス OS, D2-3-3, 2025 年 3 月.
- [2] 奥富 秀俊, 真尾 朋行, 梅野 健, カオス尺度の測度論的な解釈について信学技報, vol. 125, no. 70, CCS2025-21, pp. 79-83, 2025 年 6 月.
- [3] Walters, P., An Introduction to Ergodic Theory. Springer New York, NY, 1982.
- [4] Dorfman, J. R., An Introduction to Chaos in Nonequilibrium Statistical Mechanics, Cambridge University Press, Cambridge, 1999.

周期軌道に着目した順序ネットワークを用いた位相的エントロピーの数値計算

Numerical Calculation of Topological Entropy by Ordinal Partition Network with Periodic Orbits

福島 真太郎 (Shintaro Fukushima)¹, 谷澤 俊弘 (Toshihiro Tanizawa)¹

¹ トヨタ自動車株式会社 (Toyota Motor Corporation)

e-mail : s.fukushima@mail.toyota.co.jp

1 概要

時系列データに対して力学系の複雑さを特徴づけるために、順序パターン (ordinal pattern)[1] を用いて位相的エントロピー [2] を推定する手法が提案されている [3, 4]. しかし、2 次元以上の力学系に適用する際に、推定に必要な順序パターンの個数の見積もりが難しいという課題がある. 本研究では、順序分割ネットワーク (ordinal partition network) を用いた手法 [4] に着目し、周期軌道の情報を利用した推定手法を提案し、その有効性を数値実験により確かめる.

2 提案手法と実験結果

2.1 順序分割ネットワークを用いた手法の課題

順序ネットワーク用いた手法 [4] は、ウィンドウサイズ m の順序パターン間の遷移行列を構成し、その最大固有値の対数を位相的エントロピーとして推定する. Hénon 写像 ($a = 1.4, b = 0.3$) に対して、ある 1 つの初期値から写像を $N = 10^5$ 回反復させて得られる軌道に対して m を変化させたとこ、図 1a を得た. これを見ると、 x 軸と y 軸の両方の順序を考慮した場合は $m \approx 14$, x 軸のみ、または y 軸のみの順序を考慮した場合は $m \approx 24, 25$ において先行研究 [5, 6] で得られた位相的エントロピーの推定値 $h = 0.465$ と比較的近い値が推定されているが、 m がこの値よりも小さい場合は過大に、逆に m が大きい場合は過小に推定されていることがわかる.

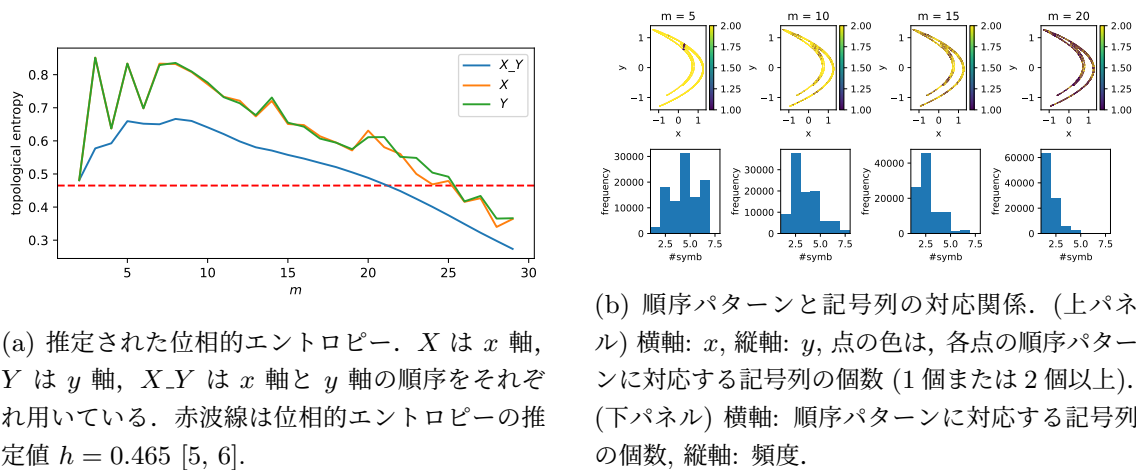


図 1: Hénon 写像に対して順序分割ネットワークを用いた手法 [4] により推定された位相的エントロピー, および順序パターンと記号列の関係

この原因を調べるために、 $m = 5, 10, 15, 20, 25$ に対して順序パターンと記号力学系の記号列 [5] との対応関係を調べた。その結果、図 1b に示すように、 $m = 5, 10, 15$ では 1 個の順序パターンに対して 2 個以上の記号列が対応し、 $m = 20, 25$ では 1 個の記号列が対応する場合が多いことがわかる。

2.2 周期軌道に着目した推定手法

本研究では、不安定周期軌道に着目した推定手法を提案する。そのアイデアは、不安定周期軌道から構成される順序分割ネットワークを基調としつつ、それ以外の軌道から構成される順序分割ネットワークを補足的に用いることにより、順序パターンの遷移の増大率を適切に捉えることにある。具体的には、前者の順序分割ネットワークの隣接行列 A_{upo} と、後者の順序分割ネットワークの隣接行列 A_{ord} を按分した行列 $A = \alpha A_{\text{upo}} + (1 - \alpha) A_{\text{ord}}$ ($\alpha \in (0, 1)$) の最大固有値 λ_{max} に対して、位相的エントロピーを $h = \log \lambda_{\text{max}}$ で推定することである。遷移行列を構成する際は、各順序パターン間での遷移の回数をその最大値で除することにより、遷移行列の各要素の値を $[0, 1]$ に収めている。

周期軌道の検出には再帰的な近傍探索と局所線形近似を組み合わせた手法 [7] を使用し、再帰性の判定に用いる閾値 $\epsilon = 0.05$ 、局所線形近似に用いる近傍の点数 $N_{\text{neigh}} = 12$ を設定し、周期 20 までの周期軌道を検出した。按分の割合 $\alpha = 0.999$ に対して、図 2 を得た。 $m = 5$ から 8 にかけては、先行研究で得られた位相的エントロピーの値 $h = 0.465$ に比較的近い値が得られていることがわかる。

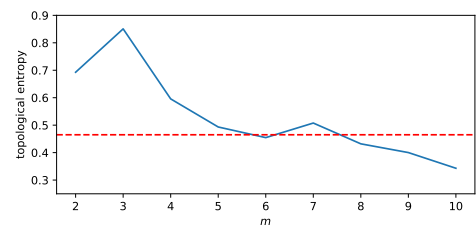


図 2: 提案手法による位相的エントロピーの推定値

参考文献

- [1] J. M. Amigó, Permutation complexity in dynamical systems, Springer, 2010.
- [2] R. L. Adler, A. G. Konheim and M. H. McAndrew, Topological entropy, Trans. Amer. Math. Soc., 114 (1965), 309.
- [3] J. M. Amigó and M. B. Kennel, Topological permutation entropy, Physica D, 231(2) (2007), 137–142.
- [4] K. Sakellariou, T. Stemler and M. Small, Estimating topological entropy using ordinal partition networks, Phys. Rev. E, 103 (2021), 022214.
- [5] Y. Hirata and A. I. Mees, Estimating a generating partition from observed time series: Symbolic shadowing, Phys. Rev. E, 67 (2003), 026205.
- [6] 福島真太郎, 村重淳, 写像により変換された曲線の折返し点を用いた位相的エントロピーの計算, 電子情報通信学会論文誌 A 90 (2007), 932–939.
- [7] P. So, E. Ott, S. J. Schiff, D. T. Kaplan, T. Sauer, and C. Grebogi, Detecting unstable periodic orbits in chaotic experimental data, Phys. Rev. Lett. 76(25) (1996), 4705–4708.

整数化した 4 次元 Lorenz-Stenflo 方程式の 出力値系列に関する乱数性の調査

Investigation of Randomness in The Output Value Series of The Integerized 4D Lorenz-Stenflo Equation

神崎 啓志 (Keishi Kanzaki)¹, 高市 康平 (Kohei Takaichi)¹, 顔錦柱 (Jun-Juh Yan)²,
宮崎 武 (Takeru Miyazaki)³, 上原 聡 (Satoshi Uehara)⁴, 荒木 俊輔 (Shunsuke Araki)¹
¹ 九州工業大学 (Kyushu Institute of Technology)
² 台湾国立勤益科技大学 (National Chin-Yi University of Technology)
³ 九州情報大学 (Kyushu Institute of Information Sciences)
⁴ 北九州市立大学 (The University of Kitakyushu)
 e-mail : kanzaki.keishi997@mail.kyutech.jp

1 はじめに

現代の情報通信において、データの秘匿性を確保するために暗号技術は不可欠である。情報セキュリティ技術にはランダム性を与えるために擬似乱数が欠かせない。そこで我々は、カオス写像に着目した擬似乱数生成器の研究を行っている。この種の多くの研究では、本来の定義通りに浮動小数点演算で計算機実装されている。一方で、浮動小数点演算には、精度がハードウェアや計算環境によって異なるという問題がある。我々のグループでは Lin らが用いた 4 次元 Lorenz-Stenflo 方程式を整数化した手法 [2] を提案した。整数演算のみになることで、環境依存性の低減などの利点があるが、その出力値系列に関する議論はまだ乏しい。本研究では、整数化した 4 次元 Lorenz-Stenflo 方程式における出力値系列の統計的特性を評価した。

2 整数化した 4 次元 Lorenz-Stenflo 方程式

[2] で提案した整数化された 4 次元 Lorenz-Stenflo 方程式について説明する。はじめに、変数とパラメータの整数化方法を式 (1) に示す。

$$x_i = \frac{128X_i}{2^n} - 64, \quad \text{for } i = 1, \dots, 4 \text{ and } X_i \in [0, 2^n]. \quad (1)$$

ただし、 n は演算精度、 x_i は本来の Lorenz-Stenflo 方程式における 4 つの内部変数を示す。これをもとに、整数化した 4 次元 Lorenz-Stenflo 方程式を次の式 (2) に示す。このとき、 $\dot{X}_i(t)$ は微分値を示す。

$$\begin{aligned} \dot{X}_1(t) &= \frac{-AX_1(t) + AX_2(t) + \Lambda X_3(t) - 2^{n-1}\Lambda}{2^n}, \\ \dot{X}_2(t) &= \frac{-DX_1(t) + \Gamma X_2(t) - 128X_1(t)X_4(t) - 2^{n-1}\Gamma}{2^n} \\ &\quad + \frac{2^{n+6}(X_1(t) + X_4(t)) + 2^{n-1}D - 2^{2n+5}}{2^n}, \\ \dot{X}_3(t) &= \frac{-CX_1(t) - 2^n X_3(t) + 2^{n-1}C + 2^{2n-1}}{2^n}, \\ \dot{X}_4(t) &= \frac{128X_1(t)X_2(t) - BX_4(t) - 2^{n+6}(X_1(t) + X_2(t)) + 2^{n-1}B + 2^{2n+5}}{2^n}. \end{aligned} \quad (2)$$

また、パラメータ $(A, B, C, D, \Gamma, \Lambda)$ を本来のパラメータの 2^n 倍した整数値を用いる。

3 写像回数によるビットごとの 0/1 の出現割合

Lorenz-Stenflo 方程式を用いた擬似乱数生成器において、我々は出力値の任意のビットを抽出することを考えている。そのため、出力値系列の値をそれぞれ 2 進数展開した場合に、抽出対象となるビット位置での 0/1 の出現頻度に差がないことは重要な統計的性質である。本稿では、Lorenz-Stenflo 方程式の出力値における、0 と 1 の出現割合に関して議論する。4 次元 Lorenz-Stenflo 方程式のパラメータを $(A, B, C, D, \Gamma, \Lambda) = (11 \times 2^n, 2.9 \times 2^n, 5 \times 2^n, 23 \times 2^n, -1 \times 2^n, 1.9 \times 2^n)$ とし、初期値を $x_i(0) = 20.0$ に設定した。また、演算精度を $n = 15$ 、写像回数を 1000~100000 ステップに設定し、1000 回毎の各写像回数に対する 4 次元 Lorenz-Stenflo 方程式の出力値 X_i の全ビットの 0 の出現割合を求めた。その実験結果を図 1 に示す。実験の結果、全ての内部変数 X_i の、どのビット位置においても写像回数の増加に伴い、各ビット位置の 0 の出現割合がより 50% に収束していることがわかる。これは、十分な写像回数を経ることで、各ビットにおいて 0 と 1 が均等に出現する傾向にあることを示す良い結果である。この結果は特に擬似乱数生成器の品質評価や 4 次元 Lorenz-Stenflo 方程式の出力値系列を解析する上で重要な知見を提供するものである。

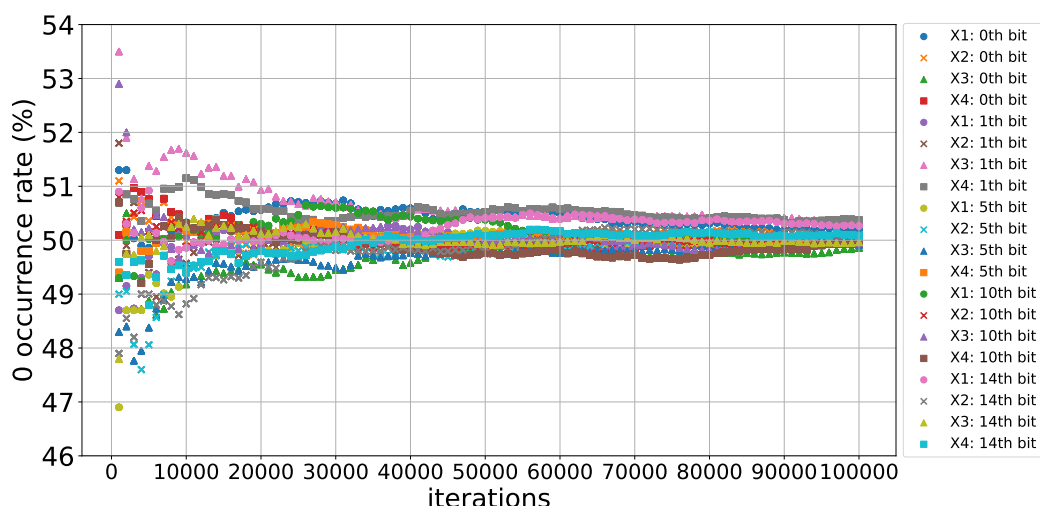


図 1. 写像回数に対するビット毎の 0 の出現割合

4 おわりに

本研究では、整数化した 4 次元 Lorenz-Stenflo 方程式の出力値系列を調査した。写像回数を増加させた場合に出力値の各ビット位置の 0 の出現割合がより 50% に収束する傾向が確認され、写像回数の増加が 4 次元 Lorenz-Stenflo 方程式の出力精度を向上させることがわかった。今後の課題としては、パラメータを変更した際の出力値に関する議論に加え、演算時間や出力値の周期性についても解析する予定である。

参考文献

- [1] C. Lin, G. Hu, J. Chen, and J. Yan, “Novel Design of Cryptosystems for Video/Audio Streaming via Dynamic Synchronized Chaos-Based Random Keys,” *Multimedia Systems*, pp. 1792-1808, 2022.
- [2] 荒木, 高市, 顔, 宮崎, 上原, “擬似乱数生成に向けたローレンツ方程式の整数化に関する研究,” *IEICE Technical Report*, vol. IT2024-22, pp. 48-51, 2024.

整数化した4次元Lorenz-Stenflo方程式を用いた擬似乱数ビット列共有手法における同期に関する一考察

A Study on Synchronization in Pseudo-Random Bit String Sharing Method Using Integerized 4D Lorenz-Stenflo System

高市 康平 (Kohei Takaichi)¹, 顔 錦柱 (Yan Jun-Juh)²,
宮崎武 (Takeru Miyazaki)³, 上原 聡 (Satoshi Uehara)⁴, 荒木 俊輔 (Shunsuke Araki)¹
¹ 九州工業大学 (Kyushu Institute of Technology),
² 国立勤益科技大学 (National Chin-Yi University of Technology),
³ 九州情報大学 (Kyushu Institute of Information Sciences),
⁴ 北九州市立大学 (The University of Kitakyushu)
e-mail : takaichi.kohei283@mail.kyutech.jp

1 はじめに

我々は Lin らにより提案された4次元Lorenz-Stenflo方程式を用いた動的ランダム鍵生成手法 [1] について研究をしている。これはローレンツ方程式を拡張した式である4次元Lorenz-Stenflo方程式を用いて送信者と受信者の方程式にある値を一致させ、その値を共通鍵とするシステムである。Linらの方法では浮動小数点演算はCPUが異なると演算結果に微妙な誤差が生じ、その差が原因で出力値が異なる可能性があり、問題となる。

本稿では上記問題を解消することを目的とした4次元Lorenz-Stenflo方程式の整数化手法について提案するとともに、整数化前後での同期について比較を行い提案手法が有効であることを示す。

2 動的ランダム鍵生成器

動的ランダム鍵生成器は4次元Lorenz-Stenflo方程式とハッシュ関数によって構成されている。動的ランダム鍵生成器の概要を図1に示す。システム内のパラメータは送信側と受信側で同じ値、内部変数は異なる値を持っている。このシステムでは送信側の写像と同時に事前に設計された同期信号がその時の内部変数を基に生成され、受信側に送られる。この写像を繰り返すと受信側の4次元Lorenz-Stenflo方程式の内部変数が漸近的に送信側の4次元Lorenz-Stenflo方程式の内部変数と同じ値をとるようになる。同じ値をとった内部変数をハッシュ関数に通して得られるハッシュ値を共通鍵として秘密通信に用いている。

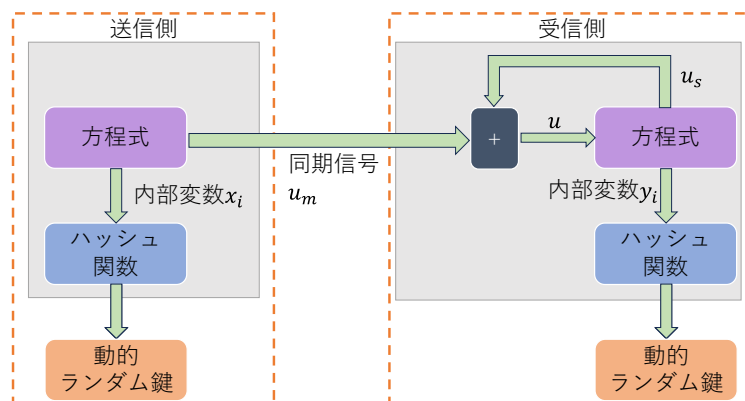


図 1: 動的ランダム鍵生成器の概要

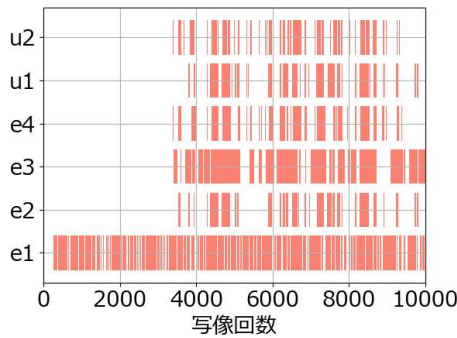
我々は動的ランダム鍵生成器に用いられているローレンツ方程式である 4 次元 Lorenz-Stenflo 方程式を整数化した物を定義し, 用いている. 整数化した 4 次元 Lorenz-Stenflo 方程式を式 (1) に示す.

$$\begin{aligned}
\dot{X}_1(t) &= \frac{-AX_1(t) + AX_2(t) + \Lambda X_3(t) - \Lambda 2^{n-1}}{2^n} \\
\dot{X}_2(t) &= \frac{DX_1(t) - 2^{n-1}D - X_2(t) + 2^{n-1} + 2^{n+6}X_1(t) + 2^{n+6}X_4(t) - 128X_1(t)X_4(t) - 2^{2n+5}}{2^n} \\
\dot{X}_3(t) &= \frac{-CX_1(t) - 2^{n-1}X_3(t) + 2^{n-1}C + 2^{2n-1}}{2^n} \\
\dot{X}_4(t) &= \frac{128X_1(t)X_2(t) - BX_4(t) - 2^{n+6}X_1(t) - 2^{n+6}X_2(t) + 2^{n-1}B + 2^{2n+5}}{2^n}
\end{aligned} \tag{1}$$

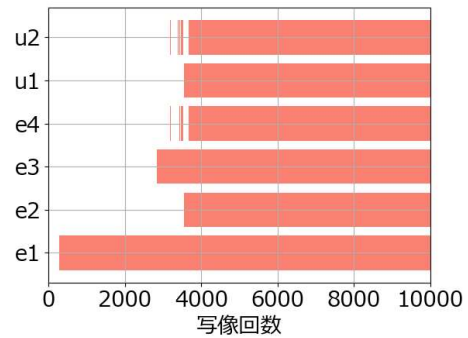
このとき A, B, C, D, Λ はパラメータであり, $\dot{X}_1(t), \dot{X}_2(t), \dot{X}_3(t), \dot{X}_4(t)$ は内部変数の微分値を示している.

3 信号の整数化による同期の安定化

整数化前後で送信側と受信側の内部変数と同期信号が同じ値を取り, 共通の鍵を生成できるか調査を行った. 写像回数毎の各内部変数と各同期信号の値の一致について整数化前の結果を図 2(a) に, 整数化後の結果を図 2(b) に示す. 整数化前は内部変数と同期信号がすべて同じ値をとっていたとしても同期が外れるタイミングが存在するが, 整数化後ではすべての値が一致すると写像を繰り返しても同期が外れないことが確認できる. 整数化を行うと各内部変数の全てのビットが一致するため, 一回の写像でより多い情報量を鍵生成に用いることが可能になっている.



(a) 整数化前の値の一致



(b) 整数化後の値の一致

図 2: 整数化前後での各値の一致について

4 おわりに

本研究では, 4 次元 Lorenz-Stenflo 方程式の整数化に関する議論を行った. Lin らの動的ランダム鍵生成器での利用を想定し, 二者間での擬似乱数列の同期に関する実験を行い, 整数化することで同期の不安定性が解消されることを示した.

参考文献

- [1] C. Lin, G. Hu, J. Chen, J. Yan and K. Tang, “Novel design of cryptosystems for video/audio streaming via dynamic synchronized chaos-based random keys,” *Multimedia Systems*, Vol. 28, pp.1793-1808, 2022.