国立大学法人岩手大学　情報処理センター研究紀要　第 1 号　2013 年　Online edition: ISSN 2188-4811
Bulletin of Iwate University Super Computing and Information Sciences Center, No.1, 2013

カオス・ニューラルネットワークの周期的δ 擬軌道と準安定状態

吉田等明[†1]　　村上武[†2]

限られた精度を持つコンピュータでの計算においては，発生させたカオス軌道の周期を評価することが，予測不可能性が求められる暗号への応用上重要なポイントである．今回，カオス出力の下位ビットを切り捨てることにより周期的δ擬軌道の周期を短周期化し，その周期と過渡集合への滞在時間を実験的に求めた．興味深いことに，δ擬軌道はすぐには周期軌道へと収束せず，長く準安定状態にとどまることを見出した．暗号への応用の際には，周期を持たない準安定状態の存在は非常に重要である．

Periodic δ-Pseudo-Orbit and Metastable State on Chaos Neural Network (CNN)

Hitoaki YOSHIDA[†1] and Takeshi MURAKAMI[†2]

Using a real computer with limited precision, evaluation of the period of the generated chaos orbit is an important key point on the cipher system which needs unpredictability. A period of CNN outputs has been reduced with truncation, and thereby a period of a periodic δ-pseudo-orbit and sojourn time of a transitional δ-pseudo-orbit have been experimentally obtained. It is interesting to note that δ-pseudo-orbit has stayed a metastable state for a long time from a cryptographic standpoint.

1. はじめに

限られた精度を持つコンピュータを用いて，カオス力学系の時間発展を正確に数値計算することは通常困難であることが多い．丸め誤差等の計算時の微小誤差が急激に増加するからである．

Benettin らは，このような計算された軌道を真の軌道に対して擬軌道（pseudo-orbit）と呼んでいる．[1] [2] [3]
以下の差分方程式が，初期値 y_0 に対して，誤差を含まない真の軌道（$\{y_n\} = \{y_0, y_1, y_2, \cdots\}$）を生み出すと仮定する．

$$y_{n+1} = F(y_n) \tag{1}$$

δ擬軌道($\{x_n\} = \{x_0, x_1, x_2, \cdots\}$)とは，全ての n に対して，

$$|F(x_n) - x_{n+1}| < \delta \tag{2}$$

を満たすものである．[1][2][3][4]

カオス軌道は周期を持たないが，全ての擬軌道は終局周期的(eventually periodic)である．よって，全てのδ擬軌道は遷移を繰り返した後に，周期的δ擬軌道に吸引される．ある正の整数 p に対して，$x_{n+p} = x_n$ を満たすものは周期的δ 擬軌道と呼ばれている．[3]　しかし実際には，きわめて長い周期を持つ場合，数値計算で実証的に周期を持つことを証明することは容易ではない．

†1 岩手大学情報メディアセンター
Super Computing and Information Sciences Center, Iwate University
†2 岩手大学工学部技術室
Technical Division, Iwate University

我々は独自のカオス系であるカオス・ニューラルネットワーク（CNN）を開発し，[5]　暗号化製品（CVC）などに応用してきている．[6][7][8]　用いたニューロンモデルを図 1，式(3)～(5)に示す．ここではシグモイド関数（式(4)）を非線形関数として用いている．[9]　我々は，このニューロンモデルを 4 個用いて（N1～N4），カオス出力を得るためのカオス・ニューラルネットワーク(CNN)を構成している．（図 2）

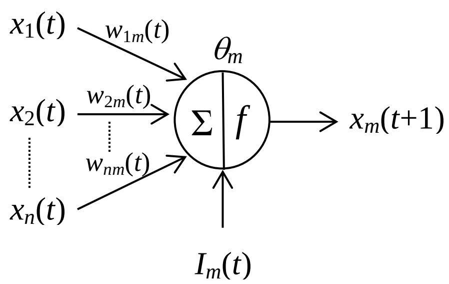

図 1　ニューロンモデル
Figure 1　Neuron Model.

$$x_m(t+1) = f(u_m) \tag{3}$$

$$f(u_m) = \frac{1}{1+\exp(-\lambda u_m)} \tag{4}$$

$$u_m = \sum_{i=1}^{N} w_{im} x_i(t) - \theta_m + I_m \tag{5}$$

ここで，各変数を以下のように定義する．

$x_i(t)$: 時刻 t におけるニューロン i の出力（内部状態）
u_m : ニューロン m への入力と閾値の総和
λ: シグモイド関数 f の傾き係数
w_{im} : ニューロン i からニューロン m への重み係数
I_m : ニューロン m への外部入力値
θ_m : ニューロン m の閾値
N : ニューロンの個数

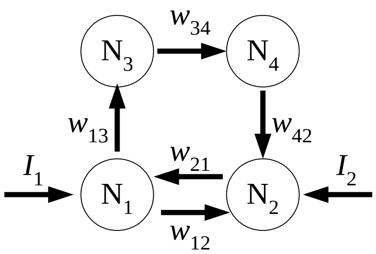

図 2　本研究で用いたカオス・ニューラルネットワーク (CNN)の構成
Figure 2　Structure of Chaos Neural Network (CNN) in this work.

CNN の状態($\boldsymbol{x}$)は，4 つのニューロンの内部状態を独立変数として，$\boldsymbol{x} = (x_1, x_2, x_3, x_4)$と表すことができる．その軌道は 4 次元空間内の軌道となる．

本研究では，CNN のδ擬軌道が，周期的δ擬軌道へ吸引される過渡状態について研究し，中間に非周期的な準安定状態を見出したので報告する．

2.　カオス出力の暗号への応用

我々の暗号化製品（CVC）は，CNN からのカオス出力から疑似乱数列を取り出すことによって，暗号へ応用している．[6][8]　その疑似乱数列の性質は，NIST800-22 によって統計的に良好であることを確認している．NIST800-22 利用上の問題点に関しても検討を行い，より良い利用方法について提案している．[11]

しかしながら，計算機で有限の精度で計算を行っている限り，CNN から得た疑似乱数列もまた周期を持つことになる．予測不可能性が要求される暗号系にとって，これは問題点となりえる．

double 型変数を用いた場合の通常の CNN の周期は，10^{18} 以上の場合もあり，その性質を計算機実験するのは時間的な制約から難しい．そこで今回は，CNN 出力の下位 24 bit あるいは 16 bit を切り捨てて，意図的に CNN 出力の周期を低下させて実験を行った．切り捨てビットの長さと反比例して，周期が短くなることは以前報告している．[9]

δ擬軌道の実例としては，ある精度δの丸め誤差を持つ式(6)の計算が挙げられる．

$$x_{n+1} = \delta \mathrm{Int}\,[F(x_n)/\delta] \tag{6}$$

ここで，Int (z)は，z の整数部分に等しい．

我々が扱っている CNN 出力はシグモイド関数の出力であるので(0,1)の範囲の有界な軌道である．24 bit 切り捨ての場合の最大の丸め誤差は，2^{-29} であるので，今回我々の扱っている系では$\delta = 2^{-29}$（あるいはδ=1.863×10^{-9}）として扱う．δ の求め方については付録に示した．

2.1　ω極限集合とδ擬軌道の距離

次に，v_0 を初期値とする軌道$\{f^n(v_0)\}$の前方極限集合（ω極限集合）とは，以下の集合である．

$\omega(v_0)$={v: 任意の N と任意のεに対して，｜$f^n(v_0)$ - v｜< ε を満たす $n > N$ が存在する}　(7)

また，$\{f^n(v_0)\}$がカオス軌道であり，$v_0 \in \omega(v_0)$　である場合，$\omega(v_0)$はカオス集合と呼ばれる．[4]

周期軌道の前方極限集合は周期軌道自身であるから，周期的δ擬軌道の前方極限集合も，周期的δ擬軌道自身である．

この周期的δ擬軌道上の点からなる前方極限集合$\omega(v_0)$へどれだけ近づいているかを調べるために，集合と軌道の距離を考える．

まず，距離空間内の 2 つの集合 A と集合 B の間の距離 d(A,B)は，以下のように定義できる．

$$d(\mathrm{A},\mathrm{B}) = \inf\,\{d(a,b) \mid a \in \mathrm{A},\ b \in \mathrm{B}\} \tag{8}$$

ここで，集合 B は時刻 t において 1 点 $b(t)$からなる集合とすると，

$$d(\mathrm{A},b(t)) = \inf\,\{d(a, b(t)) \mid a \in \mathrm{A}\} \tag{9}$$

この距離 d は，時間 t によって変化する関数となる．

この定義に基づいて，δ擬軌道上の点（$b(t)$）と周期的δ擬軌道上の点の集合（A）との距離 d を考え，これによって過渡状態の性質を探っていく．

CNN の初期値を $\boldsymbol{x}_0 = (x_1, x_2, x_3, x_4)$とし，そこから出発する$\delta$擬軌道を考えることとする．CNN 出力は有界であるので前方極限集合の存在性により，前方極限集合$\omega(\boldsymbol{x}_0)$は必ず存在する．CNN のδ擬軌道（丸め誤差から，$\delta = 2^{-29}$ととれる）は，終局周期的（eventually periodic）であり，いずれは周期的δ擬軌道に落ち込む．周期的δ擬軌道の前方極限集合は周期的δ擬軌道自身である．この前方極限集合と，同じ初期値を持つ軌道$\{\boldsymbol{x}(t)\}$上の一点 $\boldsymbol{x}(t)$の時刻 t におけるユークリッド距離 d を考えると，以下のようになる．

$$d(\omega(\boldsymbol{x}_0), \boldsymbol{x}(t)) = \inf\,\{d(\boldsymbol{c}, \boldsymbol{x}(t)) \mid \boldsymbol{c} \in \omega(\boldsymbol{x}_0)\} \tag{10}$$

次に，前方極限集合$\omega(\boldsymbol{x}_0)$とδ擬軌道$\{\boldsymbol{x}(t)\}$の距離は，前方極限集合と 1 点集合の閉包性から，最小値に等しい．従って時刻 t における距離は，式(11)で表すことができる．

$$d(\omega(\boldsymbol{x}_0), \boldsymbol{x}(t)) = \min\{d(\boldsymbol{c}, \boldsymbol{x}(t)) \mid \boldsymbol{c} \in \omega(\boldsymbol{x}_0)\} \quad (11)$$

予想される CNN のδ 擬軌道の時間変化の模式図を図 3 に示す．周期的δ擬軌道の周期を p，過渡状態に滞在する時間を q とする．暗号に利用できるのは $p+q$ から初期状態（通常 1000 単位時間）を取り除いた時間の間に発生させた乱数ということになるため，暗号への応用上も q の長さは重要である．ここで，過渡状態の点の集合を過渡集合（transitional set）と呼び，Q で表すことにする．

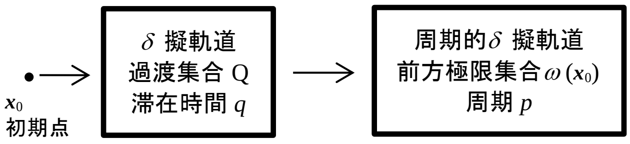

図 3　CNN のδ 擬軌道の時間変化の模式図

Figure 3　Time Course of δ-Pseudo-Orbit of CNN.

初期値 $\boldsymbol{x}_0$=(0, 0, 0, 0)とした時の距離 $d(\omega(\boldsymbol{x}_0), \boldsymbol{x}(t))$の時間変化は以下のようになる．また，前方極限集合$\omega(\boldsymbol{x}_0)$と$\delta$擬軌道の距離 $d(\omega(\boldsymbol{x}_0), \boldsymbol{x}(t))$の度数分布を図 4 に示す．

1) t=0 の時，初期点 $\boldsymbol{x}_0$ から軌道がスタートする．

2) t=1-4 では，急激に距離 $d(\omega(\boldsymbol{x}_0), \boldsymbol{x}(t))$が減少し，これ以後は d_1 より大きくならない．（過渡集合 Q_1）

3) t=5-287529 という長い時間，範囲 $(d_2, d_1)=(1.8\times10^{-6}, 2.2\times10^{-2})$の間に留まる．（過渡集合 Q_2）

即ち，周期的δ 擬軌道から 2.254×10^{-3} を最頻値 d_{mode} として，範囲 (d_2, d_1)の間を増減しながら動き続ける．これはこれまで予想できなかった興味深い結果である．この準安定状態に対応する過渡集合を Q_2，それに達するまでの過渡集合を Q_1 と呼び，Q_2 以後周期的δ 擬軌道までの間の過渡集合を Q_3 と呼ぶことにする．(図 4)

d_1 は，それ以後は d_1 より大きくならず，かつ準安定な過渡集合 Q_2 に属するようになる境界の点で，集合 Q_1 と集合 Q_2 の距離の中点と定義する．

4)　t=287530-287542　距離が一旦 d_2 以下になると，再び d_2 以上になることはない．（過渡集合 Q_3）

d_2 は，それ以後は d_2 より大きくならず，かつ過渡集合 Q_3 に属するようになる境界の点で，集合 Q_2 と集合 Q_3 の距離の中点と定義する．

5) t=287543 において周期的δ 擬軌道へ達し，これ以降は $d(\omega(\boldsymbol{x}_0), \boldsymbol{x}(t))=0$　となる．この時の周期は，p=40621 である．

過渡集合 Q_1, Q_2, Q_3 への滞在時間を，それぞれ q_1, q_2, q_3 とすると，　$q_1 = 4$, $q_2 = 287525$, $q_3 = 13$　である．

図 6，図 7 に示すように，これ以外のパラメータで時間変化を調べた時にも同様の過渡集合 Q_1〜Q_3 が観測され，長時間に渡り，準安定状態に対応する過渡集合 Q_2 に留まることが示された．

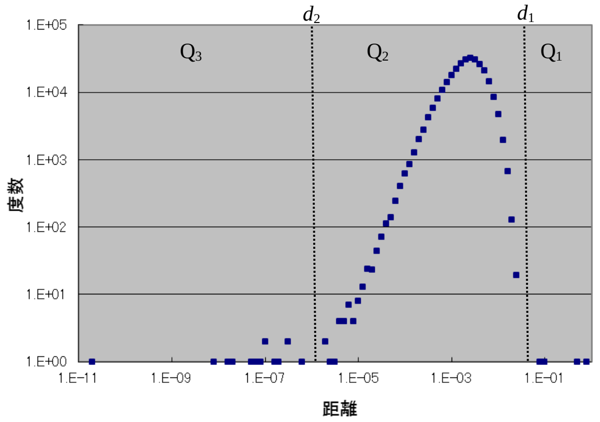

図 4　前方極限集合とδ擬軌道の距離 d の度数分布

Figure 4　Frequency Distribution of the Distance d between Omega Limit Set $\omega(\boldsymbol{x}_0)$ and δ-Pseudo-Orbit.

前方極限集合$\omega(\boldsymbol{x}_0)$とδ擬軌道の距離 $d(\omega(\boldsymbol{x}_0), \boldsymbol{x}(t))$を測定した際に使用した前方極限集合$\omega(\boldsymbol{x}_0)$の点の分布を図5に示す．即ち，式(11)で表される c のうち最小の距離 d を与えた点の度数をプロットしたものである．

このように，度数こそ異なってはいるが，前方極限集合$\omega(\boldsymbol{x}_0)$内の点の近くをくまなく巡っているものと思われる．

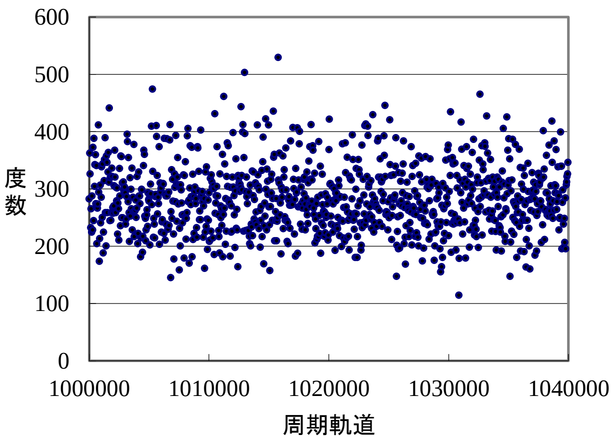

図 5　距離 $d(\omega(\boldsymbol{x}_0), \boldsymbol{x}(t))$の測定に使用した前方極限集合$\omega(\boldsymbol{x}_0)$上の点の度数分布

Figure 5　Frequency Distribution of the Points within Omega Limit Set $\omega(\boldsymbol{x}_0)$ that Are Used for Measuring the Distance, $d(\omega(\boldsymbol{x}_0), \boldsymbol{x}(t))$.

2.2　初期値の効果

この過渡集合 Q_2 に留まる時間が長くなるように制御することができれば，実質的により多くの乱数系列を暗号化に利用することが可能となるであろう．

次に表 1 のように，シグモイド関数の傾きや初期値をパラメータとして変化させて，同様の検討を行った．ここで切り捨てビットは 16bit を用いた．No.1～No.7 のどの場合においても，過渡集合 Q_2 が存在する．16bit 切り捨ての場合の最大の丸め誤差は，2^{-37} であるので，今回我々の扱っている系では$\delta = 2^{-37}$(あるいはδ=7.276×10^{-12}) として扱う．

表 1 の No.1～No.4 では，初期値 $\mathbf{x}_0$ を変えても同じ周期を持つ周期的δ 擬軌道に吸引された．しかしこの場合は，過渡集合 Q_2 への滞在時間 q_2 が異なる結果が得られてきた．興味深いことにこの時，最頻値は全て同じ距離 d_{mode}＝2.84×10^{-4} を取る．（図 6，表 2）

表 1　実験に用いたパラメータと周期的δ擬軌道の周期 p 及び過渡集合 Q_2 への滞在時間 q_2

Table 1　Experimental Parameters, Period of Periodic δ-Pseudo-Orbit p and Sojourn Time q_2 in Transitional Set Q_2 .

No.	λ	初期値 $\mathbf{x}_0$	p	q_2	p+q_2
1	0.99	(0.5,0.5,0.5,0.5)	4431435	1398623	5830058
2	0.99	(0,0,0,0)	4431435	2100438	6531873
3	0.99	(0.1,0.1,0.1,0.1)	4431435	2283987	6715422
4	0.99	(0.9,0.9,0.9,0.9)	4431435	2643339	7074774
5	0.996	(0.9,0.9,0.9,0.9)	621431	1223510	1844941
6	0.995	(0.1,0.1,0.1,0.1)	1326377	1572563	2898940
7	1.0	(0.9,0.9,0.9,0.9)	5413897	1886866	7300763

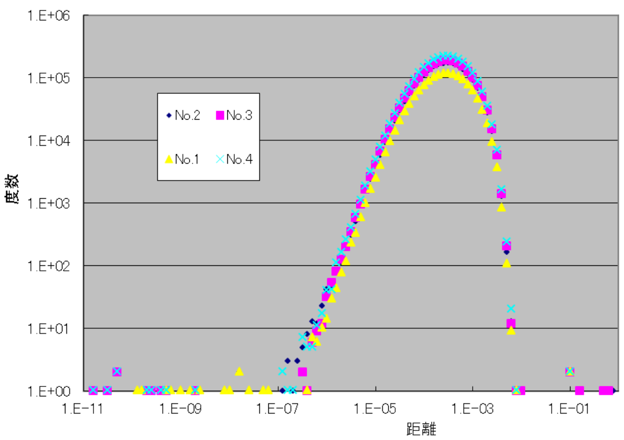

図 6　表 1 のパラメータ No.1～No.4 を用いた実験での前方極限集合$\omega(\mathbf{x}_0)$とδ擬軌道の距離 d の度数分布

Figure 6　Frequency Distribution of the Distance d between Omega Limit Set $\omega(\mathbf{x}_0)$ and δ-Pseudo-Orbit using Parameter No.1-No.4 (Table1).

No.5～No.7 のパラメータを用いた場合には，別々の周期を持つ異なる周期的δ 擬軌道に吸引された．また，過渡集合 Q_2 への滞在時間 q_2 も異なるという結果が得られてきた．周期的δ擬軌道の周期 p が大きいほど，最頻値は小さい距離の方へシフトしている．（図 7，表 2）

このように，p と q_2 は通常同オーダーであり，$p > q_2$ の場合も，$p < q_2$ の場合もありえる．暗号に応用する際には，双方を考慮する必要があると考えられる．

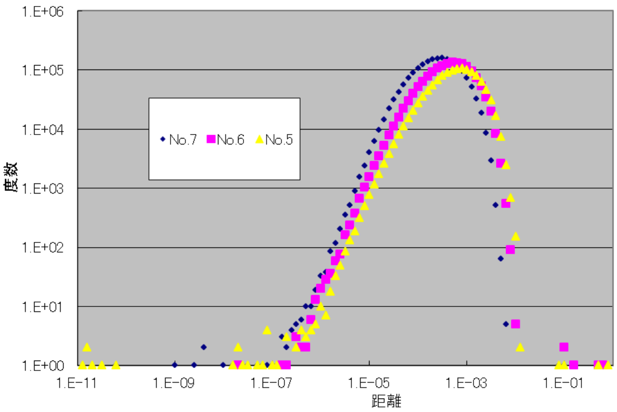

図 7　表 1 のパラメータ No.5～No.7 を用いた実験での前方極限集合$\omega(\mathbf{x}_0)$とδ擬軌道の距離 d の度数分布

Figure 7　Frequency Distribution of the Distance d between Omega Limit Set $\omega(\mathbf{x}_0)$and δ-Pseudo-Orbit using Parameter No.5-No.7 (Table1).

表 2　実験に用いたパラメータと周期的δ擬軌道の周期(p)及び最頻値

Table 2　Experimental Parameters, Period of Periodic δ-Pseudo-Orbit p and Mode of the Distance d_{mode}.

No.	λ	初期値 $\mathbf{x}_0$	p	最頻値 d_{mode}
1	0.99	(0.5,0.5,0.5,0.5)	4431435	2.84×10^{-4}
2	0.99	(0,0,0,0)	4431435	2.84×10^{-4}
3	0.99	(0.1,0.1,0.1,0.1)	4431435	2.84×10^{-4}
4	0.99	(0.9,0.9,0.9,0.9)	4431435	2.84×10^{-4}
5	0.996	(0.9,0.9,0.9,0.9)	621431	7.13×10^{-4}
6	0.995	(0.1,0.1,0.1,0.1)	1326377	4.50×10^{-4}
7	1.0	(0.9,0.9,0.9,0.9)	5413897	2.84×10^{-4}

2.3　周期的δ擬軌道と過渡集合 Q_2 の性質

典型的な例として，短周期（p=128244）の周期的δ擬軌道が作る前方極限集合と，過渡集合 Q_2 を図 8 と図 9 に示す．また，長周期（p=2654009580）の周期的δ擬軌道が作る前方極限集合と，過渡集合 Q_2 を図 10 と図 11 に示す．

周期の有無，周期や滞在時間の長短に関わらず 4 つともほぼ同じ値で，最大 Lyapunov 指数は約 0.2，相関次元は約 2.2 であった．最大 Lyapunov 指数が正の値を取っていることから，カオスに特徴的な初期値鋭敏性を有することが示唆される．[12][13]

また 4 つとも，アトラクタは 4 次元位相空間上で，カオス特有の折り畳み構造を持ったシート状の形状をしており，単純な閉曲線とも違い，相関次元は約 2.2 と非整数値である．カオスに特有のストレンジ・アトラクタであると考えて矛盾ない．この 4 つの異なるアトラクタを，見た目の形状から区別するのは困難である．(図 8〜図 11) 尚，ここで 4 次元目の座標は，色彩で表現している．

4 つの軌道は，初期値や時間が異なるだけで，同じ力学系 f に属しており，Lyapunov 指数は同じであっても矛盾ない．

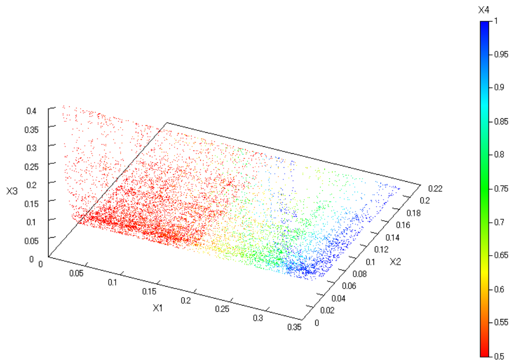

図 8　短周期の周期的δ擬軌道が作る前方極限集合

Figure 8　Omega Limit Set Based on Short Periodic δ-Pseudo-Orbit.

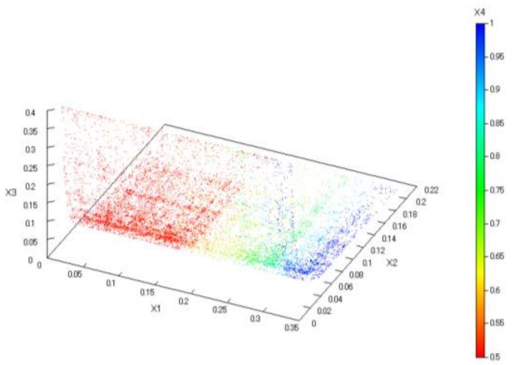

図 9　短周期の周期的δ擬軌道に対応する過渡集合 Q_2

Figure 9　Transitional Set Q_2 Corresponding to Short Periodic δ-Pseudo-Orbit.

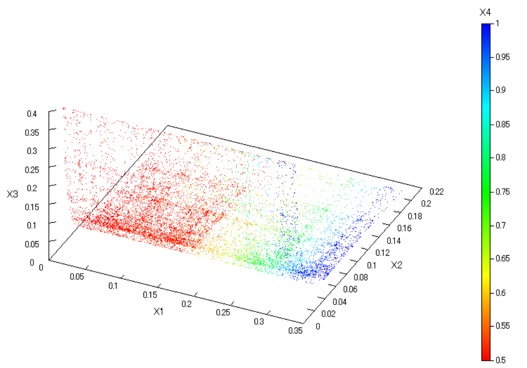

図 10　長周期の周期的δ擬軌道が作る前方極限集合

Figure 10　Omega Limit Set Based on Long Periodic δ-Pseudo-Orbit.

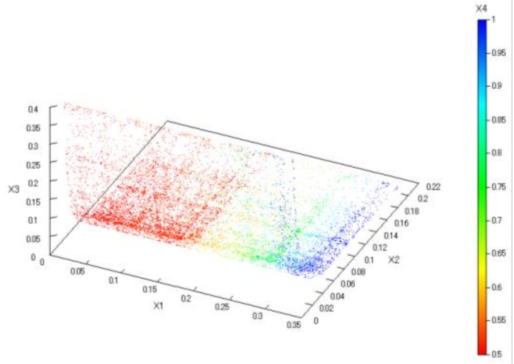

図 11　長周期の周期的δ擬軌道に対応する過渡集合 Q_2

Figure 11　Transitional Set Q_2 Corresponding to Long Periodic δ-Pseudo-Orbit.

3.　結論

CNN 出力の下位ビットを切り捨てることにより短周期化し，周期的δ擬軌道の周期 p と過渡集合 Q への滞在時間 q を，実験的に求めることができた．この際，δ擬軌道が長く準安定状態にとどまることを見出した．この準安定状態にある点の集合を過渡集合 Q_2 と名付け，その滞在時間 q_2 を実験的に求めた．調べた範囲内では，p と q_2 は通常同オーダーであった．

前方極限集合$\omega(\mathbf{x_0})$と過渡集合 Q_2 はそれぞれカオスアトラクタ（ストレンジ・アトラクタ）に特徴的な構造を持ち，また対応するそれぞれの軌道はカオスに特徴的な初期値鋭敏性を持っていることを示唆する結果を得た．このように前方極限集合$\omega(\mathbf{x_0})$と過渡集合 Q_2 を，周期以外で区別することは難しいため，一般に計算機で発生させたカオスが非常に長い周期を持つ場合には，周期的δ擬軌道と過渡集合を区別せずに議論が行われているケースがあるものと思われる．

次にδ擬軌道が前方極限集合$\omega(\mathbf{x_0})$へ吸引される様子であるが，以下の様な予想を超えた奇妙なものである．

1) 漸近的に少しずつ距離が減少して近づくのではない．
2) ある瞬間に突然，前方極限集合$\omega(\mathbf{x_0})$に達するのではない．
3) 一旦，準安定な過渡集合 Q_2 へ吸引され，軌道は前方極限集合$\omega(\mathbf{x_0})$の近く（d_{mode} を最頻値として）をしばらく巡回する．

あたかも，この δ擬軌道こそがカオス軌道であるかのように振る舞うが，何かのきっかけで周期的δ擬軌道へトラップされてしまう．トラップされる際も同様に，少しずつ漸近的に$\omega(\mathbf{x_0})$に近づくのではなく，ある瞬間に突然 Q_2 から$\omega(\mathbf{x_0})$に達するのでもない．トラップ領域に侵入した点がアトラクタに吸引される時のように，多少の増減を繰り返しながら近づいていく．

4.　今後の課題と提案

以上の結果は, 過渡集合 Q_2 の性質がカオス的であるということを強く示唆するものである．周期的δ擬軌道と異なり，周期も持たないため，暗号に応用するのは実用的に可能と期待できる．つまり，できるだけ長時間，軌道が過渡集合 Q_2 に留まり，周期的δ擬軌道へトラップされないように制御できれば良い．

一例を提案すると，初期条件(x_1, x_2, x_3, x_4 やλなど)が変わると様々な過渡集合 Q が得られるが，中には等しいものもありえる．初期条件をγ, カオス軌道を与える初期条件の集合をΓとすると（$\gamma \in \Gamma$），Γを添字集合として過渡集合 Q 全体が作る集合族$\{Q_\gamma\}_{\gamma \in \Gamma}$ を考えることができる．その集合族を改めて $\mathbb{Q}$ と書き表す．

ここでもし $\mathbb{Q}$ が不変集合となるように以下の式(12)を満たす力学系 g を適切に決めてやれば，周期的δ擬軌道にトラップされることを阻止できると考えられるため，暗号に応用した際の有効性が大いに期待できる．すなわち，過渡集合の集合族の中で写像を繰り返す g を f の代わりに用いることにより，前方極限集合へ吸い込まれて周期を持つことを阻止する．詳細については，次回以降の論文で報告する予定である．

$$g(\mathbb{Q})=\mathbb{Q} \qquad (12)$$

謝辞　本研究は，岩手大学情報処理センターが運用する高速計算サーバ，日本 SGI 製 Altix3700（Intel Itanium2 1.5GHz）を利用して行った研究である．運用及び維持管理に尽力しておられる情報処理センタースタッフ諸氏に深く感謝の意を表します．

参考文献

1)　Benettin, G.A., Casartelli, G.M., Galgani, L., Giorgilli, A. and Strelcyn, J.M.: On the reliability of numerical studies of Stochasticity. I: Existence of Time Averages, Nuovo Cimento 44B, pp.183-195 (1978).
2)　Jackson, E. A.: Perspectives of Nonlinear Dynamics: Volume 1, Cambridge University Press (1989).
3)　国府 寛司: 力学系の基礎 (カオス全書), 朝倉書店, p.15 (2000).
4)　Alligood, K.T., Sauer, T.D. and Yorke, J.A.: Chaos- An Introduction to Dynamical Systems, Springer (1997).　Alligood, K.T., Sauer , T.D. and Yorke, J.A., 津田 一郎(監訳): カオス第 1～3 巻，力学系入門，シュプリンガー・ジャパン (2006).
5)　Yoshida, H., Yoneki K., Tsunekawa, Y. and Miura, M.: Chaos Neural Network, Proc, of ISPACS'96, Vol.1 of 3, pp.16.1.1-16.1.5 (1996).
6)　Kawamura, S., Yoshida, H., Miura, M. and Abe, M.: Implementation of Uniform Pseudo Random Number Generator and Application to Stream Cipher based of Chaos Neural Network, the International Conference on Fundamentals of Electronics, Communications and Computer Sciences, R-18, Tokyo, Japan (2002).
7)　吉田等明，中西貴裕: 暗号化システム，特許第 4586163 号（特許登録日 2010/9/17），出願人 国立大学法人岩手大学 (2005).　製品の一例は，J-Crypt < http://www.adtek.co.jp/seihin/J-crypt/>
8)　吉田等明, 村上武: 擬似乱数生成システム, 特願 2010-111688, 出願人 国立大学法人岩手大学 (2010).
9)　吉田等明，村上武，川村暁: カオス・ニューラルネットワークから発生させた周期的δ擬軌道に関する研究，電子情報通信学会技術研究報告，NLP2008-51, pp. 31-34 (2008).
10)　蛎崎哲也，吉田等明: 近傍集合を用いたカオス時系列の過渡状態に関する研究，電子情報通信学会技術研究報告，NLP2008-50, pp. 25-30 (2008).
11)　吉田等明，村上武，川村暁: NIST SP800-22 rev.1a による疑似乱数の検定に関する一考察，信学技法，NLP2012-78，pp.13-18 (2012).
12)　Wolf, A., Swift, J.B., Swinney, H.L. and Vastano, J.A.: Determining Lyapunov exponents from a time series, Physica 16D, pp.285-317 (1985).　Sato, M. and Sawada, Y.: Measurement of the Lyapunov Spectrum from a Chaotic Time Series, Physical Review Letters, Vol.55, No.10, pp. 1082-1085 (1985).
13)　山田泰司，合原一幸 : リカレンスプロットと 2 点間距離分布による非定常時系列解析，電子情報通信学会論文誌 A, Vol.J82-A, No.7, pp.1016‑1028 (1999).　Galka, A., Maass, T. and Pfister, G.: Estimating the dimension of high-dimentional attractors: A comparison between two algorithms, Physica D, Vol.121, pp.237-251 (1998).
14)　IEEE Computer Society (August 29, 2008), IEEE Standard for Floating-Point Arithmetic, IEEE, doi:10.1109/IEEESTD.2008.4610935, IEEE Std 754-2008.

付録

本研究でのδ 値の求め方を以下に示す．

実験に用いた C 言語の double 型変数が表す 10 進数は，

$$(-1)^{符号部} \times 2^{(指数部-1023)} \times 1.仮数部$$

の形になる．[14]
シグモイド関数の出力は 1 未満であるから，指数部の最大値は 1022 であり，この時に丸め誤差が最大になる．以下で仮数部も含めた丸め誤差を見積もる．

(i) 下位 24 bit を切り捨てた場合
下位 24 bit が 2 進表記で全て 1 である数を丸めた時に誤差は最大となる．よって，

$$\delta = 2^{(1022-1023)} \times (2^{-29} + 2^{-30} + 2^{-31} \ldots + 2^{-50} + 2^{-51} + 2^{-52})$$

$$\delta = (2^{-30} + 2^{-31} + 2^{-32} \ldots + 2^{-51} + 2^{-52} + 2^{-53})$$

大きめに見積もると，一番近い 2 のべき乗より，
$\delta = 2^{-29} > (2^{-30} + 2^{-31} + 2^{-32} \ldots + 2^{-51} + 2^{-52} + 2^{-53})$
とすることができる．

10 の累乗で表すと，
$2^{-29} = 1.86264 \cdots \times 10^{-9} < 1.863 \times 10^{-9} = \delta$

(ii)下位 16 ビットを切り捨てた場合
同様にして，下位 16 ビットが 2 進表記で全て 1 である数を丸めた時に誤差は最大となる．よって，

$$\delta = 2^{(1022-1023)} \times (2^{-37} + 2^{-38} + 2^{-39} \ldots + 2^{-50} + 2^{-51} + 2^{-52})$$

$$\delta = (2^{-38} + 2^{-39} + 2^{-40} \ldots + 2^{-51} + 2^{-52} + 2^{-53})$$

大きめに見積もると，一番近い 2 のべき乗より，
$\delta = 2^{-37} > (2^{-38} + 2^{-39} + 2^{-40} \ldots + 2^{-51} + 2^{-52} + 2^{-53})$
とすることができる．

10 の累乗で表すと，以下のようになる．
$2^{-37} = 7.27595 \cdots \times 10^{-12} < 7.276 \times 10^{-12} = \delta$