論　文

整数ロジスティック写像の諸性質：発散，収束，周期性

董　　際国[†a)]　　森田　啓義[††b)]

Various Characters of Integer Logistic Map : Divergence, Convergence, and Periodicity

Jiguo DONG[†a)] and Hiroyoshi MORITA[††b)]

あらまし　本研究は，整数ロジスティック写像 $X_{t+1} = \lfloor 4X_t(2^N - X_t)2^{-N} \rfloor$ において，初期値敏感性を示さない初期値の集合の存在範囲とその大きさを明らかにする．また，整数ロジスティック写像の逆対応 $(\tilde{X}_t = \lfloor \frac{2^N}{2} \pm \frac{\sqrt{2^N(2^N - \tilde{X}_{t+1})}}{2} \rfloor)$ を用いて，不動点を含む任意の値に落ち入る軌道の存在を調べる方法を提案する．そして，数値計算により，整数ロジスティック写像が生成できる平均的な非周期状態長と計算精度 N との近似的な関係を与える．

キーワード　整数ロジスティック写像，初期値敏感性，逆対応，非周期状態長

1. まえがき

擬似乱数生成への応用にカオスが期待されている [1] のは，カオスが初期値敏感性を有するからである．この初期値敏感性を有するため，微小な差しかもたない初期状態から生成した系列がたちまち全く異なる軌道を辿る．本論文の筆者らは整数ロジスティック写像 [2] の内部演算において，乗算結果の上位ビットと下位ビットの XOR をとるという撹拌演算を加えた乱数生成法を提案した [3].

この撹拌乱数生成法は，高速処理が可能で，よい統計的乱数性を有し，また文献 [3] では，撹拌乱数生成法は，メルセンヌ・ツイスター法 (MT) [4] より強い初期値敏感性を有することが計算機数値実験より示されている．

MT は GFSR を改良したモンテカルロ法用の擬似乱数生成法で，長周期，良質な乱数を高速に生成できることで知られている [5], [6].

撹拌乱数生成法は，入出力 N ビットの整数ロジスティック写像の繰返し演算で発生する $2N$ ビットの計算結果を利用して，毎回の写像ごとに，上位 N ビット（整数ロジスティック写像の出力）と下位 N ビット（出力する際に切り捨てられる小数）との間で XOR 演算を施した N ビットの値を擬似乱数として出力する．ただし，整数ロジスティック写像の繰り返し演算には $2N$ ビットの計算結果の上位 N ビットを用い，N ビットの XOR 演算は出力（擬似乱数）を生成するのみに用いる．このため，出力される擬似乱数の性質（初期値敏感性や周期性など）は整数ロジスティック写像が生成する系列に依存しているが，逆に XOR 演算は整数ロジスティック写像の計算結果に影響を与えない．

整数ロジスティック写像を擬似乱数生成へ利用する場合，乱数生成法には高速生成性と良質性以外に，生成される系列が初期値敏感性を有し，長い非周期状態長を有することが求められる．

しかし，整数ロジスティック写像は，初期値によっては，初期値敏感性を示さない場合がある．本論文では新たに初期値敏感性を示さない初期値の集合の存在範囲とその大きさについて考察する．これらの初期値の集まりを本論文ではホール (Hall) と呼ぶ．

整数ロジスティック写像 ℓ_N は，不動点以外の値を初期値にして擬似乱数を生成するとき，いったん不動点に落ち入れば，その後何度 ℓ_N を施しても，得られ

† セリック株式会社，東京都
Selic Corporation, 705, 7–5, Sanbancho, Chiyoda-ku, Tokyo, 102–0075 Japan
†† 電気通信大学大学院情報システム学研究科，調布市
Graduate School of Information Systems, The University of Electro-Communications, 1–5–1 Chofugaoka, Chofu-shi, 182–8585 Japan
a) E-mail: jiguo@selicco.com
b) E-mail: morita@is.uec.ac.jp

た数列は全て同じ値をとる．ℓ_N は可逆ではないが，逆対応が存在している．本論文では ℓ_N の発散とその逆対応の収束を利用して，ℓ_N を繰り返し施した場合に，不動点に落ち入る時系列を調べる方法とその例を示す．これを用いて，不動点以外の初期値から不動点に落ち入ることを避けることが可能となる．

浮動小数点法に限らず，有限けたの演算を用いた場合，ロジスティック写像には複数の異なる周期長のループが存在し，周期状態に入る前にはリーダーと呼ばれる過渡状態の系列が存在している [7]．したがって，整数ロジスティック写像が生成できる非周期状態長（同じ値が現れない系列の長さ）は，リーダー長 ℓ と周期長 S に決定される $(\ell + S)$．また，任意に選ばれた初期値は，複数の異なる周期長のループの中のある一つの系列に属するため，整数ロジスティック写像における非周期状態長を考察するとき，リーダー長 ℓ と周期長 S だけではなく，初期値に依存して得られるループの頻度分布を併せて議論する必要がある．

これまで，ℓ_N において，計算精度 $9 \sim 16$ ビットのときの周期長とリーダー長の平均値が示されたが [2]，異なる複数の周期長の頻度分布については考慮されていない．また，特定のループと初期値との間の関係についても明らかにされていない．

本論文では，$18 \sim 72$ ビットの計算精度による数値計算から，周期長の頻度分布を用いて，ℓ_N における平均的な非周期状態長と計算精度 N との関係を求めた．

本論文の構成は次のとおりである．まず，**2.** では初期値敏感性を示さない場合について考察する．**3.** では ℓ_N の不動点に入る時系列に関する調べ方について述べる．そして **4.** では ℓ_N における計算精度 N と非周期状態長の近似的な関係について考察し，**5.** では結論を述べる．

2. 発　　散

［定義 1］　整数ロジスティック写像 [2] とは

$$\ell_N : \{0, 1, \ldots, 2^N - 1\} \to \{0, 1, \ldots, 2^N - 1\};$$
$$\ell_N(X) = \lfloor 4X(2^N - X)2^{-N} \rfloor,\ 0 \le X < 2^N,$$

X：整数である．

ここで，実数 x に対して，$\lfloor x \rfloor$ は x を超えない最大の整数である．　□

本論文では，ℓ_N を用いて定まる差分方程式

$$\begin{cases} X_0 = 1 \text{ 以上 } 2^N - 1 \text{ 以下の任意の整数} \\ X_{t+1} = \ell_N(X_t),\ t \ge 0 \end{cases} \tag{1}$$

から生成される数列 $\{X_t\}$ について考察する．

図 1 に計算精度 $N = 8$ ビットのときの整数ロジスティック写像の状態 X_t の推移を示す．矢印 $\to$ は，整数ロジスティック写像の状態 X_t を一回写像した結果を指す．すなわち，$40 \to C0$ は $C0 = \ell_N(40)$ を意味する．また，図 1 において，整数ロジスティック写像によって同じ値に移される状態が四つ以上ある場合は楕円で囲んでいる．

カオスを擬似乱数の生成に応用する場合，用いるカオス関数が初期値敏感性を有することは重要である．しかし，ℓ_N の場合，初期値の選び方によっては，初期値敏感性を示さない場合がある．すなわち，隣接する値を X_0 として選ぶと，X_0 から，同じ X_1 が得られる場合がある（図 1 に楕円で囲んでいる，例えば，$73, 74$）．ℓ_N を低い計算精度で計算すると，初期値敏感性を示さない場合を観測することは容易であるが，任意に与えられた計算精度のもとで，その観測結果から初期値敏感性を示さない範囲や位置を確定することは難しい．本節は，ℓ_N において，初期値敏感性を示さない範囲と位置を求め，更に，それらの計算精度の影響について明らかにする．

2.1 準　　備

以下では，任意の正整数 N に対し，

$$\mathcal{Z}_N = \{0, 1, \ldots, 2^N - 1\}$$

とおく．

［定義 2］　任意の $X, Y \in \mathcal{Z}_N$ に対し，関係 $\sim$ とは

$$\ell_N(X) = \ell_N(Y)$$

となる場合で，その場合に限る．このとき，$X \sim Y$ と記す．

この関係 $\sim$ において，$X, Y \in \mathcal{Z}_N$ に対し，$X \sim X$（反射律），$X \sim Y \Rightarrow Y \sim X$（対称律）が成立つことは容易に分かる．更に，$X \sim Y,\ Y \sim Z \ \Rightarrow \ X \sim Z$（推移律）も成立するので，関係 $\sim$ は $\mathcal{Z}_N$ の同値関係である．また，$X, Y \in \mathcal{Z}_N$ に対し，$\ell_N(X) \ne \ell_N(Y)$ のとき，$X \not\sim Y$ と記す．　□

［定義 3］　任意の $A \in \mathcal{Z}_{N-1}$ に対し

$$\mathcal{S}_A = \{X \in \mathcal{Z}_N \mid A \sim X\}$$

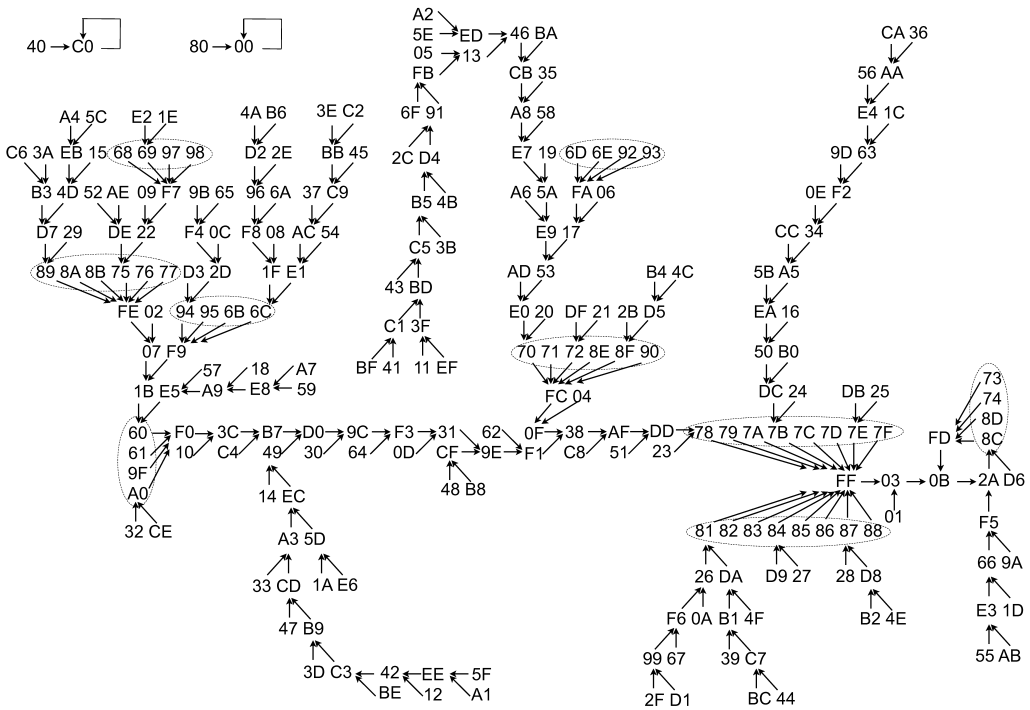

図 1　整数ロジスティック写像の状態 X_t の推移，$N = 8$
Fig. 1　Transition of state (X_t) of integer logistic map, $N = 8$.

とおく．　□

集合 $\mathcal{S}_A$ は $\mathcal{Z}_N$ の同値類である．同値類 $\mathcal{S}_A \cap \mathcal{Z}_{N-1}$ が少なくとも 2 個以上の元を含むとき，本研究では $\mathcal{S}_A \cap \mathcal{Z}_{N-1}$ をホール (Hall) と呼び，

$$\mathcal{H}_A = \mathcal{S}_A \cap \mathcal{Z}_{N-1}$$

とおく．また，定義 1 から，$X \sim 2^N - X$ が成立する．

ホールについては次の命題が成立する．

［命題 1］　もし，任意の $A \in \mathcal{Z}_{N-1}$，$X_1, X_2 \in \mathcal{Z}_{N-1}$ に対し，

$$X_1, X_2 \in \mathcal{H}_A \text{ かつ } X_1 < X_2$$

ならば，任意の $X_1 < X_3 < X_2$ を満たす，$X_3 \in \mathcal{Z}_{N-1}$ に対し，

$$X_3 \in \mathcal{H}_A$$

である．

（証明）　まず，$\delta_k = 4X_k(2^N - X_k)2^{-N} - \ell(X_k)$ とおく $(k = 1, 2, 3)$．すると，ℓ_N の定義 1 から $0 \le \delta_1, \delta_2, \delta_3 < 1$ である．更に，

$$\begin{aligned}&\ell_N(X_3) - \ell_N(X_2)\\ &= \lfloor 4X_3(2^N - X_3)2^{-N} \rfloor - \lfloor 4X_2(2^N - X_2)2^{-N} \rfloor\\ &= 4(X_3 - X_2)(1 - (X_3 + X_2)/2^N) + (\delta_2 - \delta_3)\end{aligned}$$

ところで，仮定より，$X_3 - X_2 < 0$，また，$1 - (X_3 + X_2)/2^N > 0$，$-1 < \delta_2 - \delta_3 < 1$ なので，

$$\ell_N(X_3) - \ell_N(X_2) < 1 \tag{2}$$

が成り立つ．同様に，

$$\begin{aligned}&\ell_N(X_3) - \ell_N(X_1)\\ &= 4(X_3 - X_1)(1 - (X_3 + X_1)/2^N) + (\delta_1 - \delta_3)\end{aligned}$$

仮定より，$X_3 - X_1 > 0$，また，$1 - (X_3 + X_1)/2^N > 0$，$-1 < \delta_3 - \delta_1 < 1$ なので，

$$\ell_N(X_3) - \ell_N(X_1) > -1 \tag{3}$$

更に，$\ell_N(X_1) = \ell_N(X_2)$ より，$\ell_N(X_3) = \ell_N(X_1) = \ell_N(X_2)$ が成り立ち，題意を得る．　□

［定義 4］　もし，X と $\Delta \ge 1$ が，$0 \le X < 2^{N-1}$，

$0 \le X + \Delta < 2^{N-1}$ を満たすならば，$\Delta\ell_N$ を

$$\Delta\ell_N = \ell_N(X+\Delta) - \ell_N(X)$$

で定義する．

［補題 1］ 任意の $X \in \mathcal{Z}_{N-1}$ に対し，整数 Δ が $1 \le X + \Delta < 2^{N-1}$ を満たすならば，

$$\frac{\Delta\ell_N}{\Delta} \ge \lfloor 4(2^N - 2X - \Delta)2^{-N} \rfloor \tag{4}$$

（証明） 定義 1 に従い，$\ell_N(X+\Delta)$ を変形すると，

$$\begin{aligned}
&\ell_N(X+\Delta)\\
&= \lfloor 4(X+\Delta)(2^N - X - \Delta)2^{-N} \rfloor\\
&= \lfloor 4X(2^N - X)2^{-N} + 4\Delta(2^N - 2X - \Delta)2^{-N} \rfloor\\
&\ge \lfloor 4X(2^N - X)2^{-N} \rfloor + \lfloor 4\Delta(2^N - 2X - \Delta)2^{-N} \rfloor\\
&= \ell_N(X) + \lfloor 4\Delta(2^N - 2X - \Delta)2^{-N} \rfloor.
\end{aligned}$$

それゆえ，

$$\Delta\ell_N \ge \lfloor 4\Delta(2^N - 2X - \Delta)2^{-N} \rfloor \tag{5}$$

が成立する．$\Delta \ge 1$ は整数なので，式 (5) は，更に $\Delta\ell_N \ge \Delta\lfloor 4(2^N - 2X - \Delta)2^{-N} \rfloor$ と変形できる．□

2.2 ホールの存在範囲とその大きさ

2.2.1 ホールが存在しない範囲

［定理 1］ もし，$N \ge 2$ に対して，$\Delta \ge 1$ かつ，

$$X \le \frac{3}{8}2^N - \frac{1}{2}\Delta \tag{6}$$

ならば，$X + \Delta \not\sim X$ である．

（証明） 任意の $X \in \mathcal{Z}_{N-1}$ に対して，式 (6) の両辺を 2 倍して変形していくと，

$$2X \le 3 \times 2^{N-2} - \Delta = 2^N - 2^{N-2} - \Delta$$

となり，

$$2^N - 2X - \Delta \ge 2^{N-2}$$

と変形でき，更に両辺を 2^{N-2} で割ると，

$$4(2^N - 2X - \Delta)2^{-N} \ge 1$$

をえる．したがって，

$$\lfloor 4(2^N - 2X - \Delta)2^{-N} \rfloor \ge 1 \tag{7}$$

一方，$\Delta \ge 1$ より，補題 1 の不等式 (4) が成り立ち，これと式 (7) から題意をえる． □

定理 1 と命題 1 により，式 (6) は，整数ロジスティック写像において，ホールの存在しない範囲を与える．

2.2.2 ホールの大きさ

［定理 2］ 式 (1) において，任意の

$$\frac{3}{8}2^N \le A < 2^{N-1}$$

に対し，

$$\mathcal{H}_A = \{X | A_1 \le X < A_2\}.$$

ここで，

$$\begin{cases}
A_1 = \dfrac{2^N}{2} - \left\lfloor \dfrac{2^{N/2}\sqrt{2^N - \ell_N(A)}}{2} \right\rfloor\\[2ex]
A_2 = \dfrac{2^N}{2} - \left\lceil \dfrac{2^{N/2}\sqrt{2^N - \ell_N(A) - 1}}{2} \right\rceil
\end{cases} \tag{8}$$

とおいた．ここで，実数 x に対して，$\lceil x \rceil$ は x より大きい最小の整数である． □

（証明） 定義 1 より，

$$\ell_N(X) \le 4X(2^N - X)2^{-N} < \ell_N(X) + 1$$

をえる．$X \in \mathcal{H}_A$ なら，$\ell_N(X) = \ell_N(A)$ なので，

$$\ell_N(A) \le 4X(2^N - X)2^{-N} < \ell_N(A) + 1$$

と書き直せる．この不等式を X に関する解を求め，$\ell_N(A) \le 4X(2^N - X)2^{-N}$ より

$$\begin{aligned}
&\frac{2^N}{2} - \frac{2^{N/2}\sqrt{2^N - \ell_N(A)}}{2} \le X\\
&\quad \le \frac{2^N}{2} + \frac{2^{N/2}\sqrt{2^N - \ell_N(A)}}{2}
\end{aligned}$$

をえる．また，$4X(2^N - X)2^{-N} < \ell_N(A) + 1$ より

$$X < \frac{2^N}{2} - \frac{2^{N/2}\sqrt{2^N - (\ell_N(A)+1)}}{2} \text{ と}$$

$$X > \frac{2^N}{2} + \frac{2^{N/2}\sqrt{2^N - (\ell_N(A)+1)}}{2}$$

をえる．ここで，$X < 2^{N-1}$ なので，

$$\begin{aligned}
&\frac{2^N}{2} - \frac{2^{N/2}\sqrt{2^N - \ell_N(A)}}{2} \le X\\
&\quad < \frac{2^N}{2} - \frac{2^{N/2}\sqrt{2^N - (\ell_N(A)+1)}}{2}
\end{aligned}$$

をえる．更に X が整数であるから，

$$\frac{2^N}{2} - \left\lfloor \frac{2^{N/2}\sqrt{2^N - \ell_N(A)}}{2} \right\rfloor \leq X < \frac{2^N}{2} - \left\lceil \frac{2^{N/2}\sqrt{2^N - \ell_N(A) - 1}}{2} \right\rceil$$

と変形され，題意をえる． □

$\ell_N(A) = 2^N - 1$ のとき，定理 2 から $|\mathcal{H}_A| = 2^{N/2-1}$ となり，$X = 2^{N-1}$ を中心に大きなホールが存在していることが分かる．例えば，$N = 128$ のとき，$|\mathcal{H}_A| = 2^{63}$ となる．

［定義 5］ $\frac{3}{8}2^N \leq A < 2^{N-1}$ を満たす A に対し，P_A^N を

$$P_A^N = |\mathcal{H}_A| 2^{-N} \tag{9}$$

と定める． □

式 (9) の P_A^N は X を等確率に選んだとき，X が $\mathcal{H}_A$ に属する確率を表す．定義 5 の式 (9) に，定理 2 の式 (8) を代入すると，次の系 5 が得られる．

［系 5］ A が $\frac{3}{8}2^N \leq A < 2^{N-1}$ を満たすならば，

$$P_A^N = \left(\left\lfloor \frac{2^{N/2}\sqrt{2^N - \ell_N(A)}}{2} \right\rfloor - \left\lceil \frac{2^{N/2}\sqrt{2^N - \ell_N(A) - 1}}{2} \right\rceil \right) 2^{-N} \tag{10}$$

$\ell_N(A) = 2^N - 1$ のとき，式 (10) より

$$P_A^N = 2^{-N/2-1}$$

である．よって，計算精度 N を高くすると，P_A^N は N の指数関数として急激に減少する．

3. 収　　束

ℓ_N を乱数生成へ利用するとき，生成される時系列が不動点に落ち入らないように初期値を慎重に選ぶ必要がある．本研究は整数ロジスティック写像の逆対応が整数ロジスティック写像と相反する性質をもつ可能性に注目する．すなわち，整数ロジスティック写像は微小な差を有する初期状態 X_0, X_0' から生成される $X_t, X_t', t = 1, 2, \ldots$ は，t の増大とともに，その差が増大する（発散する）性質を有するのに対し，その時間の向きを逆にとった逆対応は，t が小さくなるともに，その差は小さくなる（収束する）という性質をもつ．この節では，ℓ_N の逆対応を利用して，ℓ_N において，不動点を含む，任意の値に落ち入る軌道 (X_t) に関する調べる方法について述べる．

3.1 準　　備

［定義 6］ ℓ_N の逆対応 $\tilde{X}_{t+1} \to (\tilde{X}_{t+}, \tilde{X}_{t-})$ は

$$\begin{cases} \tilde{X}_{t+1} = 1 \text{ 以上 } 2^N - 1 \text{ 以下の任意の整数}, t \geq 0 \\ \tilde{X}_{t\pm} = \left\lfloor \frac{2^N}{2} \pm \frac{\sqrt{2^N(2^N - \tilde{X}_{t+1})}}{2} \right\rfloor \quad \text{（複号同順）}. \end{cases} \tag{11}$$

で定める． □

ここに，式 (11) における $\tilde{X}_{t\pm}$, $t \geq 0$ は $1 \leq \tilde{X}_{t\pm} < 2^N$ を満たす．ℓ_N の場合，式 (1) の計算は小数点以下切捨てを行っており，式 (11) は，この切り捨てられた小数の部分を考慮せずに，直接，二次方程式を解いて得られる式であり，近似解になっているため，必ずしも式 (1) の解であるとは限らない．$\tilde{X}_{t\pm}$ は必ずしも式 (1) の真の解ではないが，式 (1) の解は $\tilde{X}_{t\pm}$ の周辺に存在することが予想される．この予想については，以下で詳しく述べる．

ℓ_N から生成される 2 値系列を以下で定義する．

［定義 7］ $\{X_t\}$ に対し，2 値系列 $\{Y_t\}$ を，

$$Y_t = \begin{cases} 0, & if\ X_t < 2^{N-1} \\ 1, & else \end{cases} \tag{12}$$

と定める． □

本研究では，ℓ_N の計算を順計算，その逆対応の計算を逆計算と呼ぶ．ℓ_N を X_0 から生成される時系列 $(X_0, X_1, \ldots, X_T)$ を順軌道と呼ぶ．また，T を軌道長と呼ぶ．次に，式 (12) で定まる 2 値系列 $\mathbf{Y}^T = Y_0 Y_1 \cdots Y_T$ を逆計算符号と呼ぶ．更に，$\tilde{X}_T = X_T$ とおき，一つの逆計算符号 $\mathbf{Y}^T$ に基づき，式 (11) から得られる時系列 $(\tilde{X}_0, \tilde{X}_1, \ldots, \tilde{X}_T)$ を逆軌道と呼ぶ．ここで，逆計算軌道は全部で 2^T 個あることに注意する．

3.2 整数ロジスティック写像 ℓ_N の逆軌道

ℓ_N は切捨て演算の影響のため，順軌道と逆軌道は必ずしも一致しない．両軌道の関係を数値計算で定量的に調べた．

［定義 8］ 式 (1) と式 (11) において，$t \geq 0$ に対し，

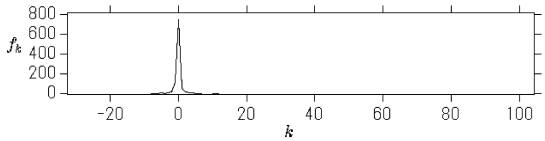

図 2　$N = 128$ ビットで得られた $\Delta X_t = X_t - \tilde{X}_t$ の頻度分布

Fig. 2　Frequency distribution of $\Delta X_t = X_t - \tilde{X}_t$ at $N = 128$ bits.

整数 ΔX_t を

$$\Delta X_t = X_t - \tilde{X}_t$$

で定義する．　□

3.2.1　順軌道と逆軌道の比較

1. 計算精度 N，軌道長 T で，区間 $[1, 3\times 2^{N-3}]$ の中から任意に選んだ M 個の値それぞれを初期値 X_0 とおき，順軌道 $(X_0, X_1, \ldots, X_T)$ を求める．

2. 式 (12) を用いて，対応する 2 値系列（逆計算符号列）$Y_0Y_1\cdots Y_T$ を出力する．

3. 逆計算は $\tilde{X}_T = X_T$ を初期値にして，逆計算符号を用いて逆計算軌道 $(\tilde{X}_0, \tilde{X}_1, \ldots, \tilde{X}_T)$ を求める．

4. 最後に，$-2^N < k < 2^N$ に対し，$\Delta X_t (0 \le t < T)$ のとる値の頻度

$$f_k = |\{t | \Delta X_t = k,\ \ 0 \le t < T\}|$$

を求める．　□

例として，$N = 128, T = 1000$ に対し，ある X_0 に対して上の手順を実施して求められた ΔX_t の取る値の頻度分布を図 2 に示す．図 2 において，横軸は ΔX_t のとる値，縦軸はその頻度である．

図 2 から $\Delta X_t = 0$ となる t の割合は 75% 以上であることが分かる．言い換えれば，$[0, T-1]$ の中からランダムに添字として整数 t を選ぶと，$X_t = \tilde{X}_t$ となる確率は 0.75 以上ある．逆軌道は順軌道と必ずしも一致しないが，一致する確率が高いことを示している．

この結果を更に詳細に吟味するために，以下の実験を行った．計算機シミュレーションによって等確率で $N = 128$ ビットの初期値 X_0 を $M = 1000$ 個発生させ，それぞれの値に対して，$T = 1000$ とおいて，上述した比較手順を実施した．1000 回の試行から逆軌道と順軌道の状態が平均 75% 以上一致している結果を得た．図 2 と同等な結果であった．

また，$|\Delta X_t| > 0$ が逆計算に拡大されなく 0 に収束していることも観察された．1000 回の試行から逆軌道と順軌道で，$\tilde{X}_0 = X_0$ となったのが 788 回あった．すなわち，対称性を利用して生成した 2 値系列（式 (12)）を逆計算に用いれば，0.75 以上の確率で，初期値が求まる．

3.3　不動点に至る全軌道の列挙

整数ロジスティック写像は $0\cdots0$ と $C0\cdots0$（16 進表示）の二つの不動点を有する．整数ロジスティック写像 ℓ_N は，不動点以外の値を初期値にして擬似乱数を生成するとき，いったん不動点に落ち入れば，その後何度 ℓ_N を施しても，得られた数列は全て同じ値をとる．すなわち，擬似乱数生成において，不動点に落ち入る状況を避ける必要がある．ここに，例として，不動点 $C0\cdots0$ に至る全ての軌道を列挙する方法を示す．

一般に，不動点 $C0\cdots0$ に至る全ての軌道は，可能なすべての逆計算符号列から逆軌道を計算することによって求めることができる．その手順を次に示す．

1.　$T = 1$，$\tilde{X}_T = 3\times 2^{N-2}$（不動点 $C0\cdots0$）にする

2.　可能な全ての 2^T 通りの Y^T を用意する

3.　各逆計算符号列 Y^T に対し，$\tilde{X}_T$ から Y^T に沿って T 回逆計算し，$\tilde{X}_0$ をえる

4.　$X_0 = \tilde{X}_0$ を用いて T 回順計算し，X_T をえる

5.　X_T と $\tilde{X}_T$ を比較して，軌道の有無を確認する

6.　全ての逆軌道に対し，ステップ 3.〜5. を繰り返す

7.　軌道が確認された場合，$T = T + 1$ にしてステップ 2. から繰り返す．軌道が確認されなかった場合に，$T = T - 1$ にして，$X_T = \tilde{X}_T$ となる軌道を出力する　□

当然，T 回の逆計算は 2^T の種類数の組合せの逆計算があり得るので，繰返しが続き，T が大きくなるに従い，計算量は T の指数関数的に増大する．ところが，ℓ_N は必ずしも全射ではない．図 1 にあるように，ある X_t に対し，必ず X_{t+1} が存在するが，X_{t-1} が存在するとは限らない．また，$N = 8$ の場合，不動点 $C0$ に至る状態は 40 だけで，00 に至る状態は 80 だけである．したがって，ℓ_N においての不動点 $C0\cdots0, 00\cdots0$ に至る可能な状態は多くないと推測される．

例えば，計算精度 $N = 128$ ビットのとき，$X_T = 3\times 2^{N-2}$ への可能な軌道については，$T = 6$ で，不動点 $C0\cdots0$ に至る全ての軌道を得た．その X_t の軌跡を図 3 に示す（X_t は 16 進表示である）．この図においては，$N = 128$ ビットの場合，不動点 $C0\cdots0$ に至

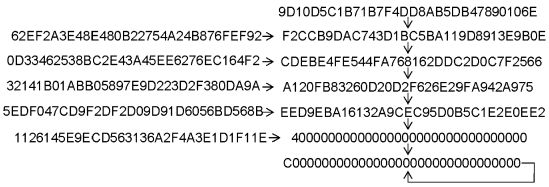

図 3　計算精度 $N = 128$ ビットの不動点 $\mathtt{C0}\cdots\mathtt{0}$ への軌跡

Fig. 3　Tracks to fixed point ($\mathtt{C0}\cdots\mathtt{0}$) of calculation accuracy $N = 128$ bits.

表 1　N と $X = 3\times 2^{N-2}$ に至る可能な X の数 N_S，軌道数 N_O 及び T

Table 1　Possible number N_S of X, number N_O of orbits, and T to $X = 3\times 2^{N-2}$ and calculation accuracy N.

N	8	32	64	96	128
T	1	1	1	4	6
N_S	2	2	2	8	12
N_O	1	1	1	4	6

る可能な状態 X の数は不動点を含めて 12 個であり，軌道数は 6 本であった．また，不動点 $\mathtt{0}\cdots\mathtt{0}$ に至る可能な状態 X は，$\mathtt{80}\cdots\mathtt{0}$ 以外にはなかった．

なお，表 1 に数値計算により，計算精度 $N = 8, 32, 64, 96, 128$ のときの不動点 $X = 3\times 2^{N-2}$ に至る可能な状態 X の数 N_S，軌道数 N_O 及び逆計算回数 T をまとめておく．この例が示すように，不動点に至る軌道に関する情報（点の数）は極めて少ないことが分かる．このような少量の値は乱数生成システムの設計時に，初期値から除外することは可能であり，システムが不動点に落ち入らないことを保障することができる．ここに，異なる計算精度での不動点 $\mathtt{C0}\cdots\mathtt{0}$ に至る可能な状態 X の正確な数は用いる計算精度に依存することに注意する．

4. 整数ロジスティック写像 ℓ_N の周期性

ℓ_N の周期性については，これまでにも，計算精度 $N = 9 \sim 16$ ビットのループ長とリーダー長の平均に対する調査結果 [2] が報告されている．しかしながら，ℓ_N を用いた乱数生成とその応用を考える上では，上述の研究に加え，更に，①異なるループの数，②初期値とループの関係，③非周期状態長，をより詳細に検討する必要がある．

しかしながら，有限計算精度でのカオスの周期性は理論的な解析は困難である [1] ので，本章では，上に述べた三つの観点から数値実験を行い，ℓ_N の周期性について新たに得られた知見について述べる．

表 2　計算精度 $N = 18 \sim 72$ において，用いた初期値の数 M

Table 2　Number (M) of the initial value used in calculation accuracy $N = 18 \sim 72$.

N	18,22,26,30	36,40,43	48	52	56	60,64	68,72
M	$2^{N-1}-2$	10^6	5×10^5	10^5	4×10^4	5000	300

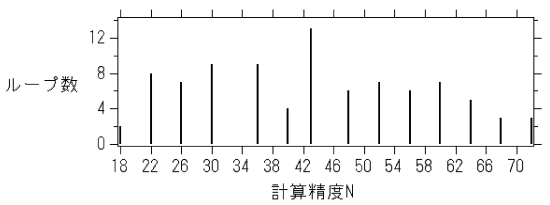

図 4　計算精度 $N = 18 \sim 72$，調べ得たループ数

Fig. 4　Number of loops obtained for investigation in calculation accuracy $N = 18 \sim 72$.

4.1 異なるループの数

ℓ_N のループ数については，以下に示す数値実験を $18 \le N \le 72$ の範囲で行った．各計算精度において用いた初期値の数 M を表 2 に示す．

計算精度 $N = 18, 22, 26, 30$ ビットにおいては，$X_0 \in [1, 2^{N-1}-1]$ に対して，$X_0 = 2^{N-2}$ を除き，取り得る全ての初期値について，落ち入るループの数を調べた．また，計算精度 $N = 36 \sim 72$ ビットにおいて，計算機シミュレーションにより，等確率で生成した M 個の初期値について，落ち入るループの数を調べた．

計算精度 $N = 18 \sim 72$ においての調査結果を図 4 に示す．横軸は計算精度 N，縦軸はその N で調査し得たループの数である．計算精度 $N = 18 \sim 72$ においての調査結果では，各計算精度ごとに検出されたループ数は様々で，計算精度との間に一定な規則は見出せないが，最大 13 個であった．

また，計算精度 $18, 22, 26, 30$ においての取り得る全ての初期値に対する調査結果では，それぞれのループ数が $2, 8, 7, 9$ であった．更に，それらの周期長はすべて異なる．

以上の実験に加え，計算精度 $33 \sim 75$ ビットの範囲で，モンテカルロ法によって周期性について調べてみると，ℓ_N が生成する系列が有するループ数の最大値は 13 と低く抑えられていた．この結果から，非周期状態長は N の指数関数的に増大することを示唆している．また，ループ数は計算精度に依存するが，計算精度との間に明確な規則は見出せない．

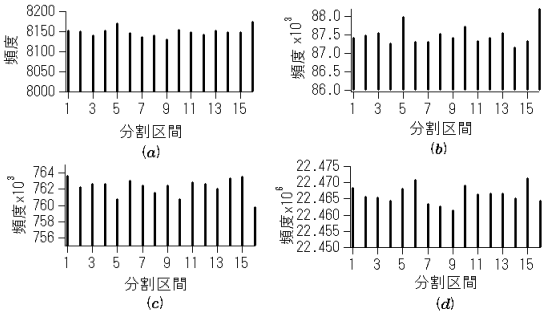

図 5　計算精度 $N = 18, 22, 26, 30$ で，区間 $[1, 2^{N-1} - 1]$ を 16 区域に分割して調べ得た最頻度のループの頻度

Fig. 5　Frequency of the highest loop of frequency obtained for investigation in calculation accuracy $N = 18, 22, 26, 30$, and $[1, 2^{N-1} - 1]$ is divided into 16 districts.

非周期状態長については以下で詳しく議論する．

4.2　初期値とループの関係

乱数生成法にとっては，ある区間 $[a, b] \subset \mathcal{Z}_N$ 内の値がすべて，ある一つのループに落ち入ることは好ましくない．逆に，特定の区間と特定のループの間に，相関関係がなければ，乱数を生成する初期値は任意に選べることができる．

そこで，次のような数値実験を考える．

計算精度 N ビットにおいて，区間 $[a, b]$ を M 等分割する．分割された各部分区間に対し，区間中の取り得る全ての値を初期値 X_0 とする軌道が落ち入るループの頻度を調べ，観察する．ただし，同じループに落ち入るかどうかの判断は，前節の最後に述べたようループごとにループ長は異なるので，ループ長で判断した．

まず，計算精度 $N = 18, 22, 26, 30$ に，$a = 1, b = 2^{N-1} - 1, M = 16$ にし，各部分区間ごとに，区間内の全ての値を初期値とする軌道を求める．これらの軌道が落ち入る最頻度のループの頻度をそれぞれ図 5 の $(a), (b), (c), (d)$ に示す．各区域においての頻度は大きな偏りがないことを見て取れる．実験は直ぐに不動点に落ち入る $X_0 = 2^{N-2}$ を除外した．

次に，計算精度 $N = 30, M = 50$ にし，二つの区間 $a = 1, b = 3276800$ と $a = 1, b = 25600$ を同様に，各部分区間ごとに，区間内の全ての値を初期値とする軌道を求めた．それぞれ図 6 の $(a), (b)$ に示す．同様に，各区域においての頻度は大きな偏りがないことが示されている．

以上の結果は，ℓ_N において，計算精度 N の値によらず，特定のループに落ち入る初期値がある特定の範囲にあることは認められないことを示唆している．

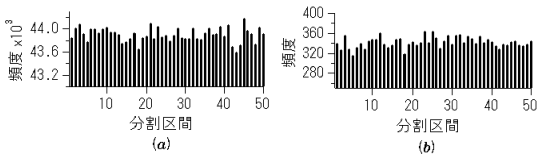

図 6　計算精度 $N = 30$ で，(a) は区間 $[1, 3276800]$ を，そして (b) は $[1, 25600]$ をそれぞれ 50 等間隔に分割して調べ得た最頻度のループの頻度

Fig. 6　Frequency of the highest loop of frequency obtained for investigation in calculation accuracy $N = 30$, and $[1, 3276800](a)$, $[1, 25600](b)$ is divided into 50 districts.

4.3　非周期状態長

ℓ_N が初期値 X_0 から生成できる非周期状態長は $\ell + S$ となる．任意に選ばれた初期値が落ち入るループも異なり，リーダー長 ℓ も異なるのは一般的である．ℓ_N を用いて乱数生成システムを設計するとき，計算精度と得られる平均的な非周期状態長の関係を知る必要がある．

ℓ_N を用いて乱数を生成する際に，初期値はランダムに選ばれることは一般に考えられる．そうして生成される順軌道が落ち入るループは，最頻度のループになる確率が最も高い．平均的な非周期状態長を求めるとき，このことを考える必要がある．

ある初期値 X_0 から得られる順軌道がもつリーダー長と周期長を求めるには，その初期値がもつリーダー長は未知であるため，これを推定する必要がある．それを推定リーダー長と呼び，ℓ' で表す．ループは $t \geq \ell$ からなるため，$\ell' < \ell$ のときは，ループは検出できない．

計算精度と得られる平均的な非周期状態長の関係を求める最も単純な方法は，モンテカルロ法によって実現できる．例えば，ランダムに M 個の初期値を選び，それぞれの初期値から生成される順軌道に対し，リーダー長と周期長を求め，総数 M の平均を求めるとよい．しかし，N が大きいと，計算量と必要のメモリが N の指数関数的に増大し，実現は難しい．そこで，本研究は計算量と必要のメモリを減らすために，正確なリーダー長を求めず，平均リーダー $\overline{\ell}$ を推定する方法をとる．ℓ' と周期長を求めるアルゴリズムは以下のようになる．

[アルゴリズム LS]

入力：N，初期値 X_0．出力：推定リーダー長 ℓ'，周

期長 S.

1. $L = 2^{N/2+1}$ を設定する.
2. ℓ_N を初期値 X_0 から L 回計算して X_L を得る.
3. 引き続き，ℓ_N を繰返し計算し，$X_L = X_{L+S}$ となった時点で，周期長 S のループが検出される.
4. $L = L/2$ にして，ステップ 2，3 をループが検出できなくなるまで繰り返す.
5. $\ell' = 2L$ と S を出力する. □

ただし，ステップ 1 での L の設定においては，**4.1** の実験と同じ条件で，最大リーダー長を求めた結果により，$\ell < 2^{N/2+1}$ を得ている.

こうすると，M 個の初期値 $X_i (i = 1, \ldots, M)$ に対し，アルゴリズム LS を適用して，得られた出力を ℓ'_i とおく．全ての初期値において，ℓ_i を X_i とした場合のリーダー長とすると，必ずしも正確なリーダー長は求められないが，ℓ_i とアルゴリズム LS の出力 ℓ'_i の間に，$\ell'_i/2 < \ell_i < \ell'_i$ の関係が成り立つ.

ここで，平均リーダー長 $\overline{\ell}$ は

$$\overline{\ell} = \sum_{i=1}^{M} \frac{\ell_i}{M}$$

で計算され，その近似を $\ell^\star$ とし，式 (13) で与える.

$$\ell^\star = \sum_{i=1}^{M} \frac{(\ell'_i/2 + \ell'_i)/2}{M} = \sum_{i=1}^{M} \frac{1}{M} 3\ell'_i/4 \qquad (13)$$

式 (13) で与える近似的な平均リーダー長 $\ell^\star$ と平均リーダー長 $\overline{\ell}$ との誤差 $\overline{\ell} - \ell^\star$ は，区間

$$\left(-\sum_{i=1}^{M} \frac{1}{M} \ell'_i/4 \, , \, \sum_{i=1}^{M} \frac{1}{M} \ell'_i/4 \right)$$

の中に含まれることが分かる.

$N = 36 \sim 72$ に対し，初期値の数 M は，表 2 と同様にして，$\ell^\star$ の値を求めた結果を図 7 に示す．図 7 において，横軸は N，縦軸は近似的な平均リーダー長 $\ell^\star$ に底 2 の対数をとった値である．なお，同図中，$f_1(N) = N/2 - 1$ を実線で表示している.

それぞれの N で求まった複数のループの中，最も長い周期長をもつループを最長周期 S_L と呼び，最頻度のループを最多周期 S_M と呼ぶことにして，それぞれ N との関係を図 8 に示す.

図 8 において，横軸は計算精度 N，縦軸は (a) に最長周期の長さ，(b) に最多周期の長さに，それぞれ底 2 の対数をとった値を示す．図 8 (a) と (b) において，

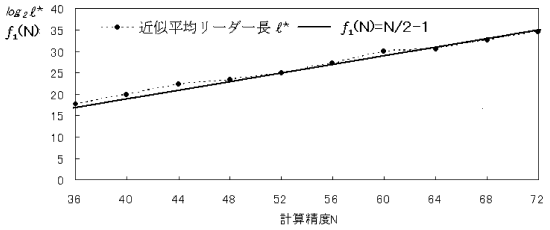

図 7 計算精度 N と近似平均リーダー長 $\ell^\star$ の関係
Fig. 7 Relation of calculation accuracy N and average leader's lengths of approximation $\ell^\star$.

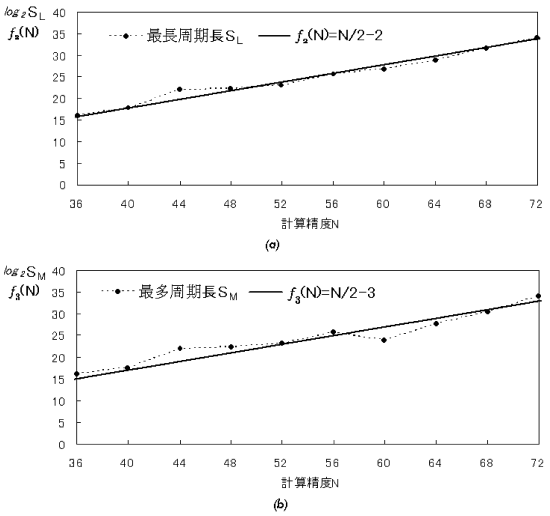

図 8 最長周期長 (a)，最多周期長 (b) と計算精度 N の関係
Fig. 8 Relation between calculation accuracy N and length of loop with the longest loop (a), length of loop with the highest frequency (b).

それぞれ $f_2(N) = N/2 - 2$ と $f_3(N) = N/2 - 3$ を実線で示している.

以上の結果より，最長周期長，最多周期長，近似平均リーダー長 $\ell^\star$ は計算精度 N と近似的に，図 7 と図 8 に示すように，

$$S_L \approx 2^{N/2-2}$$
$$S_M \approx 2^{N/2-3}$$
$$\ell^\star \approx 2^{N/2-1}$$

で表せることが分かる.

ℓ_N の非周期状態長 $(\ell + S)$ の推定値を L_c として，M 個のランダムな初期値に対してアルゴリズム LS を適用して求められた $\ell^\star$ と S_M を用いて，

$$L_c = \ell^\star + S_M$$

とおく．

$S_M \approx 2^{N/2-3}$，$\ell^\star \approx 2^{N/2-1}$ なので，すると，上述の実験結果から，

$$L_c \approx 5 \times 2^{N/2-3}$$

で与えられる．

計算精度 $N = 12 \sim 64$ の整数ロジスティック写像の平均リーダーと平均周期長についての調査結果が文献 [8] に報告されている．リーダーについての調査結果では，本論文の推測平均リーダー長と近い結果となっている．一方，周期長についての調査結果では，本論文では異なる周期長のループの分布の強い片寄りの存在を念頭に置いて，最長周期と最多周期の長さを示しているが，文献 [6] は異なる周期長のループの分布の片寄りを考慮せず，平均周期長を示している．

本論文は周期性についての調査において，$N = 72$ までとしたが，$N = 72$ で汎用 PC を用いて 1 日当りに周期を調べられる初期値の数は 10 個ほどであった．計算精度を 1 ビット上げると，平均的にリーダー長や周期長が 2 倍ほど長くなるので，$N = 72$ ビットは汎用 PC で調査できる限界に近づいているといえる．

5. むすび

異なる初期値から生成された系列が初期敏感性を示さない範囲や位置など，計算精度 N との関係を導いた．

ℓ_N の逆対応を利用して，逆計算と順計算で特定の状態 X_t を通る軌道について確認する方法を示した．それを ℓ_N の不動点に入る時系列に関する調べ方法に応用することにより，ℓ_N によって生成する系列が不動点に落ち入ることの回避に役立つ．

ℓ_N がもつ周期性と計算精度の関係について，数値計算により調べた．周期長の数が有限であるが，N に依存する．周期長の数は一定でなく，N との相関が見られない．また，ℓ_N においては，特定の周期に落ち入る初期値がある特定の範囲にあることは認められない．そして，M 個のランダムな初期値に対してアルゴリズム LS を適用して求められた最長周期長，最多周期長，平均リーダー長は計算精度 N に対し，それぞれ，$2^{N/2-2}$，$2^{N/2-3}$，$2^{N/2-1}$ によって，近似されることを観察した．

最後に，非周期状態長の推定値と計算精度 N の関係 ($L_c \approx 5 \times 2^{N/2-3}$) を与えた．

文　献

[1] 香田　徹，離散力学系のカオス，コロナ社，1998.

[2] 石田邦昭，常田明夫，井上高宏，“有限ビット演算によるカオス的系列の性質，” 信学技報，CAS98-16, 1998.

[3] 董　際国，森田啓義，“整数ロジスティック写像と撹拌演算による乱数生成，” 信学論（A），vol.J94-A, no.12, pp.923–931, Dec. 2011.

[4] M. Matsumoto and T. Nishimura, “Mersenne Twister: A 623-dimensionally equidistributed uniform pseud random number generator,” ACM Trans. Model. Comput. Simul., vol.8, pp.3–30, 1998.

[5] http://www.math.sci.hiroshima-u.ac.jp/˜m-mat/MT/mt.html

[6] http://mathsoc.jp/publication/tushin/

[7] 庄野克房，カオスエンジニアリング，シュプリンガーフェアラーク東京，2002.

[8] T. Miyazaki, S. Araki, Y. Nogami, and S. Uehara, “Rounding logistic maps over integers and the properties of the generated sequences,” IEICE Trans. Fundamentals, vol.E94-A, no.9, pp.1817–1825, Sept. 2011.

[9] 董　際国，森田啓義，“整数ロジスティック写像の諸性質：発散，収束，周期性，” 信学技報，NLP2012-27, 2012.

（平成 24 年 7 月 19 日受付，10 月 9 日再受付）

董　際国　（正員）

1984 上海科学技術大学精密機械工学卒．1997 山形大学人文学部経済学科卒．1999 同大学院社会文化システム研究科修士課程修了．2012 電気通信大学情報システム研究科博士後期修了．カオスの応用に関する研究に従事．工博．

森田　啓義　（正員：シニア会員）

1983 大阪大学大学院博士後期課程了．同年豊橋技術科学大学助手．1990 電気通信大学電気通信学部講師を経て，現代同大大学院情報システム学研究科教授．3D 画像処理，MPEG 応用，データ圧縮，誤り訂正など，情報理論とその応用に関する研究に従事．工博．情報処理学会，情報理論とその応用学会，IEEE, ACM 各会員．