整数上のピースワイズ・ロジスティック写像の区分数に関する一考察

江口 颯太[1,a)]　宮崎 武[1]　荒木 俊輔[2]　上原 聡[1]　野上 保之[3]

概要：従来の整数上のロジスティック写像では，擬似乱数生成の観点からコントロールパラメータとして選択できる値は限られた範囲となり，その範囲外では出力値の上限下限が狭まることが問題点として挙げられる．Wang らが提案した実数上のピースワイズ・ロジスティック写像では，区分数の増加に伴って選択可能なコントロールパラメータの領域が増えることが示されている．そこで我々は，演算精度 n の整数上で区分数 m のピースワイズ・ロジスティック写像 $\mathrm{PLM}_{\mathrm{Int}}^{(n,m)}(X)$ を提案し，区分数と生成系列 $X_{i+1} = \mathrm{PLM}_{\mathrm{Int}}^{(n,m)}(X_i)$ について考察する．分岐図と NIST 検定では区分数に対して改善が見られるが，周期とリンク長には大きな変化はない．

キーワード：整数上のロジスティック写像, ピースワイズ, 分岐図, リアプノフ指数, NIST 検定

A Study on the Number of Divisions in Piecewise Logistic Map over Integers

Sota Eguchi[1,a)]　Takeru Miyazaki[1]　Shunsuke Araki[2]　Satoshi Uehara[1]　Yasuyuki Nogami[3]

Abstract: Conventional logistic map over integers has limited control parameters and the difference between the upper and lower of output values becomes smaller. To make impronements on the map, the piecewise logistic map has been proposed by Wang et al. It has been shown that the range of selectable control parameters increases. So we propose the piecewise logistic map over integers $\mathrm{PLM}_{\mathrm{Int}}^{(n,m)}(X)$, where n is the calculating accuracy, and m is the number of divisions. We consider the relationship between the generated sequences $X_{i+1} = \mathrm{PLM}_{\mathrm{Int}}^{(n,m)}(X_i)$ and the number of divisions. Then, it is shown that $\mathrm{PLM}_{\mathrm{Int}}^{(n,m)}(X)$ has improvements in diagrams and NIST test, but there are no significant effect for the period and link length.

Keywords: logistic map over integers, piecewise, branch diagram, Lyapunov exponent, NIST test.

1. 序論

擬似乱数系列の生成法には様々な手法があり，その一つとしてロジスティック写像を用いるものがある．ロジスティック写像は二次式で構成される繰り返し写像による振る舞いが，コントロールパラメータの値によって 3 つの状態（出力値が一定の値に収束，いくつかの値で振動，非周期的な出力）になることが知られている．

この写像を擬似乱数生成器として計算機上で実装する際にいくつか問題点がある．実数上で定義されたロジスティック写像に含まれる二乗演算によって写像するたびに小数点以下の桁数が倍になるため，計算結果が CPU 性能に依存してしまう．そこでロジスティック写像の入力値，出力値を整数に限定し，端数切り捨て処理により計算機での実装に適した整数上のロジスティック写像が提案された．しかし，ロジスティック写像では擬似乱数系列の生成に適

[1] 北九州市立大学, 福岡県北九州市若松区ひびきの 1–1, 1–1 Hibikino, Wakamatsu, Kitakyushu City, Fukuoka 808–0135, Japan
[2] 九州工業大学, 福岡県飯塚市川津 680–4, 680–4 Kawazu, Iizuka City, Fukuoka 820–8502, Japan
[3] 岡山大学, 岡山県岡山市北区津島中 1–1–1, 1–1–1 Tsushimanaka, Kita-ku, Okayama City, Okayama 700–8530, Japan
[a)] a9mca005@eng.kitakyu-u.ac.jp

したコントロールパラメータの値を取れる範囲が限定的であることと，出力値の上限下限がコントロールパラメータの値によって左右されることが問題点として残っている．

そこで我々は，上記の問題点を改善したピースワイズ・ロジスティック写像 [2] に着目した．ピースワイズ・ロジスティック写像は実数上で定義されているため，計算機上での実装を考えると整数上に定義する必要がある．本稿では整数上のピースワイズ・ロジスティック写像を定義し，分岐図，リアプノフ指数，周期，リンク長，NIST 検定の結果から写像の性質について考察する．

2. 準備

2.1 ロジスティック写像

R. May は連続時間の微分方程式を写像し，時間を離散的にすることでカオス的な振る舞いが起きることが示されている [1]．その一つとして，次式で定義される実数上のロジスティック写像によって繰り返し写像を行うことで系列を生成することができる (図 1)．

$$\mathrm{LM}(r) = \mu r(1-r), \qquad (0 \le r \le 1), \qquad (1)$$

ただし，μ をコントロールパラメータと呼び，$0 < \mu \le 4$ となる．実数上のロジスティック写像によって生成される系列 $\{r_i\}$ は $r_{i+1} = \mathrm{LM}(r_i) = \mu r_i(1-r_i)$ と表現され，コントロールパラメータの範囲 $(0.35699\cdots < \mu \le 4)$ において特定の周期を持たない不規則な変化をすることが知られている．また，この写像は初期値敏感性を有している．実数上では繰り返し計算することにより，計算回数を重ねる度に小数点以下の値が発散し，初期値によって全く異なる系列を生成する．しかし，不動点となる写像も存在し，一度出力値が不動点に落ち入るとそれ以降繰り返し計算しても得られる値は常に同じ値となる．そのためロジスティック写像を用いて系列を生成する際には，不動点に落ち入ることが無いように，初期値を選ぶ必要がある．

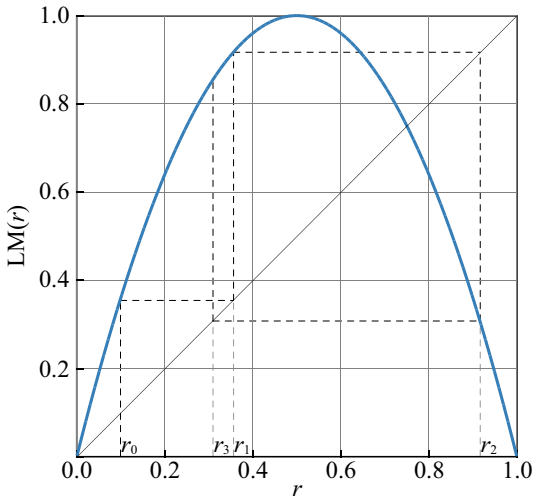

図 1 ロジスティック写像

2.2 整数上のロジスティック写像

ロジスティック写像を計算機上で実装する際にいくつかの問題点がある．その一つとして要素同士の乗算を含むので，繰り返し計算ごとに小数点以下の桁数が倍になる点が挙げられる．そのため初期値が同じだったとしても計算能力の異なる CPU 間で生成系列に差が生じる．そこで入力値，出力値を整数に限定し，小数点以下の計算処理は端数切り捨てを行う整数上のロジスティック写像が次式により定義されている．

$$X_{i+1} = \mathrm{LM}^{(n)}_{\mathrm{Int}}(X_i) = \left\lfloor \frac{\mu X_i(2^n - X_i)}{2^n} \right\rfloor, \qquad (2)$$

ただし，n は演算精度，$X_i \in \{0, 1, \cdots, 2^n\}$ とする．このように整数上のロジスティック写像は離散的な値をとるため，実数上でのロジスティック写像とは異なる性質を持つ．

周期

入力と出力を整数とするため，ある値 X_i から l 回の繰り返し演算によって得られる値 X_{i+l} がまた X_i に一致することがある．このとき X_i 以降の繰り返される写像をループ，その写像回数 l を周期と呼ぶ．また，X_0 から X_{i-1} までのループに入る前の系列をリンク，その写像回数をリンク長と呼ぶ．

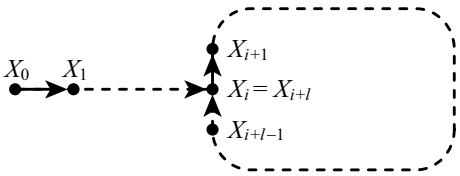

図 2 周期とリンク長

コントロールパラメータ

コントロールパラメータ μ は前述のように用いる値によって系列の振る舞いが異なる．

- 系列は収束する（$0 < \mu \le 3$）
- 系列は短い周期状態になる（$3 < \mu < 3.5699\cdots$）
- 系列は大きな周期をもつ（$3.5699\cdots \le \mu \le 4$）

整数上のロジスティック写像では，コントロールパラメータによって生成系列の性質が大きく異なるため，系列を生成する際に使用可能なコントロールパラメータの範囲が限定的になる．さらに，整数限定のため繰り返し写像の回数を増やしても出力値が発散することはない．実数上でのロジスティック写像では繰り返し計算するたびに小数点以下の値が発散するため，コントロールパラメータによる入力値と出力値の差が小さくなることは問題として挙げられなかった．しかし整数上では出力値は有限であるため，コントロールパラメータによって入力値と出力値の差が小さくなることは，演算精度に対して出力される値のバリエーションが少なくなることを意味する．

2.3 ピースワイズ・ロジスティック写像

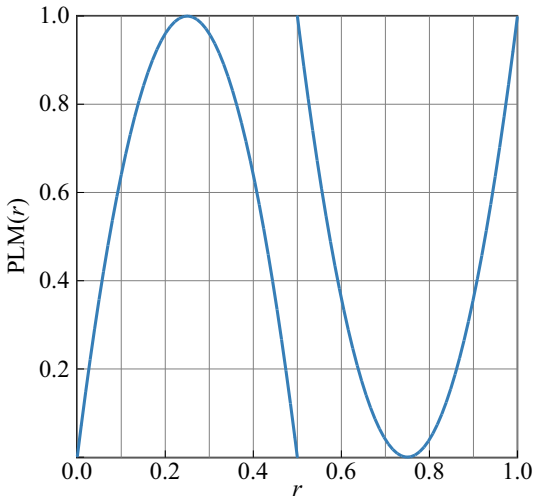

図 3 ピースワイズ・ロジスティック写像 ($N = 2$)

Y. Wang らによって提案されたピースワイズ・ロジスティック写像は，図 3 のように複数の区分に分割された領域にそれぞれ元のロジスティック写像が割り当てられる [2]．次に分割数 N のピースワイズ・ロジスティック写像の定義式を示す．

$$\mathrm{PLM}(r) = \begin{cases} N^2\mu r(\frac{1}{N} - r) & (0 < r < \frac{1}{N}), \\ 1 - N^2\mu r(\frac{1}{N} - r) & (\frac{1}{N} < r < \frac{2}{N}), \\ \quad \cdots & \\ N^2\mu(r - \frac{j-1}{N})(\frac{j}{N} - r) & (\frac{j-1}{N} < r < \frac{j}{N}), \\ 1 - N^2\mu(r - \frac{j-1}{N})(\frac{j}{N} - r) & (\frac{j}{N} < r < \frac{j+1}{N}), \\ \quad \cdots & \\ N^2\mu(r - \frac{N-2}{N})(\frac{N-1}{N} - r) & (\frac{N-2}{N} < r < \frac{N-1}{N}), \\ 1 - N^2\mu(r - \frac{N-2}{N})(\frac{N-1}{N} - r) & (\frac{N-1}{N} < r < 1), \end{cases}$$

ただし，N を分割数，j を N 区分の中の順番とする $(1 \le j \le N)$．Wang らによると，区分数を増やすと従来よりも低い μ で出力が広く分散されることが確認された．

3. ピースワイズ・ロジスティック写像の擬似乱数生成器としての計算機実装

実数上で定義されるピースワイズ・ロジスティック写像を擬似乱数生成器として計算機上に実装するには，ロジスティック写像のときと同様に二乗演算において CPU の種類やコンパイル環境によって端数処理が異なるため，同じ入力に対して異なる演算結果となる問題を生じる．そこでピースワイズ・ロジスティック写像の入力と出力を整数とする整数上のピースワイズ・ロジスティック写像を次式で定義する．このとき，演算精度を n，区分数を m とし，小数点以下は端数切り捨て処理を行うことで効率よく計算を行う．

m が偶数の時

$$\mathrm{PLM}_{\mathrm{Int}}^{(n,m)}(X_i) = \begin{cases} \left\lfloor \frac{m^2\mu X_i(\frac{1}{m}2^n - X_i)}{2^n} \right\rfloor & (0 \le X_i \le \frac{1}{m}2^n), \\ 2^n - \left\lfloor \frac{m^2\mu r_i(\frac{1}{m}2^n - r_i)}{2^n} \right\rfloor & (\frac{1}{m}2^n < X_i \le \frac{2}{m}2^n), \\ \quad \cdots & \\ \left\lfloor \frac{m^2\mu(X_i - \frac{j-1}{m}2^n)(\frac{j}{m}2^n - X_i)}{2^n} \right\rfloor & (\frac{j-1}{m}2^n < X_i \le \frac{j}{m}2^n), \\ 2^n - \left\lfloor \frac{m^2\mu(X_i - \frac{j-1}{m}2^n)(\frac{j}{m}2^n - X_i)}{2^n} \right\rfloor & (\frac{j}{m}2^n < X_i \le \frac{j+1}{m}2^n), \\ \quad \cdots & \\ \left\lfloor \frac{m^2\mu(X_i - \frac{m-2}{m}2^n)(\frac{m-1}{m}2^n - X_i)}{2^n} \right\rfloor & (\frac{m-2}{m}2^n < X_i \le \frac{m-1}{m}2^n), \\ 2^n - \left\lfloor \frac{m^2\mu(X_i - \frac{m-2}{m}2^n)(\frac{m-1}{m}2^n - X_i)}{2^n} \right\rfloor & (\frac{m-1}{m}2^n < X_i \le 2^n), \end{cases}$$

m が奇数の時

$$\mathrm{PLM}_{\mathrm{Int}}^{(n,m)}(X_i) = \begin{cases} \left\lfloor \frac{m^2\mu X_i(\frac{1}{m}2^n - X_i)}{2^n} \right\rfloor & (0 \le X_i \le \frac{1}{m}2^n), \\ 2^n - \left\lfloor \frac{m^2\mu r_i(\frac{1}{m}2^n - r_i)}{2^n} \right\rfloor & (\frac{1}{m}2^n < X_i \le \frac{2}{m}2^n), \\ \quad \cdots & \\ \left\lfloor \frac{m^2\mu(X_i - \frac{j-1}{m}2^n)(\frac{j}{m}2^n - X_i)}{2^n} \right\rfloor & (\frac{j-1}{m}2^n < X_i \le \frac{j}{m}2^n), \\ 2^n - \left\lfloor \frac{m^2\mu(X_i - \frac{j-1}{m}2^n)(\frac{j}{m}2^n - X_i)}{2^n} \right\rfloor & (\frac{j}{m}2^n < X_i \le \frac{j+1}{m}2^n), \\ \quad \cdots & \\ \left\lfloor \frac{m^2\mu(X_i - \frac{m-2}{m}2^n)(\frac{m-1}{m}2^n - X_i)}{2^n} \right\rfloor & (\frac{m-1}{m}2^n < X_i \le 2^n), \end{cases}$$

ただし，j を N 区分の中の順番とする．そこで，j が奇数の範囲は m が偶数のときに $j = 1, 3, 5, \cdots, m-1$，m が奇数のときに $j = 1, 3, 5, \cdots, m-2$ となる．なお，$m = 1$ では該当する j は存在しないが，m が奇数の場合の $\mathrm{PLM}_{\mathrm{Int}}^{(n,m)}(X_i)$ の一番上の式より，整数上のロジスティック写像と同等な式になることを確認できる．

また，コントロールパラメータ μ は

$$\mu = \frac{4 \times 2^{n+A} - M}{2^{n+A}}, \qquad (0 \le M \le 2^n) \tag{3}$$

と計算する．M, A は整数で A の値により μ の取りえる範囲が決まる．

表 1 A と μ との対応

A	-1	0	1	2	$\cdots$
μ	$2 \le \mu \le 4$	$3 \le \mu \le 4$	$3.5 \le \mu \le 4$	$3.75 \le \mu \le 4$	$\cdots$

4. $\mathrm{PLM}_{\mathrm{Int}}^{(n,m)}(X_i)$ の評価

整数上で定義された繰り返し写像 $\mathrm{PLM}_{\mathrm{Int}}^{(n,m)}(X)$ のコントロールパラメータによる乱数性を確認するために分岐図とリアプノフ指数を示すとともに，周期とリンク長，NIST 検定による評価を行う．

分岐図

分岐図は，各コントロールパラメータに対して対象とする系列の収束具合を視覚的に確認できるグラフで，実際には複数の初期値から生成される系列の数十番目以降の要素を用いて描画される．したがって，分岐図の縦方向に大きな空間があれば，対応するコントロールパラメータで生成される系列が収束する傾向にあることが想像できる．

リアプノフ指数

A. Lyapunov は一般的なシステムの安定性についての研究において，リアプノフ指数の符号によってそのシステムの安定性を判断できることを示した．ここに示すリアプノフ指数 λ は，X_i における写像関数 f の 1 階微分値 f' の対数を連鎖的に総和し，その平均値として求められる [3].

$$\lambda = \lim_{L\to\infty} \frac{1}{L} \sum_{i=0}^{L-1} \log |f'(X_i)| \tag{4}$$

リアプノフ指数が負である時はシステムが安定状態にあり，正の場合には発散状態にある．

整数上のピースワイズ・ロジスティック写像は離散値をとるため，微分不可能であり，そのまま適用することはできない．そのため，本稿では整数上のピースワイズ・ロジスティック写像で計算した出力値を実数上のピースワイズ・ロジスティック写像を微分した式に代入してリアプノフ指数を求める．次に $m = 1$ の場合を例に説明する．

$$f(X) = \frac{\mu X(2^n - X)}{2^n} \tag{5}$$

として両辺 X で微分をすると

$$f'(X) = \frac{\mu}{2^n}(2^n - 2X) \tag{6}$$

となる．式 (6) に整数 X_i を代入して擬似的なリアプノフ指数 λ_m を求める．

$$f'(X_i) = \frac{\mu}{2^n}(2^n - 2X_i) \tag{7}$$

$$\lambda_m = \lim_{L\to\infty} \frac{1}{L} \sum_{i=0}^{L-1} \log |f'(X_i)| \tag{8}$$

本来のリアプノフ指数と分岐図の関係性から，系列を生成する前から写像の乱数性を数学的に確認することができる．しかし，λ_m はあくまでも擬似的なリアプノフ指数であるため，分岐図との正確な対応関係を確認できていない．

周期とリンク長

暗号用途を想定した擬似乱数系列の生成には予測困難性が必要不可欠である．しかし，ロジスティック写像のような非線形の繰り返し写像では，予測困難性は周期に依存する．整数上のピースワイズ・ロジスティック写像では n の値で出力の最大値が決まり，同じ値が不規則に 2 回以上出力されることはないため，リンク長が長い場合は周期が短くなる．したがって，m の値によって周期にどのような影響があるのかを調べる必要がある．

NIST 検定

乱数検定評価ツールにはいくつかあるが，本稿では NIST 検定を用いる．米国商務省標準技術局 (NIST) が公開している乱数検定ツールであり，米国政府機関がセキュリティ対策を実施する際に利用することを前提に作成されている [4]．1Gbit 分の 2 進数乱数系列を 188 項目のテストにより乱数性を評価する．

4.1 コントロールパラメータによる収束

分岐図とリアプノフ指数を重ね合わせた図を図 4 に示す．それぞれの分岐図からコントロールパラメータによる出力の状態を確認する．$m = 1$ では $\mu \leq 3.56$ の範囲で出力が収束しているが，$m = 2$ では出力が収束するのは $\mu \leq 2.0$ の範囲となり，$m = 3$ では $\mu \leq 1.2$，$m = 4$ では $\mu \leq 1.0$ を除くと出力に関する収束は見られない．この結果より，m の値は μ の使用できる範囲に関係していることが分かる．また，出力の上限下限に注目すると，$m = 1$ では $\mu = 4$ で最大となり以降最大値と最小値の差は減少し，収束することになるが，$m = 2, 4$ では $\mu = 2.0$ 付近まで，$m = 3$ では $\mu = 2.4$ まで出力の分布が狭くなることはない．

またリアプノフ指数では，$m = 1$ において λ_m が正となる領域が $\mu \geq 3.4$ の範囲であり，$m = 2$ では $\mu \geq 1.8$，$m = 3$ では $\mu \geq 1.2$，そして $m = 4$ では $\mu \geq 1.0$ となっている．しかしながら，分岐図が縦に密となっているように見える部分でもリアプノフ指数が負となる箇所も散見される．この部分に対応する μ は他の分岐図が明らかに疎となっている部分と同じく系列が収束している．なお，本稿でのリアプノフ指数 λ_m は擬似的なものであり，$m = 4$ の $\mu = 2.5$ 付近では分岐図と対応することなく値が乱高下していると考える．

4.2 周期とリンク長

整数上のピースワイズ・ロジスティック写像は非線形写像のため，最大周期になる初期値を狙って選択することが困難である．そのため，各 m の値で $\mu = 4$ として，低い演算制度（小さな n）において平均周期と平均リンク長を求めて比較する．

一部を除いて $m = 2$ の場合がもっとも長い周期となり，$n = 36$ までは m が大きくなるにつれて周期は短く，$n \geq 37$ では $m = 3$ よりも $m = 4$ の方が長い周期となった（表 2）．$n = 40$ における平均周期を比較すると，一番大きい $m = 2$ に対する一番小さい $m = 3$ の場合においてもおよそ 72% 程であり，極端に周期が短くなることはない．

平均リンク長は $m = 1$ で最大となり，$m = 1$ 以外では m が増えるにつれて平均リンク長も長くなる傾向にある．

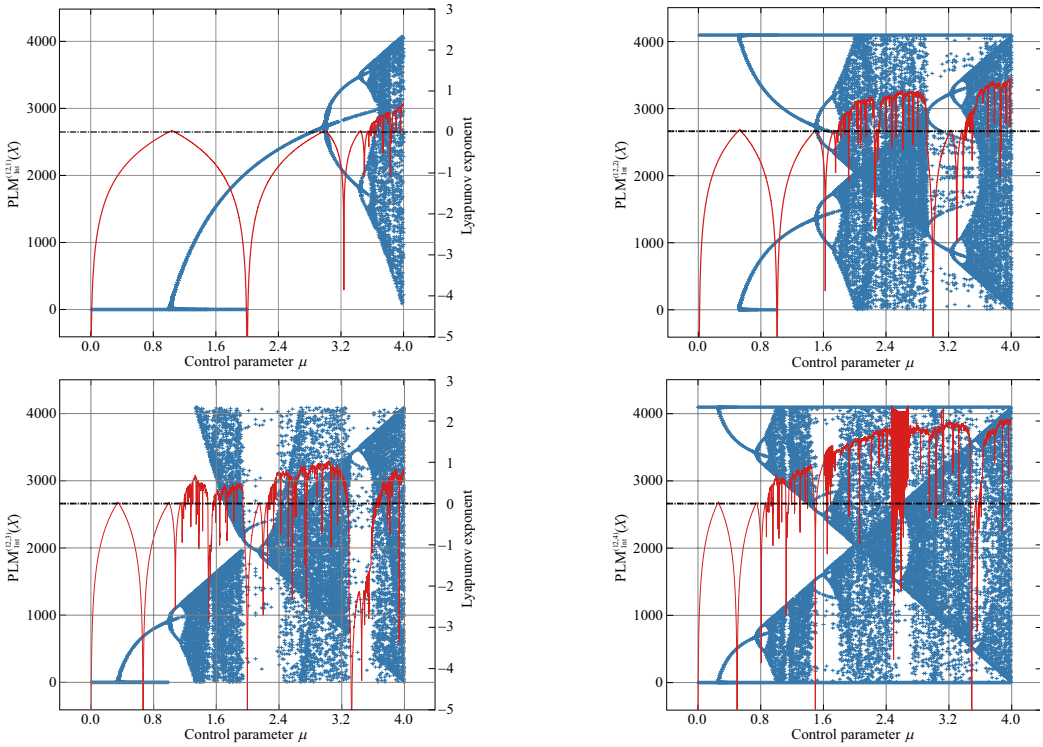

図 4　分岐図とリアプノフ指数

表 2　平均周期

演算精度	$\mathrm{PLM}_{\mathrm{Int}}^{(n,1)}$	$\mathrm{PLM}_{\mathrm{Int}}^{(n,2)}$	$\mathrm{PLM}_{\mathrm{Int}}^{(n,3)}$	$\mathrm{PLM}_{\mathrm{Int}}^{(n,4)}$
16bit	119	125	114	81
24bit	1,715	1,694	1,432	1,306
32bit	23,221	24,837	21,120	19,187
33bit	32,031	36,209	29,976	27,469
34bit	46,540	46,899	41,289	37,438
35bit	64,008	72,448	51,039	54,723
36bit	85,734	102,875	77,982	75,491
37bit	132,297	145,118	104,133	111,510
38bit	177,822	205,300	134,789	157,155
39bit	258,516	293,067	199,548	201,136
40ibt	332,336	385,928	279,025	302,017

表 3　平均リンク長

演算精度	$\mathrm{PLM}_{\mathrm{Int}}^{(n,1)}$	$\mathrm{PLM}_{\mathrm{Int}}^{(n,2)}$	$\mathrm{PLM}_{\mathrm{Int}}^{(n,3)}$	$\mathrm{PLM}_{\mathrm{Int}}^{(n,4)}$
16bit	120	79	106	96
24bit	1,700	1,110	1,442	1,254
32bit	23,175	16,048	20,573	19,858
33bit	33,097	24,687	29,643	25,910
34bit	44,250	33,974	41,271	37,655
35bit	62,427	48,714	49,816	56,510
36bit	94,717	66,957	71,486	74,262
37bit	134,676	96,321	101,492	113,831
38bit	186,960	135,129	147,774	160,091
39bit	251,286	179,609	208,807	213,160
40ibt	352,022	255,860	279,302	289,835

$n = 40$ における平均リンク長は，一番長い $m = 1$ に対して一番短い $m = 2$ の場合は約 73% となり，極端にリンク長が短くなることもない．

系列を $n = 40$ において平均周期の長さを順に並べると $m = 2, 1, 4, 3$ で平均リンク長の長さを順に並べると $m = 1, 4, 3, 2$ となった．しかし，分割数 m とコントロールパラメータ μ を選択する上で，m に対する平均周期と平均リンク長を比較した結果から大きな差はなく，m の値については特に優位性は見られない．

4.3　NIST 検定

本写像では，ランダムな初期値より 100 回写像した後に出力された下位 $\frac{2}{n}$bit を抽出して 1Gbit の擬似乱数系列を生成した．✓ は NIST 検定において全項目で合格したことを示し，B は 1 ∼ 3 の不合格の項目があることを表す．また，F は 4 項目以上で不合格になったことを示す．✓ の個数は $m = 1$ では 4 個，$m = 2$ では 12 個，$m = 3$ では 13 個，$m = 4$ では 17 個となり，区分数を増やすほど検定に全合格する個数は増える傾向にあった．また，B の検定不合格内容はほとんどの場合 NonOverlappingTemplate であった．

5.　結論

本稿では整数上のピースワイズ・ロジスティック写像を定義し，その性質について分岐図，リアプノフ指数，周期，リンク長，NIST 検定の項目で評価を行った．

分岐図より，分割数 m が増えることにより使用できるコントロールパラメータの選択肢が増えることが期待され，

表 4 NIST 検定結果 $n = 64$ $(2 \leq \mu < 3.9375)$

μ	2	2.0625	2.125	2.1875	2.25	2.3125	2.375	2.4375	2.5	2.5625	2.625	2.6875	2.75	2.8125	2.875	2.9375
$m = 1$	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
$m = 2$	✓	✓	✓	B	F	B	✓	✓	B	✓	B	B	✓	B	✓	F
$m = 3$	F	F	F	F	F	F	✓	✓	F	✓	B	✓	✓	✓	B	B
$m = 4$	✓	✓	✓	✓	✓	✓	✓	✓	F	F	F	B	✓	✓	B	✓
μ	3	3.0625	3.125	3.1875	3.25	3.3125	3.375	3.4375	3.5	3.5625	3.625	3.6875	3.75	3.8125	3.875	3.9375
$m = 1$	F	F	F	F	F	F	F	F	F	F	✓	B	✓	B	✓	✓
$m = 2$	F	F	F	F	F	F	F	B	F	✓	✓	B	F	✓	✓	B
$m = 3$	✓	✓	B	B	✓	F	F	F	F	✓	B	✓	B	✓	✓	✓
$m = 4$	B	B	✓	B	B	✓	✓	F	F	B	B	✓	✓	B	B	✓

リアプノフ指数と NIST 検定によって実際に使用できるコントロールパラメータが増えることを確認した．また出力値を $m = 1$ と $m = 2, 3, 4$ で比較すると，コントロールパラメータ μ がある程度低くても出力の上限下限が狭まることが少ないことを示した．次に，$\mu = 4$ において平均周期と平均リンク長をそれぞれ示し，最大のものと最小のものを比較した．どちらも最小のものは最大の 70 ∼ 75% 程になった．最後に，NIST 検定の結果から m が増加すると検定の全合格数する μ の範囲も増加する傾向となった．さらに，分岐図から区分数 m を増やせば生成系列の性質は改善されるが，区分数が周期やリンク長に与える影響は少ないことを確認した．

整数上のピースワイズ・ロジスティック写像では，$\mu = 4$ における各写像の頂点と $y = x$ と写像との交点，また各写像の分岐点（$\frac{j}{m}2^n$ 等）が出力されると，次の出力が 0 となって 0 ループや極端に周期が短くなることが問題として挙げられる．しかし，m が奇数の場合には，写像の分岐点が整数とならないため 0 ループに陥る可能性が少なくなると予測される．

今後の課題として，$m \geq 2$ における j の偶奇性によってコントロールパラメータを変化させて，小さな μ においても常に出力値が存在するような写像の提案とその評価について考察したい．

参考文献

[1] R.M. May, *Theoretical Ecoligy:Principles and Applications*, Blackwell Scientific Publishers. ISBN 0-632-00768-0, 1976.
[2] Y. Wang, Z. Liu, and P. Lei, “Cryptographic properties analysis of piecewise logistic Map,” Proc. of 2014 Inter. Symp. on Nonlinear Theory and its Applications, pp. 393-396, 2014.
[3] J. Kaplan and J.Yorke, “Chaotic behavior of multidimensional difference equations,” Functional Differenctial Equations and Approximation of Fixed Points, Lecture Notes in Mathematic, Volume 730, pp. 204-227, 1979.
[4] NIST, “A statistical test suite for random and pseudorandom number generators for cryptographic applications,” Special Publicatation 800-22, 2001.
[5] 合原一幸,「カオス学入門」, 放送大学振興会, 2001.
[6] 長島弘幸, 馬場良和,「カオス入門」, 培風館, 1992.
[7] T. Miyazaki, S. Araki, and S. Uehara, “Some properties of logistic maps over integers,” IEICE Trans. on Fundamentals, vol. E93-A, no. 11, pp. 2258-2265, Nov. 2010.
[8] T. Miyazaki, S. Araki, Y. Nogami, and S. Uehara, “Rounding logistic maps over integers and the properties of the generated sequence,” IEICE Trans on Fundamentals, vol. E94-A, no. 9, pp. 1817-1825, Sep. 2011.
[9] 董際国,「整数ロジスティック写像を用いた乱数生成法とその応用」, 電気通信大学博士論文, 2012.
[10] 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,” 電子情報通信学会論文誌, vol. J94-A, no.12, pp. 923-931, Dec. 2011.