整数上のロジスティック写像における制御変数の定義域の変化に対する出力値系列の類似性に関する一考察

小薗 元[1,a)]　荒木 俊輔[1]　宮崎 武[2]　上原 聡[2]　礒崎 賢一[1]

概要：本稿では，整数上のロジスティック写像を用いた擬似乱数生成に適した出力値系列を取得可能な制御変数の定義域について議論する．これまでは，整数上のロジスティック写像の特徴的な性質を調査するために，制御変数を区間 $[3, 4]$ としてきた．しかしながら，この区間には十分な乱数性を持つ出力を得ることが困難な範囲を含んでいる．そこで，制御変数の定義域を変化させて系列を取得し，その出力値系列の類似性を評価することにより制御変数の新たな定義域を示す．

キーワード：共通鍵暗号，暗号用ハッシュ関数・乱数，擬似乱数生成器，整数上のロジスティック写像，非線形写像

A Study on Similarity of Output Sequences for Different Domains of Control Parameter of the Logistic Map over Integers

Gen OSONO[1,a)]　Shunsuke ARAKI[1]　Takeru MIYAZAKI[2]　Satoshi UEHARA[2]
Ken'ichi KAKIZAKI[1]

Abstract: In the presented paper, we discuss the domain of the control parameter that can give suitable output sequences for pseudorandom number generatoion using the logistic map over integers. We defined the control parameter in the closed interval $[3, 4]$ because of investigating the characteristic properties of the logistic map over integers. However, the interval includes a range where it is difficult to obtain outputs with sufficient randomness. After we execute some numerical experiments, we will show a suitable definition of the control parameter.

Keywords: Common Key Cryptosystem, Cryptographic Hash Function · Random Number, Pseudorandom Number Generator, Logistic Map over Integers, Nonlinear Map

1. はじめに

May [9] により広く知られることとなったロジスティック写像は，写像の出力値を次の写像への入力とすることで，カオス的に振る舞う出力値系列を取得できる．この写像を用いた応用の一つに，暗号モジュール向けの擬似乱数生成器がある [1].

我々はロジスティック写像による写像の繰り返しにより得られたカオス的に振る舞う系列を元に擬似乱数を生成することを目標としている．ロジスティック写像では写像毎に値の表現に必要なビット長が倍になるため，メモリの容量に制約がある計算機上では写像の入出力値を有限精度で表現し，写像演算毎に端数処理を行う必要がある．このとき，有限精度下でのロジスティック写像の振る舞いは理想的な環境下での振る舞いとは異なるため，その振る舞いを把握した上で擬似乱数生成器の設計を決定する必要がある．そのため，我々は有限精度演算におけるロジスティック写像の振る舞いを研究している．特に，実装の容易さや演算の速さに着目して，整数演算下で定義されたロジスティッ

[1] 九州工業大学
Kyushu Institute of Technology, Fukuoka 820-0067, Japan
[2] 北九州市立大学
The University of Kitakyushu
[a)] gen.osono615@mail.kyutec.jp

ク写像である整数上のロジスティック写像について研究を進めている．

整数上のロジスティック写像を用いた擬似乱数生成器を構成する上で，3 つの基本操作とそれらから構成される擬似乱数生成器の基本モデルを定義した上で，写像の振る舞いに基づいてモデル内の操作毎の設計パラメータを定めるために，整数上のロジスティック写像の振る舞いに関する研究成果を示してきた [2–8]．

$0 \leq \mu \leq 4$ を満たす実数で与えられる制御変数を，他の変数と同様に整数値で扱えるように，定義式を与えた．これまでは，整数上のロジスティック写像の特徴的な性質を調査するために，$3 \leq \mu \leq 4$ に相当する範囲を設定できる制御変数の定義式を用いてきた．しかしながら，制御変数が $3 \leq \mu \leq 3.5$ に相当する範囲では，十分な乱数性をもつ出力を得ることが困難であることも分かってきた．

本稿では，擬似乱数生成器に適した出力値系列を取得可能な制御変数の定義域について議論する．

2. 整数上のロジスティック写像

一般的なロジスティック写像，すなわち実数上のロジスティック写像は

$$\mathrm{LM}_{\mathrm{R}}(r) = \mu r(1-r) \tag{1}$$

と表される．ここで，入力 r は $0 \leq r \leq 1$ を満たす実数値であり，制御変数 μ は写像の入出力値の関係を制御する $0 \leq \mu \leq 4$ を満たす実数値である．r_i を i 番目の入力とすると，式 (1) に対する繰り返し写像は

$$r_{i+1} = \mathrm{LM}_{\mathrm{R}}(r_i) \tag{2}$$

と書き表すことができる．$\mu = 4$ のとき，式 (2) が生成する出力系列 r_i は，カオス的な振る舞いを示すことで知られている．式 (1) より，ロジスティック写像は入力値の積を含んでいるため，出力値を表現するために少なくとも入力値の表現の倍のビット数が必要になる．そこで，ロジスティック写像をメモリ量に制約を持つ計算機上で実装するには，有限精度演算を必要とする．本稿では，演算精度と任意の精度実装の容易さに着目して，有限精度演算として整数値を用いる．この整数上のロジスティック写像はを以下のように簡単に導く．

整数の演算精度 n に対して，$\bar{r} = 2^n r$ とする．ここで，$0 \leq r \leq 1$ に対して，$0 \leq \bar{r} \leq 2^n$ である．すると $\overline{\mathrm{LM}}_{\mathrm{R}}^{(n)}(\bar{r}) = 2^n \mathrm{LM}_{\mathrm{R}}(r)$ より，式 (1) を

$$\overline{\mathrm{LM}}_{\mathrm{R}}^{(n)}(\bar{r}) = \frac{\mu \bar{r}(2^n - \bar{r})}{2^n} \tag{3}$$

と書き換えることができる．実数値 A に対して，$\lfloor A \rfloor$ を A の小数部を切り捨てる床関数とすると，整数上のロジスティック写像を

$$\mathrm{LM}_{\mathrm{Int}}^{(n)}(X) = \left\lfloor \frac{\mu X(2^n - X)}{2^n} \right\rfloor \tag{4}$$

と表せる．ここで，演算精度 n は写像の入出力値一つを表現するために用いるビット数である．入力値 X は $X = \lfloor \bar{r} \rfloor$ であり，$0 \leq X \leq 2^n$ を満たす整数値である．しかし，式 (4) では μ が実数値のままであり，系列にカオスな振る舞いが生じない値域を多分に含んでいる．そこで，この μ を整数値で制御するために，μ を

$$\mu = \frac{4 \cdot 2^{\alpha} \cdot 2^n - M}{2^{\alpha} \cdot 2^n} \tag{5}$$

と定義した．ここで，M は μ を制御するために定義された $0 \leq M \leq 2^n$ を満たす整数値である．式 (5) で表現される μ の値域は $3 \leq \mu \leq 4$ である．この値域の中にも系列にカオスな振る舞いが生じない値域が含まれている．これは整数上のロジスティック写像の振る舞いを調査するために，意図して含めている．また，$\alpha = 1$ のとき，μ の値域は $3.5 \leq \mu \leq 4$ であり，$\alpha = 2$ のとき，μ の値域は $3.75 \leq \mu \leq 4$ を満たす．このように，α を変化させることで，M の定義域を変えることなく，μ の定義域を変化させることができ，α が大きくなるにつれ，μ の最小値が 4 に近づく．

式 (5) を用いて，式 (4) を書き換えると

$$\mathrm{LM}_{\mathrm{Int}}^{(n,M)}(X) = \left\lfloor \frac{(4 \cdot 2^{\alpha} \cdot 2^n - M)X(2^n - X)}{2^{\alpha} \cdot 2^{2n}} \right\rfloor \tag{6}$$

となる．

$\mathrm{LM}_{\mathrm{Int}}^{(6,0)}(X)$ と $\mathrm{LM}_{\mathrm{Int}}^{(6,32)}(X)$，$\mathrm{LM}_{\mathrm{Int}}^{(6,64)}(X)$ における入出力の関係を図 1 に示す． 図 1 において，横軸は入力値，縦

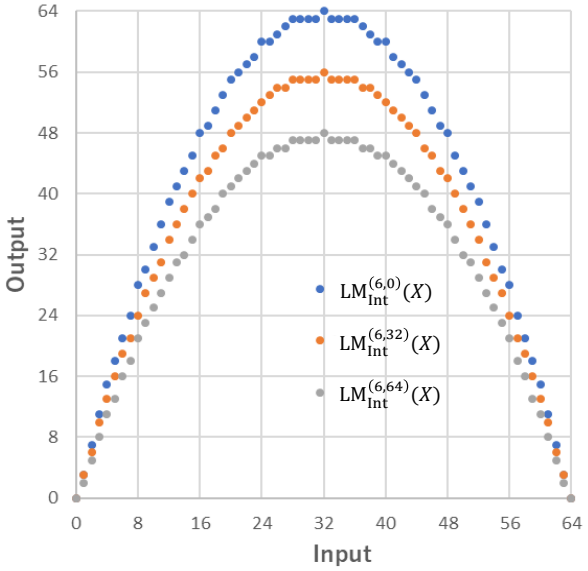

図 1 $\mathrm{LM}_{\mathrm{Int}}^{(6,0)}(X)$，$\mathrm{LM}_{\mathrm{Int}}^{(6,32)}(X)$，$\mathrm{LM}_{\mathrm{Int}}^{(6,64)}(X)$ における入出力の関係

軸は出力値であり，図中の点は写像の出力値を表している．図 1 より，M の変化によって写像の入出力の関係が変化していることが分かる．ただし，式 (5) より，M は μ との間に負の比例関係を持ち，M が 1 増える毎に μ は $1/2^n$ 減ることになる．例えば，$\mathrm{LM}_{\mathrm{Int}}^{(6,1)}(X)$ において，初期値

を 47 として式 (6) を用いて写像していくと，出力値系列は $\{47, 49, 45, 53, 36, ...\}$ となる．本稿では，これ以降 M を制御変数と呼ぶ．

3. 制御変数の定義域と分岐図

3.1 分岐図

分岐図とは，$0 \leq M \leq 2^n$ を満たす M の値に対して過渡現象を除いた軌道の最終的な振る舞いを示したものである．本稿では，以下の手順で分岐図を求める．

[分岐図作成手順]

(1) 初期パラメータを $M = 0$，$X = 1$ とする．

(2) 式 (6) を用いて写像の出力値の計算を行う．このとき，始めの 100 回の写像の反復は無視し，101 回目から 1000 回目までの値をプロットする．

(3) $M \leq 2^n$ であれば，M を決められた増分だけ増やし，手順 2 に戻る．

以降で示す分岐図は $n = 16$, M の増分を $256(= 2^8)$ としたときのものである．

式 (5) において，$\alpha = 0$ とする．このとき，制御変数の値域は $3 \leq \mu \leq 4$ となり，整数上のロジスティック写像の出力値そのものを取得できる．$n = 16$ における $\alpha = 0$ が表す値の分岐図を図 2 に示す．

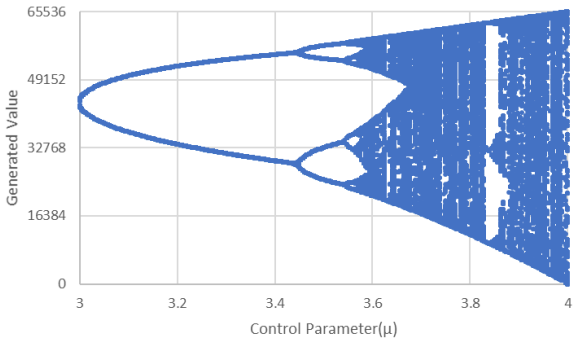

図 2　$n = 16$ における $\alpha = 0$ が表す値の分岐図

なお，図 2 において，横軸は制御変数 μ，縦軸はその制御変数のときの周期的な軌道を示している．以降，同様グラフでは，横軸は制御変数 μ，縦軸はその制御変数のときの周期的な軌道を示し，横軸の左端が $\mu = 3$，右端が $\mu = 4$ に対応するように，M を横軸から降順に並べている．これより，ロジスティック写像が生成する系列が持つカオスな振る舞いは，整数上のロジスティック写像の生成する系列にも現れていることが見て取れる．また，μ の定義を式 (5) と与えることで，M の分解能を変えないまま制御変数 μ の区間を変えることができるようになった．

$n = 16$ における $\alpha = 1$ が表す値の分岐図を図 3 に，$n = 16$ における $\alpha = 2$ が表す値の分岐図を図 4 に，$n = 16$ における $\alpha = 3$ が表す値の分岐図を図 5 にそれぞれ示す．

図 2,3 より α が小さいときは，μ の最小値が 3 に近くなるため，十分な乱数性を持つ出力を得ることが困難である領域を多分に含んでいることが分かる．逆に α が大きくなるにつれ，μ の最小値が 4 に近づくので，図 5 のように乱数性が十分でない領域を外すことができ，制御変数 M の値域 $0 \leq M \leq 2^n$ の値をよりまんべんなく出力されるようになるため，一見すると，より乱数生成に適した系列を取得できる制御変数の定義に変化する．

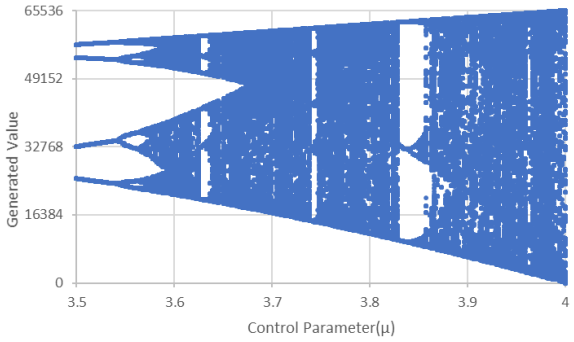

図 3　$n = 16$ における $\alpha = 1$ が表す値の分岐図

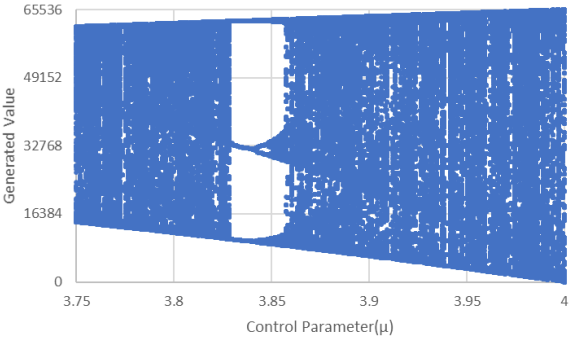

図 4　$n = 16$ における $\alpha = 2$ が表す値の分岐図

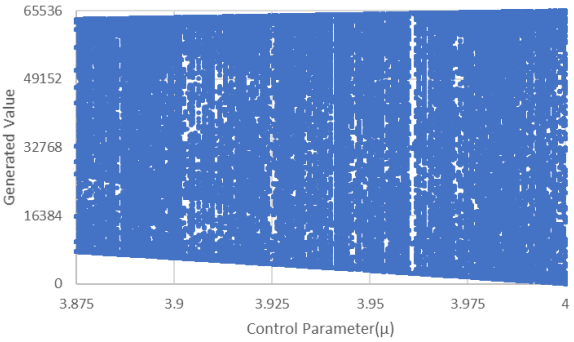

図 5　$n = 16$ における $\alpha = 3$ が表す値の分岐図

4. 制御変数の定義域の変更による出力系列の類似度

制御変数が大きく異なれば，同じ初期値でも異なる出力値系列を得ることができる．例えば，$\mathrm{LM}_{\mathrm{Int}}^{(6,34)}(X)$ において，初期値を 47 として式 (6) を用いて写像していくと，出力値系列は $\{47, 43, 48, 41, 51, ...\}$ となり，2 章で示した $\mathrm{LM}_{\mathrm{Int}}^{(6,1)}(X)$ における出力値系列と比べると，同じ初期値であってもすぐに異なる出力値系列を取得できる

ことが分かる．一方，$\mathrm{LM}_{\mathrm{Int}}^{(6,35)}(X)$ において，初期値を 47 として式 (6) を用いて写像していくと，出力値系列は $\{47, 43, 48, 41, 50, ...\}$ となり，$\mathrm{LM}_{\mathrm{Int}}^{(6,34)}(X)$ における出力値系列と比べると，同じ初期値だと異なる出力値系列を取得するまでに何回か写像しなければならない．このように，制御変数が $M, M+1$ のように近いときは，同じ初期値だと異なる出力値系列を取得するまで数回写像を待たなければならない．そこで本章では，隣り合う制御変数，すなわち M と $M+1$ における同じ初期値のときの出力値系列の類似度について議論する．

隣り合う制御変数のような悪い条件下でも，異なる制御変数が与えられたとき，たとえ初期値が同じであっても異なる系列となることを期待する．そこで，制御変数 M と $M+1$ の写像において，同じ初期値が与えられたとき，何回目の写像で異なる値を出力するようになるのかを調査した．

表 1 ～ 6 において，Quantity は，何回かの写像の後，異なる出力値系列となった初期値の個数である．つまり，10000 に満たない項目は，同じ要素からなるループに至り，何度写像しても同じ出力値系列のままである初期値が存在することを示している．α が大きくなるにつれ，同じ出力値系列のままでループに至る初期値が増え，期待とは異なる結果を示している．

一方 Average は，異なる値が出力された平均写像回数であり，Average が小さいほど，少ない写像回数で異なる出力値系列を得ることができる．

表 1 $n = 16$ のときの実験結果

α	Link	Loop	Quantity	Average
0	110.36	45.99	9795	5.45
1	138.4	48.46	9772	11.64
2	228.57	64.98	9487	23.89
3	107.12	132.34	8929	45.35
4	84.43	54.49	7431	71.29
5	100.75	91.59	5182	93.64
6	53.43	45.56	3043	108.18
7	88.59	149.6	1774	114.43
8	115.55	93.7	855	109.96
9	92.63	79.72	435	112.05
10	91.04	103.55	215	114.5

表 2 $n = 17$ のときの実験結果

α	Link	Loop	Quantity	Average
0	92.08	83.32	9856	5.46
1	132.83	124.27	9868	11.69
2	160.37	211.16	9639	24.26
3	144.75	186.41	9306	48.44
4	173.35	174.45	8122	82.73
5	107.4	161.32	6189	114.59
6	207.49	140.24	3963	141.41
7	130.74	202.55	2256	151.34
8	24.98	25.45	1214	153.75
9	146.35	167.73	601	157.6
10	66.66	128.66	317	157.32

表 3 $n = 18$ のときの実験結果

α	Link	Loop	Quantity	Average
0	85.99	71.25	9877	5.52
1	143.78	191.54	9899	11.74
2	208.65	179.96	9736	24.61
3	211.08	163.1	9605	50.45
4	183.11	205.44	8775	91.71
5	211.47	179.03	7104	141.32
6	151.74	107.49	4901	179.16
7	208.37	180.17	2881	199.54
8	239.28	200.94	1551	217.56
9	21.9	36.32	777	216.28
10	196.61	192.34	401	216.68

表 4 $n = 19$ のときの実験結果

α	Link	Loop	Quantity	Average
0	190.34	71.37	9902	5.48
1	263.1	207.69	9919	11.69
2	225.67	286.85	9814	25.29
3	298.67	335.86	9750	51.57
4	293.72	271.29	9164	98.73
5	173.05	299.97	8009	163.97
6	313.65	276.93	5827	225.5
7	218.2	263.79	3677	266.31
8	10.2	1	47	4.43
9	284.05	276.92	913	294.81
10	207.41	155.81	158	203.09

表 5　$n = 20$ のときの実験結果

α	Link	Loop	Quantity	Average
0	227.82	177.24	9921	5.48
1	424.75	327.91	9937	11.76
2	419.52	379.97	9853	25.23
3	432.78	365.99	9843	53.18
4	395.39	403.1	9525	105.16
5	4.3	1	421	4.91
6	397.2	407.48	6136	290.09
7	264.99	244.52	1636	267.84
8	238.58	154.42	377	185.68
9	82.77	83.54	65	136.22
10	89.22	103.03	13	89.23

表 6　$n = 21$ のときの実験結果

α	Link	Loop	Quantity	Average
0	24.68	23.25	9928	5.47
1	383.83	428.9	9950	11.84
2	17.57	1	5312	8.12
3	134.38	153.67	9891	74.19
4	360.16.25	359.05	7854	203.68
5	282.25	252.55	3051	238.06
6	166.52	157.17	703	181.3
7	122.79	134.62	144	119.58
8	89.7	93.58	22	77.82
9	50.13	53.81	10	32.4
10	50.23	50.32	4	10.75

5. 出力値系列についての評価

4 章より，Quantity は 10000 個の初期値のうち，異なる出力値系列を取得できた初期値の個数である．この値が 10000 に近いほど，隣り合う制御変数によって異なる出力値系列を取得できる初期値が多いということである．Average は，異なる値が出力された平均写像回数であり，Average が小さいほど，少ない写像回数で異なる出力値系列を得ることができる．よって，α に対して，Quantity は大きい方が良く，Average は小さいほうが良い．つまり，α を大きくすると，μ の最小値が 4 に近くなり，2 章の分岐図から，一見望ましいように見える．

しかしながら，表 1 ～ 6 の結果より，$\alpha = 8$ 以上のとき，Quantity の値が 10000 と比べて小さくなりすぎているので，α を大きくしすぎるのは問題であることが分かった．

では，逆に $\alpha = 0, 1$ のように，α が小さい場合を考える．表 1 ～ 6 の結果では，α に対して，Quantity は大きく，Average は小さいため，一見望ましいように見える．しかし，2 章で述べたように，α が小さいと，μ の最小値が 3 に近くなるため，十分な乱数性を持つ出力を得ることが困難である領域を多分に含んでいるので α が小さすぎるのも問題であることが分かった．

よって，Quantity と Average の大きさのバランスを鑑みると，今回の数値実験では，$\alpha = 3$ もしくは 4 が適切であることが分かった．$\alpha = 3$ のとき，制御変数の値域は $3.875 \leq \mu \leq 4$ である．さらに，$\alpha = 4$ のとき，制御変数の値域は $3.9375 \leq \mu \leq 4$ であるので，2 章の分岐図を考えても十分な乱数性をもつ系列を取得できる領域であるといえる．

6. おわりに

本研究では，整数上のロジスティック写像による写像の繰り返しによって得られたカオス的に振る舞う系列を元に擬似乱数を生成することを目的としている．これまでは，整数上のロジスティック写像の特徴的な性質を調査するために，$3 \leq \mu \leq 4$ に相当する範囲を設定できる制御変数の定義式を用いてきた．しかしながら，十分な乱数性を持つ出力を得ることが困難である領域が存在する．

整数上のロジスティック写像では，生後変数が大きく異なれば，同じ初期値であっても異なる出力値系列を取得することができる．そこで本稿では，隣り合う制御変数のような悪い条件下でも，異なる制御変数が与えられたとき，たとえ初期値が同じであっても異なる系列となることを期待し，隣り合う制御変数 M と $M + 1$ の写像において，同じ初期値が与えられたとき，何回目の写像で異なる値を出力するようになるのかを調査した．また，α によって制御変数の定義域が変更された場合，制御変数 M と $M + 1$ の写像が同じ系列を取得する確率を調査した．

その結果，α を大きくしすぎると，隣り合う制御変数によって得られる出力値系列が異なる初期値が少なくなるため，α が大きければ良い，つまり，制御変数 μ の値域の最小値が 4 に近づくことが必ずしも良いということは言えないことが分かった．

今後の課題として，本稿では，最大演算精度を 21 ビットとして調査した．これまでの研究で，演算精度が 50 数ビットであれば整数上のロジスティック写像を用いた単純な構成をもつ擬似乱数生成器でも擬似乱数出力が NIST 検定 [10] を合格できることを確認している．よって，50 ビットを超えるような演算精度で今回のような調査を行いたい．

また，今回の実験では，$\alpha = 3$ もしくは 4 が適切であることが分かったと述べた．しかし，これはあくまでも制御変数 μ の定義域が適切であれば，取得できる出力値系列は十分な乱数性があるだろうという予想であるため，それが正しいことを証明するために，NIST の乱数検定を用いて乱数性の評価を行いたい．

参考文献

[1] S. Phatak and S. Rao, “Logistic map: A possible random number generator,” Phys. Rev. E, Vol. 51, Iss. 4, pp. 3670-3678, 1995.
[2] T. Miyazaki, S. Araki and S. Uehara, “Some properties of logistic maps over integers,” Special Section on Signal Design and its Applicationin Communications, IEICE Trans. Fundamentals, Vol. E93-A, No. 11, pp.2258-2265, 2010.
[3] T. Miyazaki, S. Araki and S. Uehara, “Relations between periods and control parameters in the logistic maps over integer,” IEICE Trans., Vol. E93-A, No. 11, pp. 2258-2256, 2010.
[4] S. Araki, T. Miyazaki, S. Uehara and K.Kakizaki, “A study on precision of pseudorandom number generators using the logistic map,” Proc. of International Symposium on Information Theory and its Applications(ISITA2012), pp.740-744, 2012.
[5] S. Araki, T. Miyazaki, S. Uehara and K. Kakizaki, “A study on distance between two seq uences by the logistic map over integers with slightly different parameters,” Proc. of the Sixth Intern ational Workshop on Signal Design and its Application in Communications, pp.64-67, 2013.
[6] 荒木, 宮崎, 上原, 碓崎, “整数上のロジスティック写像におけるビット毎の出現確率に関する考察,” 日本応用数理学会論文誌, 25 巻 3 号, pp.191-206, 2015.
[7] H Muraoka, S. Araki, T. Miyazaki, S. Uehara and K.Kakizaki, “Occurrence Rate per Bit for Any Control Parameter on the Logistic Map over Integers,” Proc. of International Symposium on Informati on Theory and its Applications(ISITA2016), pp.822-826, 2016.
[8] 村岡, 荒木, 宮崎, 上原, 碓崎, “整数上のロジスティック写像を用いた疑似乱数生成器におけるビット抽出位置と乱数性の関係に関する考察,” 2017 年 暗号と情報セキュリティシンポジウム予稿集,4B2-1, pp.1-8, 2017.
[9] R. May, “Simple mathematical model with very complicated dynamics,” Nature, Vol. 261, No. 5560, pp. 459-467, 1976.
[10] NIST, “A statistical test suite for random and pseudorandom number generators for cryptographic applications,” Special Publication 800-22, 2001.