Vol. 27 No. 3 情報処理学会論文誌 Mar. 1986

擬似乱数とカオス†

香田 徹†† 柿本厚志††

擬似乱数発生器として非線形写像で生成されるカオスを利用しようとする試みが行われている．この際，カオスが従来の擬似乱数と比較して，乱雑さに関する性質の良い乱数であるか否かがまず問題とされなければならないが，これに関する検討は十分ではない．性質の良い乱数を定義することは容易ではなく，また，実数値系列の乱雑さの度合いの測定も容易ではない．与えられた実数値系列を閾値関数により2値系列に変換し，2値系列の乱雑さから実数値系列のそれを検討する方法が最近提案されている．本稿では，性質の良い乱数に関する一つの考え方を提案する．すなわち，変換して得られる2値系列が閾値とは無関係に常にベルヌイ試行に十分近いとき，もとの実数値系列を性質の良い乱数とみなすものである．このような考え方にたつと，従来の擬似乱数の検定法では，任意の閾値に対して得られる2値系列とベルヌイ試行との近さを議論していないので従来の検定法は十分ではない．本稿では，ロジスティック写像で生成されるカオスの乱雑さと従来の擬似乱数発生法としての線形合同法，M系列，平方採中法による数列のそれとを比較検討した．なお，与えられた2値系列とベルヌイ試行との近さは連テストと組合せテストの χ^2 検定により測った．その結果，従来の擬似乱数の方がカオスより性質の良い乱数であるとの結論を得た．

1. まえがき

カオスを擬似乱数として用いようとする試みのために，カオスと乱数の関係がしばしば議論の対象とされている[6),7),9)]．カオスを擬似乱数発生器として用いる場合には，カオスが従来の擬似乱数と比較して乱雑さに関して十分に性質の良い乱数であるか否かがまず問題とされなければならないが，これに関する検討は十分とは言えない．乱雑さに関する性質の良い乱数を定義することは難しい問題であり，また，与えられた実数値系列の乱雑さの度合いの測定も容易ではない[1)]．与えられた実数値系列 $\{x_n\}_{n=0}^{\infty}$ を2値系列 $\{\sigma_c(x_n)\}_{n=0}^{\infty}$ ($\sigma_c(x)$ は $x \leq c$ ($x>c$) により "0" ("1") を取る) に変換し，2値系列の乱雑さでもとの実数値系列のそれを検討しようとする方法が最近提案されている[6),7)]．与えられた2値系列の乱雑さは，乱雑な2値系列の典型例であるベルヌイ試行との近さで測ることができる．

本稿は，性質の良い乱数に関する一つの考え方を提案しようとするものである．すなわち，変換して得られる2値系列が，閾値 c とは無関係に常にベルヌイ試行に十分近いとき，もとの実数値系列は性質の良い実数値型のベルヌイ試行発生器であるので，その実数値系列を性質の良い乱数とみなそうとするものである．

しかしながら，従来の擬似乱数の検定法においては，特定の c の値 ("0", "1"の生起確率が等しくなるような値) に対して得られた2値系列とベルヌイ試行との近さだけが検討されており，それ以外の任意の c に対して得られた2値系列とベルヌイ試行との近さに対する検討はほとんど行われていない[2)~4)]．

本稿は，上記のことに鑑み，ロジスティック写像で生成される "pure chaos"[13)] と呼ばれるカオスの乱雑さと従来の擬似乱数発生器としての線形合同法，M系列，平方採中法による数列のそれとを比較検討しようとするものである[11)]．与えられた2値系列とベルヌイ試行との近さの測定は，従来の検定法である連テストや組合せテスト以外にも，酔歩問題のモンテカルロ・シミュレーションによる方法 (以後，酔歩テストと呼ぶ) などがある[6)~8),11)]．前稿[11)]では，酔歩テストにより，上記の乱数に関する検定を行い，カオスは，従来の擬似乱数と比較して，性質の良い乱数ではないとの結論を得た．通常の擬似乱数検定法では，連テスト，組合せテストが最も一般的な方法であるので，本稿では任意の閾値 c に対して得られた2値系列とベルヌイ試行との近さはこれらの方法を用いて測ることとした．その結果，前稿と同様の結論が得られた．すなわち，従来の擬似乱数は適切な初期値を選べば，性質の良い実数値型ベルヌイ試行発生器であるのに対し，ロジスティック写像は写像の多重化を行わなければ性質の良い実数値型ベルヌイ試行発生器にならないということである．したがって，カオス擬似乱数発生器として用いるにはさらに詳しい考察が必要であろう．

† Pseudorandom Number Generators and Chaotic Orbits in the Logistic Map by TOHRU KOHDA and ATSUSI KAKIMOTO (Department of Computer Science and Communication Engineering, Faculty of Engineering, Kyushu University).

†† 九州大学工学部情報工学科

2. 2値系列の乱雑さに関する検定

2.1 ベルヌイ試行発生器

非線形写像

$$y=\tau(x)x,\quad y\in[0,\ 1] \tag{1}$$

によって生成されるカオスと呼ばれる解軌道は，あたかも確率的な事象であるかのように不規則な振舞いを示す．このような性質から，カオスと乱数の関係はしばしば議論の対象とされ，これまでにカオスを擬似乱数発生器として用いようとする研究が幾つか行われている[6),7),9)]．カオスを擬似乱数発生器として用いる場合には従来の擬似乱数発生器と比較して，カオスが十分に性質の良い乱数であるか否か，また，簡便な発生法であるか否かという評価が，まず問題とされるべきであろう[1)]．性質の良い乱数の定義は難しい問題であり，実数値系列の乱雑さの度合いの測定も容易ではない[1)]．与えられた実数値系列 $\{x_n\}_{n=0}^{\infty}$ を2値系列変換法

$$\sigma_c(x)=\begin{cases}1, & x>c\\ 0, & x\leq c\end{cases} \tag{2}$$

で2値系列 $\{\sigma_c(x_n)\}_{n=0}^{\infty}$ に変換し，その2値系列からもとの実数値系列の乱雑さを検討しようとする方法が提案されている[6)]．

本稿では式(2)から得られた $\{\sigma_c(x_n)\}_{n=0}^{\infty}$ が閾値 c と全く無関係にベルヌイ試行に近いときに，もとの実数値系列 $\{x_n\}_{n=0}^{\infty}$ を性質の良い実数値型のベルヌイ試行発生器であると呼ぶことにする．さらに，ベルヌイ試行発生器であるような $\{x_n\}_{n=0}^{\infty}$ は性質の良い乱数の一種であると考えることにする．従来の検定法においては[2)~4)]，与えられた2値系列とベルヌイ試行との近さを“0”，“1”の生起確率が等しい場合しか測っていないので，与えられた2値系列が等確率のベルヌイ試行発生器であることを保証しているに過ぎない．そこで，2.2, 2.3節で，各々“0”，“1”の生起確率が等しくない場合の連テスト，組合せテストについて考えることにする．

2.2 等確率でないベルヌイ試行を用いた連テスト

よく使用される連テストには2通りある[1),2)]．一つは乱数列 $\{x_n\}$ について検定する方法で，その値の増加の傾向（上昇連）あるいは減少の傾向（下降連）について検定する方法で，他の一つは乱数列 $\{x_n\}$ が閾値 c より小なら“0”，大なら“1”を対応させてできる“0”，“1”の系列中に同種の値が続く長さについて検定する方法である[2)~4)]．本稿では与えられた2値系列のベルヌイ試行への近さを検討の対象としているので，後者のテストを用いることにする．“0”，“1”の生起確率が等しい場合のベルヌイ試行を L 回行ったとき，長さ d の連の発生頻度は

$$\langle r(d;\ 1,\ L)\rangle=(L-d+3)/2^{d+1} \tag{3}$$

となることが一般に知られている[2)~4)]．式(3)の導出と同様な計算で，等確率でないベルヌイ試行における連の発生頻度が容易に得られることを以下に示す．

“0”，“1”の生起確率を各々 p, q とし

$$\theta=p/q \tag{4}$$

と置く．長さ d の“1”の連は，両端が“0”で挟まれている場合と系列の端にある場合のどちらかであって，そのような連の生起確率は各々，

$$P\{0\ 1^d\ 0\}=p^2\cdot q^d \tag{5}$$

$$P\{0\ \ 1^d\}=P\{1^d\ 0\}=p\cdot q^d \tag{6}$$

で表される．ただし，$P\{\text{event}\}$ は事象“event”(あるいは系列）が起きる確率を表し，1^d は“1”が d 個続くことを意味する．ベルヌイ試行を L 回行うとすれば，全試行の中に $\{0\ 1^d\ 0\}$ の現れ方は $(L-d-1)$ 通りである．これと $\{0\ 1^d\}$, $\{1^d\ 0\}$ の現れ方が各々1通りずつあるので長さ d の“1”の連の発生頻度は

$$\begin{aligned}&(L-d-1)P\{0\ 1^d\ 0\}+P\{0\ 1^d\}+P\{1^d\ 0\}\\&=p^2\cdot q^d\cdot(L-d-1+2/p)\\&=\theta^2\cdot(L-d+1+2/\theta)/(1+\theta)^{d+2}\end{aligned} \tag{7}$$

となる．同様に長さ d の“0”の連の発生頻度は

$$\theta^d\cdot(L-d+1+2\theta)/(\theta+1)^{d+2} \tag{8}$$

となる．故に，“0”，“1”の生起確率の比が θ であるベルヌイ試行を L 回行ったときに，長さ d の“0”または，“1”の連が発生する頻度は

$$\langle r(d;\ \theta,\ L)\rangle=\frac{(L-d+1)(\theta^2+\theta^d)+2\theta(\theta^d+1)}{(\theta+1)^{d+2}} \tag{9}$$

となる．一方，与えられた長さ L の2値系列における長さ d の連の発生頻度を $[r(d;\ \theta,\ L)]$ とすれば，その系列とベルヌイ試行との近さは通常の χ^2 検定法に従い以下のように測ることとする．$\langle r(d;\ \theta,\ L)\rangle$ の分布の自由度を ν とする（すなわち，連に関する事象を $(\nu+1)$ 個の互いに排反な事象に分ける）．ただし，$\langle r(d;\ \theta,\ L)\rangle$ $\langle 10$となるような事象は一括して一つの事象とみなすこととする．i 番目の事象を E_i で表す．ベルヌイ試行及び与えられた系列における E_i の発生頻度をそれぞれ $\langle r(d_i;\ \theta,\ L)\rangle$, $[r(d_i;\ \theta,\ L)]$ とする．統計量

$$\chi^2_\nu=\sum_{i=0}^{\nu}\frac{\{[r(d_i;\ \theta,\ L)]-\langle r(d_i;\ \theta,\ L)\rangle\}^2}{\langle r(d_i;\ \theta,\ L)\rangle} \tag{10}$$

を計算する．自由度 ν の χ^2 分布から有意水準5％の χ^2 の値 χ_0^2 を求める．次の比

$$\xi_\nu=\chi_\nu^2/\chi_0^2 \tag{11}$$

を定義しよう[3]．以後，通常の χ^2 検定法と同様に $\xi_\nu<1$ ならば，与えられた2値系列はベルヌイ試行に十分近い系列であるとする[3]．

2.3 等確率でないベルヌイ試行を用いた組合せテスト

“0”, “1” の生起確率が各々，p, q（比が θ）であるベルヌイ試行を L 回行ったとする．この2値系列を k 組($k=L/h$：本稿では $h=20$ とした）に分けるとすれば，一つの組の中に “1” が d 個現れる確率は

$$P\{\mathrm{Num}(1)=d\}={}_h\mathrm{C}_d\cdot q^d\cdot p^{h-d}={}_h\mathrm{C}_d\cdot\theta^{h-d}/(1+\theta)^h \tag{12}$$

で表される．ただし，Num(1)は一組中の “1” の個数を意味する．したがって，“0”, “1” の生起確率の比が θ であるベルヌイ試行を L 回行ったとき，k 組の中で “1” の数が d 個となる組の発生する頻度は

$$\langle m(d;\theta,L,K)\rangle=k\cdot P\{\mathrm{Num}(1)=d\}=k\cdot{}_h\mathrm{C}_d\cdot\theta^{h-d}/(1+\theta)^h \tag{13}$$

となる．一方，与えられた長さ L の2値系列における k 組中，“1” の数が d 個である組の発生頻度を $[m(d;\theta,L,k)]$ で表し，連テストと同様に両頻度を χ^2 検定に適用して，与えられた2値系列とベルヌイ試行との近さを測ることとする．

3. 検定結果

3.1 ロジスティック写像の検定結果

ロジスティック写像

$$\tau_b(x)=bx(1-x) \tag{14}$$

は，カオスが存在する非線形写像として著名で，$b=4.0$ のとき，そのカオスは “pure chaos” と称されている[13]．式(14)で生成される実数値系列 $\{\tau_b^n(x)\}_{n=0}^{\infty}$ の乱雑さに関しては，いろいろ検討されている[6)-8),11)]．

表1 ロジスティック写像における b, c と θ の関係

Table 1 Ratio θ of probability of outcomes “0” and one of “1” in chaotic sequences generated by the logistic map τ_b with a parameter b when the threshold c of the real-to-binary transformation and b are varied.

b \ c	0.2	0.3	0.4	0.45	0.5	0.55	0.6	0.7	0.8
3.62			0.26	0.40	0.55	0.64	0.78	1.00	1.43
3.70		0.10	0.20	0.24	0.29	0.37	0.45	0.76	2.32
3.80	0.50	0.19	0.29	0.34	0.39	0.46	0.63	1.05	1.86
3.90	0.17	0.26	0.50	0.64	0.75	0.86	0.99	1.28	1.71
3.99	0.34	0.49	0.66	0.75	0.85	1.00	1.15	1.56	2.20
3.999	0.38	0.54	0.72	0.82	0.93	1.06	1.21	1.51	2.31
4.0	0.42	0.59	0.77	0.88	1.00	1.13	1.29	1.71	2.39

表2 連テストにおけるロジスティック写像の b, c と ξ_ν の関係

Table 2 Ratio $\xi_\nu=\chi_\nu^2/\chi_0^2$ of the run test for chaotic sequences generated by the logistic map τ_b with a parameter b when the threshold c is varied. ν indicates of the number of the degrees of freedom whose the expected frequencies $\langle r(d;\theta,L)\rangle$ of the run test for Bernoulli trials with the ratio θ is given by Eq. 9. d and L represent the run length and the sequence length, respectively. χ_0^2 indicates the 5% value of χ^2-distribution with ν degrees of freedom. χ_ν^2 indicates the measure of difference between $\langle r(d;\theta,L)\rangle$ and the observed frequencies $[r(d;\theta,L)]$ for tested sequences (Eq. 10). $\xi_\nu<1$ means that the tested sequence generates Bernoulli trials.

b \ c	0.2	0.3	0.4	0.45	0.5	0.55	0.6	0.7	0.8
3.62			317	152	194	332	190	1,043	286
3.7		153	551	578	802	1,122	1,847	6,088	1,663
3.8		269	257	336	552	977	1,623	3,926	1,739
3.9	174	380	250	645	922	1,324	1,754	2,816	2,020
3.99	368	409	316	193	167	157	333	1,108	897
3.999	18.2	8.29	28.5	21.8	4.61	1.28	3.54	27.8	121
4.0	402	468	164	46.4	0.71	55.7	208	839	721

表 3 組合せテストにおけるロジスティック写像の b, c と ξ_r の関係
Table 3 Ratio ξ_r of the combination test for chaotic sequences generated by the logistic map with parameter b when the threshold c is varied. The expected frequencies $\langle m(d;\theta,L,k)\rangle$ of the combination test for Bernoulli trials with the ratio θ is given by Eq. 13. The observed frequencies of the test for the tested sequences is denoted by $[m(d;\theta,L,k)]$. k denotes the number of groups of L/k elements.

b \ c	0.2	0.3	0.4	0.45	0.5	0.55	0.6	0.7	0.8
3.62			2,063	2,039	3,149	4,282	6,594	9,872	5,069
3.7		136	124	39.5	38.5	88.2	69.8	129	68.2
3.8	58.0	133	125	103	82.1	75.9	90.7	102	123
3.9	9.13	112	93.2	52.0	17.0	15.2	23.3	116	217
3.99	7.22	17.1	51.0	38.4	17.7	3.21	4.33	36.0	147
3.999	369	447	198	68.6	28.9	87.8	261	946	821
4.0	56.1	2.41	9.19	6.36	0.59	4.48	3.25	14.6	98.1

表 4 連テスト及び組合せテストにおける $\tau_{4.0}^s$ の iteration s と ξ_r の関係 ($b=4.0$)
Table 4 Ratio ξ_r of the run test and the combination test for chaotic sequences generated by the s-th iterated logistic map $\tau_{4.0}^s$ with $b=4.0$ when s and c are varied.

	Run test					Combination test				
s \ c	0.3	0.4	0.5	0.6	0.7	0.3	0.4	0.5	0.6	0.7
1	468	178	0.71	208	839	2.41	9.19	0.59	3.25	14.6
2	175	149	0.56	77.5	198	24.4	9.89	0.30	6.15	21.1
4	1.69	0.76	0.43	0.32	1.74	0.51	0.42	1.15	0.65	0.50
8	1.00	1.28	0.72	1.48	0.81	0.18	0.29	0.39	0.58	0.35
16	0.33	0.65	0.49	0.25	0.54	0.74	0.69	0.70	0.58	0.57
32	0.48	0.59	0.61	0.89	0.78	0.53	0.35	0.44	0.31	0.34

酔歩テストによる検定においては，b に対して閾値 c を適切に選んでやるか[8]，もしくは，τ_b の写像の多重化を行えば[7),11]，ロジスティック写像は性質の良い実数値型のベルヌイ試行発生器であるという結果が得られている．

本稿では，連テストと組合せテストを行うために2章の式を利用して，$\{\tau_b^n(x)\}_{n=0}^{\infty}$ から得られる2値系列 $\{\sigma_c(\tau_b^n(x))\}_{n=0}^{\infty}$ とベルヌイ試行との近さを議論する．**表1** は種々な b と c に対する2値系列における“0”と“1”の生起確率の比 θ (式(4)) である．式(14)に従って2,000回ごとに初期値を更新して発生させた10万個の乱数について連テスト及び組合せテストを行った結果を**表2, 3** に掲げる．表より，両検定においては，$b=4.0$, $c=0.5$ の場合の系列だけがベルヌイ試行に近く，それ以外の b, c の場合は，ベルヌイ試行と大きく隔った2値系列しか得られていないことがわかり興味深い．この結果は，酔歩テストに合格した2値系列[8]でも連テスト及び組合せテストには不合格であることを意味している．

次に，τ_b の s 重写像* τ_b^s から得られる2値系列 $\{\sigma_c(\tau_b^n(x))\}_{n=0}^{\infty}$ について連テスト及び組合せテストを行った結果を**表 4～6** に掲げる．表では，$b\neq 4.0$ の場合も s の増加と共に閾値 c とは無関係に $\xi_r<1$，すなわち，ベルヌイ試行に近い2値系列が得られる傾向を示している．以上のことからロジスティック写像 τ_b のカオスを利用して性質の良い実数値型ベルヌイ試行発生器を得るためには，$b=4.0$, $c=0.50$ と選ぶか，もしくは，写像の十分な多重化が必要であることがわかる．前者の場合には，等確率のベルヌイ試行しか実現できないことに注意されたい．

3.2 擬似乱数の検定結果

本節では，ロジスティック写像から得られるカオスが，従来の擬似乱数と比較して乱雑さに関して十分に性質の良い乱数であるか否かを検討していくことにする．

ここで取り挙げた従来の擬似乱数は線形合同法，M

* ここで写像の s 多重化とは，数列を s 個ずつとばしてサンプルすることを意味する．

表 5 連テストにおける τ_b^s の iteration s と ξ_r の関係 ($b \neq 4.0$)
Table 5 Ratio ξ_r of the run test for chaotic sequences generated by the s-th iterated logistic map τ_b^s with $b \neq 4.0$ when s and c are varied.

	$b=3.75$				$b=3.80$				$b=3.90$			
s \ c	0.4	0.5	0.694	0.8	0.4	0.5	0.690	0.8	0.4	0.5	0.606	0.8
1	1,030	918	4,577	2,016	257	552	36,350	1,739	250	922	1,813	2,020
2	337	236	292	832	201	137	1,476	473	188	161	606	386
4	43.6	34.1	83.0	174	6.72	9.82	29.6	93.4	23.5	122	576	448
8	21.7	29.2	51.9	36.8	12.4	3.95	19.7	3.68	13.9	45.9	90.7	65.4
16	0.52	1.04	4.31	2.97	1.87	1.90	8.04	4.36	0.96	1.45	1.20	2.36
32	1.17	0.93	1.92	1.51	0.68	0.43	0.47	0.29	0.49	0.93	1.01	0.49

表 6 組合せテストにおける τ_b^s の iteration s と ξ_r の関係 ($b \neq 4.0$)
Table 6 Ratio ξ_r of the combination test for chaotic sequences generated by the s-th iterated logistic map τ_b^s with $b \neq 4.0$ when s and c are varied.

	$b=3.75$				$b=3.80$				$b=3.90$			
s \ c	0.4	0.5	0.694	0.8	0.4	0.5	0.690	0.8	0.4	0.5	0.606	0.8
1	206	73.9	78.8	138	125	77.0	74.5	115	93.2	17.0	25.8	217
2	13.1	1.58	133	27.1	22.1	2.39	18.7	1.21	4.59	1.79	1.03	5.14
4	3.14	10.3	2.14	16.6	2.79	0.81	5.31	1.04	11.1	1.99	17.4	16.4
8	7.06	6.71	4.66	6.85	1.41	0.55	4.49	0.83	1.98	3.98	6.37	8.86
16	0.68	0.52	0.40	1.34	0.83	0.86	0.82	0.81	0.63	0.29	0.42	0.31
32	0.38	0.43	0.46	0.86	0.41	0.68	0.44	0.34	0.33	0.22	0.26	1.15

系列，平方採中法で，各々の発生式は次式で与えられる[1),2),5)]．

線形合同法：$X_{n+1}=65539 \cdot X_n \bmod 2^{31}$ (15)

M 系 列：$X_n=X_{n-t} \oplus X_{n-u}$ (16)

平方採中法：$X_{n+1}=\lfloor (X_n^2 \bmod 10^{15})/10^5 \rfloor$ (17)

ただし，式(16)の記号⊕は，X_n を2進展開して各各の bit に排他的論理和を施すことを意味し，t, u $(t>u)$ は，GF(2)上の原始多項式

$$F(x)=x^t+x^u+1 \quad (18)$$

を定義する整数である．また，式(17)の記号 $\lfloor \cdot \rfloor$ は小数部分の切り捨てを示す Gauss 記号である．さらに，式(15)～(17)で生成される $[0, M]$ 間の整数値系列 $\{X_n\}$ から $[0,1]$ の実数値系列 $\{x_n\}$ への変換は

$$x_n=X_n/M \quad (19)$$

によるとする．上記の擬似乱数に関する連テスト及び組合せテストは既に行われているが[2)~4)]，“0”，“1”の生起確率が等しくなるような特定の c の値に関して得られた2値系列 $\{\sigma_c(X_n)\}_{n=0}^{\infty}$ とベルヌイ試行との近さしか議論していない．本稿では，式(9)及び式(13)を利用して，“0”，“1”の生起確率が等しくない場合における検定を行った．その結果を**表 7～9** に掲げる．これらの表より，線形合同法，M 系列，平方採中法は，いずれも，適切な初期値を選択すれば，ロジスティック写像で得られた結果と異なり，写像の多重化を行わなくても閾値 c とは無関係に性質の良い実数値型のベルヌイ試行発生器であることがわかる．平方採中法は一般に知られているように，やがては短い周期に陥るかあるいは0に退化してしまうという欠点がある（付録1参照）[1),2)]．しかし，本検定及び酔歩テスト[11)]の結果から適切な初期値を選択すれば，周期に落

表 7 線形合同法の連テスト及び組合せテストの結果 (ξ_r の値)
Table 7 Ratio ξ_r of the run test and the combination test for sequences generated by the linear congruential method (Eq. 15) when c is varied.

		Run test				Combination test			
c	θ	ν	χ_ν^2	χ_0^2	ξ_r	ν	χ_ν^2	χ_0^2	ξ_r
0.2	0.25	26	26.8	38.9	0.69	11	10.6	19.7	0.54
0.3	0.43	19	13.6	30.1	0.45	12	14.1	21.0	0.67
0.4	0.67	14	10.3	23.7	0.44	13	21.7	22.4	0.97
0.5	1.02	12	13.5	21.0	0.64	13	16.5	22.4	0.74
0.6	1.49	14	22.7	23.7	0.96	13	19.1	22.4	0.85
0.7	2.32	19	27.2	30.1	0.90	12	17.0	21.0	0.81
0.8	4.00	26	29.4	38.9	0.76	9	8.4	21.0	0.50

表 8 M系列の連テスト及び組合せテストの結果 (ξ_r の値)

Table 8 Ratio ξ_r of the run test and the combination test for m-sequences (Eq. 16) when c is varied.
(i) $t=607$ and $u=147$, (ii) $t=521$ and $u=48$, (iii) $t=127$ and $u=15$

	Run test			Combination test		
c	(i)	(ii)	(iii)	(i)	(ii)	(iii)
0.13	0.58	0.71	0.61	0.64	0.62	0.40
0.25	0.43	0.66	1.00	0.28	0.51	0.64
0.38	0.74	0.50	0.50	0.53	0.84	0.34
0.5	0.37	0.49	0.50	0.42	1.14	0.24
0.63	0.55	0.75	0.82	0.29	1.06	0.23
0.75	0.53	0.53	0.69	0.40	0.71	0.83

表 9 平方採中法の連テスト及び組合せテスト結果 (ξ_r の値)

Table 9 Ratio ξ_r of the run test and the combination test for sequences generated by the middle-square method (Eq. 17) when c is varied.

		Run test				Combination test			
c	θ	ν	χ^2_ν	χ^2_0	ξ_r	ν	χ^2_ν	χ^2_0	ξ_r
0.2	0.25	26	35.9	38.9	0.92	11	8.8	19.7	0.45
0.3	0.43	18	17.7	28.9	0.61	12	8.2	21.0	0.39
0.4	0.67	14	23.2	23.7	0.98	13	17.4	22.4	0.78
0.5	1.02	12	21.0	21.0	1.00	13	19.1	22.4	0.85
0.6	1.52	14	19.4	23.7	0.82	13	11.9	22.4	0.53
0.7	2.37	19	23.4	30.1	0.78	12	11.0	21.0	0.52
0.8	4.12	27	21.7	40.1	0.54	10	5.6	18.3	0.31

ち込むまでに十分性質の良い乱数が得られることがわかる．また，線形合同法，M系列に関しても短い周期に陥ったり，片寄った値が続くことのないように適切な初期値を選択した．不規則解の乱雑さを示す一つの指標として Kolmogolov-Sinai エントロピー (K. S. エントロピーと略称する)

$$H(\tau)=\int_I \ln|\mathrm{d}\tau(x)/\mathrm{d}x|f(x)\mathrm{d}x \qquad (20)$$

が知られている (ただし，$f(x)\mathrm{d}x$ は解の x 近傍での出現頻度を表す τ の不変測度とする)[10),13)]．$b=4.0$ のロジスティック写像の多重写像 $\tau^{16}_{4.0}$ 及び線形合同法 $\tau'_a(x)=ax(\mathrm{mod}\ M)$ の K. S. エントロピーは簡単な計算により，各々[10),11)]

$$H(\tau^{16}_{4.0})=s\cdot\ln 2 \qquad (21)$$

$$H(\tau'_a)=\ln a \qquad (22)$$

と導かれる(付録2参照)．本稿では，式(15)のように線形合同法における乗数を $a=65539$ としているので

$$s=\ln 65539/\ln 2\fallingdotseq 16 \qquad (23)$$

となり，$\tau_{4.0}$ を16回多重化を行えばその K. S. エントロピーは，線形合同法のそれとはほぼ同じ値となり，同程度に乱雑であると思われる．これを乱数の発生効率の立場から考えてみる．計算機* 上で両方法を用いて10万個の乱数を発生する際，必要とされる CPU-time は各々，$\tau^{16}_{4.0}$: 500 msec, τ'_{65539}: 265 msec であり，発生効率の点からも，線形合同法の方が優れていると思われる．次に $b\fallingdotseq 4.0$ の場合は，不変密度の存在すら確認されておらず，その K. S. エントロピーの値は不明であるが，連テスト及び組合せテストに合格するためには，写像の多重化を32回以上行わなければならない．すなわち，$b\fallingdotseq 4.0$ の場合は，一層発生効率が悪いと思われる．

区間 $[-1,1]$ 上で定義される m 次の Tchebychev 写像

$$T_m(x)=\cos(m\cdot\cos^{-1}x),\quad x\in[-1,1] \qquad (24)$$

のカオス (2次の Tchebychev 写像は，$b=4.0$ のロジスティック写像と共型変換[13)]の関係にある) は，"pure chaos"[13)] ではあるが，**表 10, 11** で示されるように次数 m を上げれば，写像の多重化を行うことなく性質の良いベルヌイ試行発生器であることを注意しておく．ただし，Tchebychev 写像の不変測度は

表 10 2^s 次 Tchebychev 写像の連テスト結果 (ξ_r の値)

Table 10 Ratio ξ_r of the run test for chaotic sequences generated by the Tchebychev map $T_m(x)$ (Eq. 24) with degree $m=2^s$ when s and c are varied.

s \ c	−0.5	−0.2	−0.1	−0.05	0.0	0.05	0.1	0.2	0.5
1	1,365	190	47.9	10.6	0.38	13.3	47.7	178	686
2	242	79.1	41.8	12.6	0.65	14.2	52.1	143	56.4
4	180	0.26	28.8	9.3	0.48	6.9	21.8	0.33	4.0
8	0.85	1.0	0.50	0.33	0.38	0.66	0.71	1.1	0.77
16	0.66	0.59	0.71	0.61	0.97	0.86	1.0	0.86	0.36
32	0.60	0.44	0.78	0.70	0.54	0.52	0.57	0.77	0.64

* 九州大学大型計算機センター FACOM M-382 を使用．

表 11 2^s 次 Tchebychev 写像の組合せテスト結果 (ξ_r の値)
Table 11 Ratio ξ_r of the combination test for chaotic sequences generated by the Tchebychev map $T_m(x)$ with the degree $m=2^s$ when s and c are varied.

s \ c	−0.5	−0.2	−0.1	−0.05	0.0	0.05	0.1	0.2	0.5
1	76.7	4.2	4.4	2.8	0.48	4.1	7.1	8.6	15.1
2	54.0	5.8	5.9	2.5	0.81	2.5	7.6	11.1	13.4
4	2.3	0.56	2.7	1.1	0.50	0.80	1.5	0.63	0.61
8	0.50	0.56	0.70	0.50	0.53	0.34	0.48	0.34	0.71
16	0.53	0.58	0.49	0.94	0.73	0.92	0.54	0.70	0.29
32	0.61	0.79	0.63	0.72	0.52	0.47	0.37	0.31	0.33

$$f(x)\mathrm{d}x=\mathrm{d}x/(\pi\cdot\sqrt{1-x^2}) \qquad (25)$$

であり，さらに，発生効率の点でも劣る（10万個の乱数を発生するのに必要な CPU-time は 700 msec である）．以上の結果をまとめると，従来の擬似乱数は，適切な初期値を選択すれば，性質の良い実数値型のベルヌイ試行発生器であるのに対し，ロジスティック写像は写像の多重化を行わなければ，性質の良い実数値型のベルヌイ試行発生器とはならない．また，ロジスティック写像から線形合同法と同程度の乱雑さを持つ実数値系列を得るためには，写像の多重化が必要であるが，これは乱数発生効率の面からみて望ましいとはいえない．

4. むすび

本稿では，性質の良い乱数に関する一つの考え方を提案した．すなわち，与えられた実数値系列を2値系列に変換して，得られた2値系列が閾値 c とは無関係に常にベルヌイ試行に近いとき，もとの実数値系列を性質の良い乱数とみなそうとするものである．

上記の考え方を基礎にして，ロジスティック写像で生成されるカオスと従来の擬似乱数発生器としての線形合同法，M系列，平方採中法で生成される数列との乱雑さに関する考察を行った．前稿では酔歩テストを用いてこれらの数列の乱雑さを測定し，カオスは従来の擬似乱数と比べて性質の良い乱数とは言えないとの結論を得た．本稿では，任意の閾値 c に対する連テスト及び組合せテストを行うことにより，前稿と同様の結果を得た．すなわち，従来の擬似乱数は適切な初期値を選択すれば，性質の良い実数値型のベルヌイ試行発生器であるのに対し，ロジスティック写像は，写像の多重化を行わなければ，性質の良い実数値型のベルヌイ試行発生器ではないことが示された．また，高い次数の Tchebychev 写像のカオスは，発生効率の点で従来の擬似乱数に劣るが，性質の良い乱数であることも確認した．

参考文献

1) Knuth（渋谷訳）：準数値算法/乱数，サイエンス社，東京（1980）．
2) 津田：モンテカルロ法とシミュレーション，培風館，東京（1977）．
3) 津田：レーマ型合同法によらない乱数について，*bit*, Vol. 12, No. 9, pp. 1180-1191 (1980).
4) 宮武，脇本：乱数とモンテカルロ法，森北出版，東京（1978）．
5) 伏見：擬似乱数の発生法について，情報処理，Vol. 21, No. 9, pp. 968-974 (1980).
6) Kozak, J. J., Musho, M. K. and Hatlee, M. D.: Chaos, Periodic Chaos, and the Random-Walk Problem, *Phys. Rev. Lett.*, Vol. 49, No. 25, pp. 1801-1804 (1982).
7) Arneodo, A. and Sornette, D.: Monte Carlo Random-Walk Experiments as a Test of Chaotic Orbits of Maps of the Interval, *Phys. Rev. Lett.*, Vol. 52, No. 21, pp. 1857-1860 (1984).
8) 香田，緒方：ベルヌイ試行とカオス，電子通信学会論文誌 A, Vol. J 68-A, No. 2, pp. 146-152 (1985).
9) 大石：カオスと乱数発生，*bit*, Vol. 14, No. 5, pp. 704-713 (1982).
10) Oono, Y., Kohda, T. and Yamazaki, H.: Disorder Parameter for Chaos, *J. Phys. Soc. Jpn.*, Vol. 48, No. 3, pp. 738-745 (1980).
11) 香田，柿本：擬似乱数の歩行長，電子通信学会論文誌 A, Vol. J 68-A, No. 10, pp. 1016-1023 (1985).
12) Li, T. and Yorke, J.: Ergodic Maps on [0, 1] and Nonlinear Pseudo-Random Number Generators, *Nonlinear Analysis, Theory, Methods & Applications*, Vol. 2, No. 4, pp. 473-481 (1978).
13) Grossman, S. and Thomae, S.: Invariant Distributions of One-Dimensional Discrete Process, *Z. Naturforsch.*, Vol. 32a, pp. 1353-1363 (1977).

付録1 平方採中法の欠点

式(17)は，10桁の整数 X_n を2乗してできた20桁

の整数の中央の10桁を X_{n+1} とする手続きを表している．以下にこの発生法により生成される $\{X_n\}$ が陥りやすい欠点を二つの場合に分けて述べる．

A_n, B_n を各々5桁の整数として，

$$X_n=A_n\cdot 10^5+B_n \qquad (A.1)$$

であるとする．

（I） $A_n=0$（上位5桁がすべて0）のとき

式(17)より

$$X_{n+1}=\lfloor(X_n^2 \bmod 10^{15})/10^5\rfloor$$
$$=\{B_n^2-(B_n^2 \bmod 10^5)\}/10^5 \qquad (A.2)$$

であるが，$B_n<10^5$ に注意すると

$$\{B_n^2-(B_n^2 \bmod 10^5)\}<B_n^2<B_n\cdot 10^5$$

となり

$$\{B_n^2-(B_n^2 \bmod 10^5)\}/10^5<B_n$$

が成立する．したがって $X_{n+1}<X_n$ から，$\lim_{n\to\infty} X_n=0$ を得る．すなわち，一度上位5桁がすべて0になると，X_n はいずれ0に退化する*．

（II） $B_n=0$（下位5桁がすべて0）のとき

式(17)より

$$X_{n+1}=(A_n^2 \bmod 10^5)\cdot 10^5 \qquad (A.3)$$

となり，これ以後生成される系列は，下位5桁がすべて0となる．すなわち，一度下位5桁がすべて0になると，それ以後できる系列も下位5桁がすべて0となってしまう．また，このとき，$X_n=X_{n+m}$ となる周期 m は 10^5 以下となる．

付録2 線形合同法の K. S. エントロピー

線形合同法

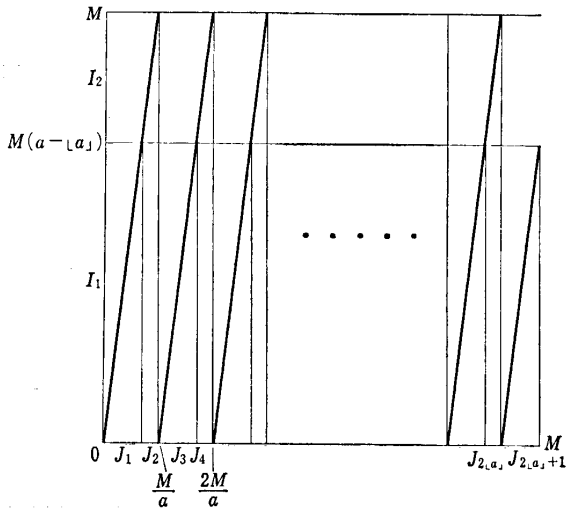
$$X_{n+1}=\tau_a'(X_n)$$
$$\tau_a'(X_n)=aX_n \pmod M \qquad (A.5)$$

において，τ_a' を図**A** のように分割する．区間 I_i, J_j における不変測度を各々 $\mu(I_i), \mu(J_j)$ とすれば

$$\mu(I_1)=a-\lfloor a\rfloor$$
$$\mu(I_2)=1-a+\lfloor a\rfloor$$
$$\mu(J_{2j-1})=(a-\lfloor a\rfloor)/a \quad (i=1,2,\cdots,\lfloor a\rfloor+1)$$
$$\mu(J_{2i})=(1-a+\lfloor a\rfloor)/a \quad (i=1,2,\cdots,\lfloor a\rfloor) \qquad (A.6)$$

となっている．K. S. エントロピーの原義に従えば，

$$H(\tau_a')=-\sum_{j=1}^{2\lfloor a\rfloor+1}\mu(J_j)\ln\mu(J_j)$$



図A 線形合同法による写像の分割

Fig. A Partition of the map $\tau_a'(x)$ (Eq. A. 5) described by the linear congruential method (Eq. 15).

$$+\sum_{i=1}^{2}\mu(I_i)\ln\mu(I_i) \qquad (A.7)$$

であるので[10]

$$H(\tau_a')=\begin{cases}\dfrac{(a-\lfloor a\rfloor)(1-a+\lfloor a\rfloor)}{a}\ln\dfrac{1-a+\lfloor a\rfloor}{a-\lfloor a\rfloor}\\ \quad +\ln a \quad (a\text{が実数のとき})\\ \ln a \quad (a\text{が自然数のとき})\end{cases} \qquad (A.8)$$

を得る．

（昭和60年5月8日受付）
（昭和60年10月17日採録）

香田 徹（正会員）

昭和21年生．昭44年九州大学工学部通信卒業．昭49年同大学院博士課程修了．同年九大・情報工学科助手，昭56年同助教授．工学博士．生体情報，聴覚系の情報処理機構および非線型システムの研究に従事．電子通信学会，日本音響学会，日本物理学会各会員．

柿本 厚志

昭和35年生．昭58年九州大学工学部情報卒業．昭60年同大学院修士課程修了．同年キャノン入社．在学中，凝似乱数やカオスの乱雑さに関する研究に従事．電子通信学会会員．

* この欠点を補うために Li & Yorke[12] により，改良平方採中法

$$X_{n+1}=\lfloor\{(X_n+10^{10})^2 \bmod 10^{15}\}/10^5\rfloor \qquad (A.4)$$

が提案されている．ただし，この発生法でも(II)の同期性に関する欠点は改良されない．