6W-3

カオス写像を用いた擬似乱数生成器の乱数性*

秋山　真一†　　川村　暁‡　　三浦　守§
公立はこだて未来大学大学院　　石巻専修大学　　公立はこだて未来大学

概要

新たな擬似乱数生成法として，カオスを用いる方法を提案する．本稿では，様々なカオス写像から取り出した出力値の微小部分を乱数とし，その乱数性を統計的検定を用いて調べた．実験結果から，既に筆者らが提案したカオス・ニューラルネットワークを用いた場合，他のカオス写像の場合と比べ，最も物理乱数の性能に近いことが明らかとなった．

1　まえがき

暗号系における鍵の生成や配送およびモンテカルロシミュレーションでは，乱数性および生成速度に優れた乱数生成器を用いることが重要である．広く知られている線形合同法や，フィードバック付シフトレジスタを用いて生成した乱数は，周期を持ち，系列が予測可能であることが明らかになっている[1]．これらを解決する新たな乱数生成法として，カオスを用いる方法を提案する．

本稿では，カオス写像から取り出した出力値の微小部分を乱数とし，その乱数性を統計的検定を用いて調べた．カオス写像には，筆者らが提案しているカオス・ニューラルネットワーク[2]，ロジスティック写像，エノン写像，池田写像およびテント写像を用いた．また乱数性の比較のため，物理乱数生成器と既存の擬似乱数生成器を用いて同様の検定を行った．実験結果から，カオス・ニューラルネットワークを用いた場合，最も物理乱数の性能に近いことが明らかとなった．

2　カオスを用いた乱数生成

系に内在する非線形性により，確率的現象と等価な振る舞いを示すカオスを，乱数の生成に利用する研究が行われている．カオスの系が有する初期値に対する鋭敏な依存性，アトラクタの稠密性により，予測不可能で無周期である乱数の生成が可能であると考えられる．さらにアトラクタの周辺の点を初期値とした場合，軌道がアトラクタ上に吸い込まれていく性質から，カオス写像の初期値を乱数の種とすることができると考えられる．

筆者らは，形式ニューロンモデルをベースとし，ネットワーク構造によりカオス応答する人工ニューラルネットワーク (カオス・ニューラルネットワーク;CNN[2]) を提案し，その応用として，擬似乱数生成器 CNN PRNG[3] を構成した．CNN のニューロンモデルを式 (1)，(2) に，ネットワーク構造を図 1 に示す．ただし，$y_j(t)$ は時刻 t でのニューロン j の出力，$x_i(t)$ は時刻 t でのニューロン i からの入力，u_j はニューロン j の内部状態，w_{ij} はニューロン i からニューロン j への結合荷重，θ_j はニューロン j の閾値，I_j はニューロン j の外部入力値である．また出力関数 f には，シグモイド関数を用い，その傾き係数 $\lambda = 1$ である．

$$y_j(t) = f(u_j) = \frac{1}{1 + exp(u_j/\lambda)} \tag{1}$$

$$u_j = \sum_{i=1}^{n} w_{ij} x_i(t-1) + \theta_j + I_j \tag{2}$$

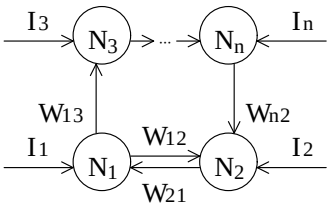

図 1　CNN のネットワーク構造 (ニューロン数 n)

CNN PRNG では，高速に乱数を生成するため，カオス系特有の信号値の偏りを除いた値，すなわちニューロンの出力値の微小部分を乱数とする乱数生成法を用いている．具体的には，ニューロンの出力値を IEEE754 標準の倍精度実数で表現し，その仮数部下位 bit 側から数 bit を乱数とする．CNN PRNG の乱数生成法を図 2 に示す．

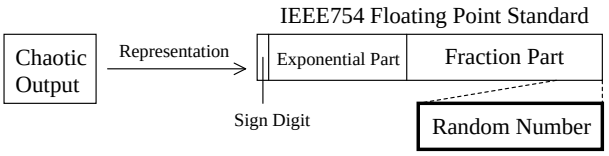

図 2　CNN PRNG の乱数生成法

3　計算機実験

様々なカオス写像に対して図 2 の方法を用いて乱数を生成し，その乱数性を統計的検定を用いて調べた．本実験では，図 2 において，仮数部下位 bit 側から 8bit を乱数とした．乱数生成には，筆者らが提案する CNN(ニューロン数 3)，ロジスティック写像，エノン写像，池田写像およびテント写像を用いた．カオス写像に 10,000 通りの初期値を与え生成した乱数に対して

---

* The Randomness of Pseudo Random Number Generators Using Chaos Map

† Graduate School of System Information Science, Future University - Hakodate

‡ School of Science and Engineering, Ishinomaki Senshu University

§ School of System Information Science, Future University - Hakodate

表 1　実験に用いた乱数生成器

乱数生成器名	概要
CNN PRNG	CNN を用いた乱数生成器
LOG PRNG	ロジスティック写像を用いた乱数生成器
HENON PRNG	エノン写像を用いた乱数生成器
IKEDA PRNG	池田写像を用いた乱数生成器
TENT PRNG	テント写像を用いた乱数生成器
RPG102	物理乱数生成器
MRAND48	C の mrand48 関数

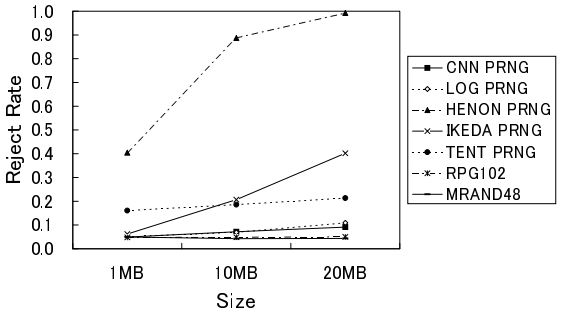

図 3　頻度検定結果 (1bit 単位)

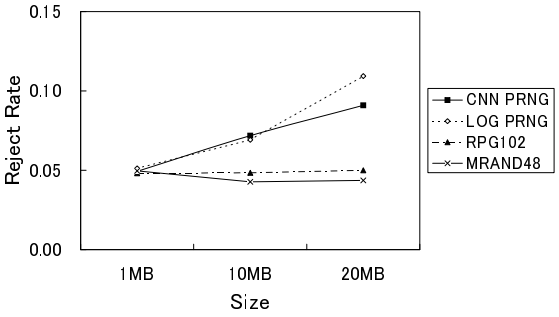

図 4　頻度検定結果 (1bit 単位):一部

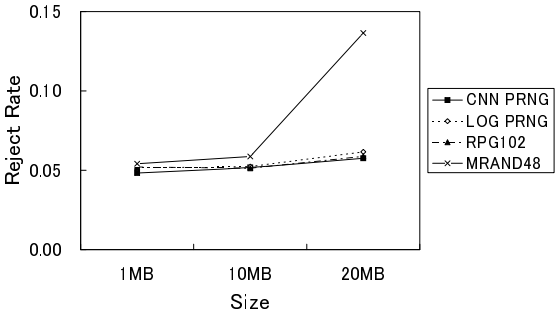

図 5　頻度検定結果 (8bit 単位):一部

統計的検定 (両側 5% 検定) を行い，検定で棄却された割合 (棄却率) と，得られた p 値が一様に分布しているか KS 検定 (両側 5% 検定) を用いて調べ，乱数性を評価した．統計的検定には，1,2,4,8,16bit 単位の頻度検定 [4](size:1MB,10MB,20MB) を用いた．乱数性の比較のため，物理乱数生成器 Random Streamer RPG102(発売元:FDK 株式会社)，C の擬似乱数生成関数 mrand48 を用いて同様の検定を行った．物理乱数生成器を用いて生成した乱数の数は，1MB:10,000 個，10MB:3,200 個，20MB:1,600 個である．本実験に用いた乱数生成器を表 1 に示す．

4　検定結果

1bit 単位の頻度検定結果を図 3 に，同検定での棄却率が 0.00〜0.15 の範囲にある乱数生成器の検定結果を図 4 に示す．検定結果より，エノン写像，池田写像およびテント写像を用いた場合，比較的棄却率が高いことがわかった．また RPG102 の棄却率に最も近い乱数生成器は，MRAND48 であり，カオスを用いた乱数生成器の中では，CNN PRNG が最も近いことが明らかになった．8bit 単位の頻度検定での棄却率が 0.00〜0.15 の範囲にある乱数生成器の検定結果を図 5 に示す．検定結果より，MRAND48 は，乱数のサイズが 20MB のとき，比較的棄却率が高いことがわかった．以上の結果より，物理乱数と区別がつかない乱数を最も多く生成した乱数生成器は，CNN PRNG であった．

1bit の頻度検定で得られた p 値に対する KS 検定結果を表 2 に示す．検定結果より，乱数のサイズが 1MB のとき，CNN PRNG，LOG PRNG は，物理乱数生成器と区別がつかない乱数生成器であるといえる．また乱数のサイズが 10MB および 20MB のとき，すべての擬似乱数生成器が物理乱数生成器と区別がついた．

表 2　p 値に対する KS 検定結果

乱数生成器名	1MB	10MB	20MB
CNN PRNG	採択	棄却	棄却
LOG PRNG	採択	棄却	棄却
HENON PRNG	棄却	棄却	棄却
IKEDA PRNG	棄却	棄却	棄却
TENT PRNG	棄却	棄却	棄却
RPG102	採択	採択	採択
MRAND48	棄却	棄却	棄却

5　むすび

本稿では，様々なカオス写像から取り出した出力値の微小部分を乱数とし，その乱数性を統計的検定を用いて調べた．実験結果から，筆者らが提案した CNN を用いた場合，最も物理乱数の性能に近いことが明らかとなった．今後の展望として，他の統計的検定を行い，詳細な乱数性を調べることが挙げられる．

参考文献

[1] 伏見正則著，乱数，東京大学出版，1989.
[2] Hitoaki YOSHIDA, et al., Chaos Neural Network, Proc.ISPACS'96, Vol.1of3, pp.16.1.1-16.1.5, 1996.
[3] 川村暁ら，カオスに基づく擬似乱数生成器の統計的性質，電子情報通信学会信学技報，NLP2003-2, pp.7-12, 2003.
[4] 宮武修，脇本和昌著，乱数とモンテカルロ法，森北出版，1978.