The 11th Workshop on Finite Field Theory
and its Application for Pseudo-Random
Sequences (FFTPRS2025)
Hirugami-Online(Hybrid), September 16-17, 2025

補数表現を用いたバランスの良い擬似乱数系列に対するビットの拡散に関する一考察

A Study on Bit Diffusion of Balanced Sequences Using Complement Representations for Two Random Generators

桑原大雅 * 林夏生 * 宮崎武 † 荒木俊輔 ‡
Teiga Kuwahara Natsuo Hayashi Takeru Miyazaki Shunsuke Araki

上原聡 *
Satoshi Uehara

Abstract— This paper presents a comparative evaluation of pseudorandom number generation methods based on the Linear Congruential Method and the integer Logistic Map, as well as methods that combine these with shuffling operations using complement representation. In addition to the conventional NIST SP800-22 tests, this study introduces new quantitative evaluation metrics beyond NIST by analyzing bit-level shuffling and measuring the occurrence probability and variance of ones within blocks. The results show that the use of shuffling operations significantly improves randomness, producing sequences with low bias. Furthermore, block-level analysis indicates the potential to quantitatively assess short-term randomness and the unpredictability of input values. This study demonstrates the effectiveness of complement-based shuffling and the practical utility of new evaluation metrics beyond standard NIST tests.

Keywords— Pseudorandom number generators, Linear Congruential Method, Logistic Map, NIST SP800-22.

1 はじめに

近年，情報セキュリティや数値計算において，高品質な擬似乱数生成の重要性が増している．従来の線形合同法（LCM）や整数上のロジスティック写像（LM）は簡便に擬似乱数を生成できるが，有限精度の影響や構造的制約により，系列に偏りや規則性が生じる場合がある．本稿では，LCM および LM に補数表現を用いた攪拌操作を組み合わせた SLCM および SLM を対象とし，これらの擬似乱数生成法の統計的特性を比較・評価する．評価は従来の NIST SP800-22 検定に加え，ビット単位での攪拌性の分析やブロックごとの 1 の出現確率および分散の測定を行い，これにより新たな定量的評価指標を導入することを目指した．本稿は，補数表現を用いた攪拌処理の有効性と，主に短期の乱数性を評価する新しい指標の可能性を示すことを目的とする．

* 〒 802-8577 北九州市立大学, 福岡県北九州市若松区ひびきの 1-1 The University of kitakyushu, kitakyushu, Fukuoka, Japan.
† 〒 818-0117 九州情報大学, 福岡県太宰府市宰府 6-3-1, Kyushu Institute of Information Sciences, Dazaifu, Fukuoka, Japan.
‡ 〒 820-8502 九州工業大学, 福岡県飯塚市川津 680-4, Kyushu Institute of Technology, Iizuka, Fukuoka, Japan.

2 準備

ここでは、本稿で比較する擬似乱数生成法である，線形合同法と整数上のロジスティック写像について紹介する．

2.1 線形合同法

状態 $\mathrm{LC}(X_i)$ は次の漸化式で定義される：

$$\mathrm{LC}(X_i) \equiv (a\,X_i + c) \pmod{m}, \tag{1}$$

ここで，m は正の整数であるモジュラスで，乱数の周期を決定する．a は乗数，c は増分，LC_0 は初期値である．

本稿では，以下のパラメータを用いる：

- $m = 4611686014132420609 = (2^{31}-1)^2$
- $a = 48271$
- $c = 0$
- X_0 は任意

この設定により，線形合同法に基づく擬似乱数系列 LC_i を生成した．さらに，一度の写像ごとに下位 24 ビットを抽出して系列として使用している．なお，本稿では，線形合同法を単独で用いた手法を LCM（Linear Congruential Method）と呼ぶこととする．ただし，線形合同法の性質上，たとえパラメータが最適に選ばれても，統計的乱数性に偏りや問題が生じる可能性がある．

2.2 補数表現を用いた線形合同法による擬似乱数生成

本稿では，第一著者の所属する研究室内で検討している手法として，従来の線形合同法に補数表現を用いた線形合同法を組み合わせることで，乱数性の改善を試みる．補数表現を用いた線形合同法は次の漸化式で定義される：

$$\overline{\mathrm{LC}}(X_i) \equiv m - (a\,X_i + c) \pmod{m}, \tag{2}$$

また，$\mathrm{LC}(\cdot)$ と，$\overline{\mathrm{LC}}(\cdot)$ を組み合わせる手順は以下の通りである．

1. 初期化として，2 つの初期値 X'_0 および Y'_0 を設定する．

2. X'_i と Y'_i をそれぞれ $\mathrm{LC}(\cdot)$ および $\overline{\mathrm{LC}}(\cdot)$ により写像する．

$$X_i = \mathrm{LC}(X'_{i-1}) \pmod{(2^{31}-1)^2}, \quad (3)$$
$$Y_i = \overline{\mathrm{LC}}(Y'_{i-1}) \pmod{(2^{31}-1)^2}. \quad (4)$$

3. X_i と Y_i を攪拌する．

$$X'_i = (X_i \cdot 2^{14}) + \left\lfloor \frac{Y_i}{2^{14}} \right\rfloor, \quad (5)$$
$$Y'_i = (Y_i \cdot 2^{14}) + \left\lfloor \frac{X_i}{2^{14}} \right\rfloor. \quad (6)$$

4. 下位 24 ビットを出力 s_i として得る．

$$s_i = \left((X'_i \oplus Y'_i) \bmod (2^{31}-1)^2\right) \,\&\, \mathrm{0xFFFFFF}. \quad (7)$$

なお，本稿では，本手法を SLCM（Shuffle Linear Congruential Method）と呼ぶことにする．

2.3 実数上のロジスティック写像

ロジスティック写像は，カオス写像の一つであり，不規則性を持つ長周期的な数列を生成することが可能であることが知られている．実数 $\mathrm{LM}(x_i) \in [0,1]$ に対して，次の漸化式で定義される：

$$\mathrm{LM}(x_i) = \mu\, x_i \left(1 - x_i\right), \qquad 0 < \mu \le 4, \quad (8)$$

ここで，μ は制御パラメータであり，μ の値によって力学的性質（収束，周期倍分岐，カオス）が変化する．本稿では，制御パラメータとして $\mu = 4$ を用いた．

2.4 整数上のロジスティック写像

有限精度の計算を考慮し，計算機に適した形に拡張したものが整数上のロジスティック写像である．整数上のロジスティック写像により生成される系列を，本稿では LM_i と表記する．2^n を法として整数上において次式 $\mathrm{LM}_{\mathrm{int}}^{(n)}(X_i)$ で定義される：

$$\mathrm{LM}_{\mathrm{int}}^{(n)}(X_i) = \left\lfloor \frac{\mu\, X_i \left(2^n - X_i\right)}{2^n} \right\rfloor \pmod{2^n}, \quad (9)$$

本稿では，$n = 32$，$\mu = 4$ を用いた．なお，本稿では，整数上のロジスティック写像を単独で用いた手法を LM（Logistic method）と呼ぶこととする．しかし、整数上のロジスティック写像は 32bit 精度の場合カオス的性質が失われ，系列に偏りや規則性が生じるため，乱数性に問題がある．

2.5 補数表現を用いたロジスティック写像による擬似乱数生成

[1] では，従来のロジスティック写像に補数表現を用いたロジスティック写像を以下の手順で組み合わせることによって，乱数性の改善を試みた．補数表現を用いた $\overline{\mathrm{LM}}_{\mathrm{int}}^{(n)}(X_i)$ は次の漸化式で定義される：

$$\overline{\mathrm{LM}}_{\mathrm{int}}^{(n)}(X_i) = 2^n - \left\lfloor \frac{\mu\, X_i \left(2^n - X_i\right)}{2^n} \right\rfloor. \quad (10)$$

また，$\mathrm{LM}_{\mathrm{int}}^{(n)}(\cdot)$ と，$\overline{\mathrm{LM}}_{\mathrm{int}}^{(n)}(\cdot)$ を組み合わせる手順は以下の通りである．

1. 初期化として，2 つの初期値 X'_0 および Y'_0 を設定する．
2. X'_i と Y'_i をそれぞれ $\mathrm{LM}_{\mathrm{int}}^{(n)}(\cdot)$ および $\overline{\mathrm{LM}}_{\mathrm{int}}^{(n)}(\cdot)$ により写像する．

$$X_i = \mathrm{LM}_{\mathrm{int}}^{(32)}(X'_{i-1}) \pmod{2^{64}}, \quad (11)$$
$$Y_i = \overline{\mathrm{LM}}_{\mathrm{int}}^{(32)}(Y'_{i-1}) \pmod{2^{64}}. \quad (12)$$

3. X_i と Y_i を攪拌する．

$$X'_i = (X_i \cdot 2^{16}) + \left\lfloor \frac{Y_i}{2^{16}} \right\rfloor, \quad (13)$$
$$Y'_i = (Y_i \cdot 2^{16}) + \left\lfloor \frac{X_i}{2^{16}} \right\rfloor. \quad (14)$$

4. 32 ビットの出力 s_i を得る．

$$s_i = X'_i \oplus Y'_i \pmod{2^{32}}. \quad (15)$$

なお，本稿では，本手法を SLM（Shuffle Logistic Method）と呼ぶことにする．

3 評価

3.1 NIST SP800-22 検定による統計的乱数性の評価

4 つの擬似乱数生成法にランダムな初期値を与えたときに生成される系列に対して，NIST SP800-22 検定を用いて統計的乱数性の評価をした．また，各検定の内容には触れず単に検定に通るか通らないかについてを評価した．表 1 に，各擬似乱数生成法の検定に通っていない個数を示す．表より，線形合同法を単独で用いた LCM では不合格数が 8 件であり，一定の乱数性を有することがわかる．一方，LCM に攪拌処理を加えた SLCM では不合格数が 1 件に減少しており，単純な線形合同法に比べて乱数性が大幅に改善されていることが示される．整数上のロジスティック写像（LM）は 158 件の不合格を示しており，有限精度計算の影響により乱数性が十分でないことが確認できる．LM に攪拌を加えた SLM は不合格数 8 件であり，LM 単独よりは改善しているものの，SLCM ほど安定した乱数性を示してはいない．これらの結果から，攪拌処理は乱数性改善に一定の有効性があることがわかる．

表 1: 初期値 1 のときの NIST SP800-22 検定での各擬似乱数に対する不合格検定数

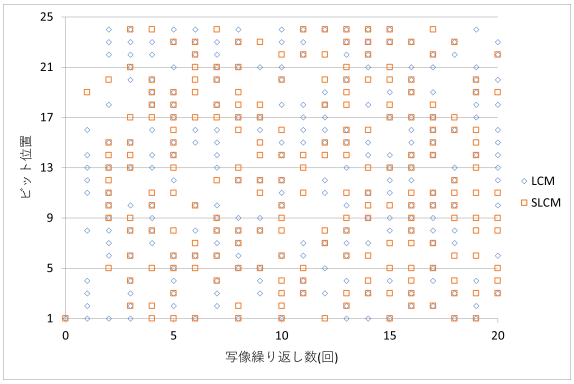
生成手法	不合格検定数
lcm	8
slcm	1
lm	158
slm	8

3.2　写像繰り返し回数に対する 1 の攪拌性

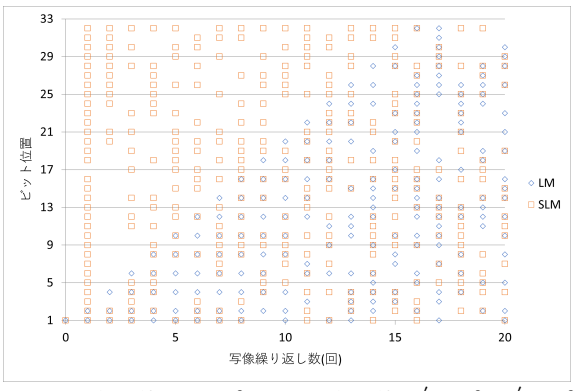
本節では，各擬似乱数生成法に初期値 1 を与え，写像の繰り返し回数に対する 1 の攪拌性を評価した．本評価は,「1 の攪拌が写像回数が少ないうちに迅速に行われるほど，乱数性が高く，入力値の予測困難性も高い」という仮説のもとで行った．横軸を写像の繰り返し回数，縦軸を各ビット位置として 1 の出現状態を散布図として表した（図 1）．縦軸が高いほど上位ビット，低いほど下位ビットを示す．結果より，LM 単独では特に下位ビットにおいて 1 の攪拌が遅く，繰り返し回数が増えても偏りが残ることが確認できた．一方，SLM によって攪拌処理を加えると，下位ビットを含む全ビットに 1 が比較的早く均等に分布することがわかる．また， LCM と SLCM はどちらも一定の攪拌性があることがわかる．以上の結果から，攪拌処理を導入ことにより，LM 単独では遅れがちなビットごとの均一性が大きく改善されることが確認できる．そして、NIST 検定において，不合格検定数が少ない手法ほど，写像回数が少ない段階で全ビットの攪拌が達成されており，入力値の予測困難性も高いことが示唆される．

3.3　1 ブロック内の 1 の出現確率と分散

次節では，初期値 1 を与えた各擬似乱数生成法から一定の長さの系列を生成し，系列を長さ N ビットのブロックに区切ったうえで，各ブロック内の 1 の出現確率および分散を調べた．今回は $N = 10, 100, 1000, 10000$ とし，短いブロック長では確率や分散の値が広く分布し，短期的な乱数性や前後のビットからの予測困難性が反映される．一方，長いブロック長では確率が理論値 0.5，分散が理論値 0.25 付近に収束するため，長期的な乱数性やビットの偏りの少なさが確認できることを理想とした．各生成法に対して，横軸にブロック位置，縦軸に平均および分散をプロットした散布図を作成した (図 2-5)．結果として，NIST 検定で多くの項目で不合格だった LM は 短いブロック長において極端なビットの偏りが確認された．一方，LCM, SLCM, SLM では，短いブロック長でも 1 の出現確率が比較的均一に分布していることが確認された．ただし、ブロック長が長くなると，手法間での目立った違いが見られなかった．LM では乱数性が



(a) LCM の初期値 $X_0 = 2^0$,SLCM の初期値 $X_0' = 2^0$, $Y_0' = 2^0$



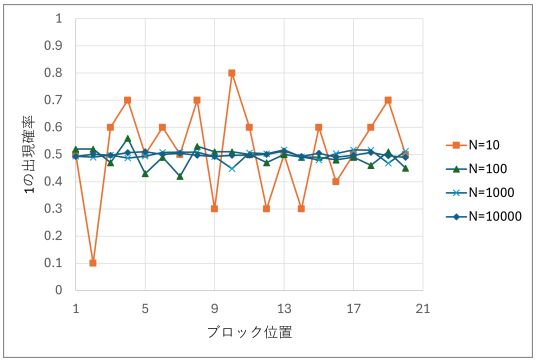
(b) LM の初期値 $X_0 = 2^0$, SLM の初期値 $X_0' = 2^0$, $Y_0' = 2^0$

図 1: 写像繰り返し回数に対する 1 の出現位置

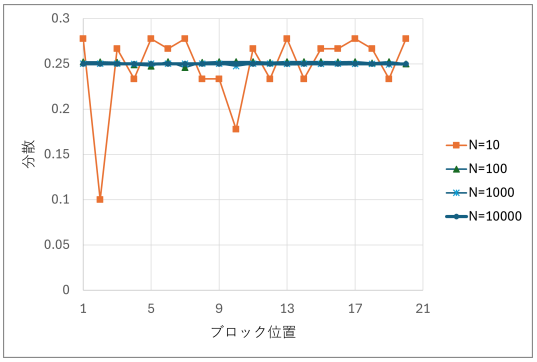
不十分であるのに対し，LCM や SLCM や SLM のような攪拌処理を施した手法は全ビットにわたり均一で安定した乱数性を示すことがわかる．また，この評価方法では，長期の乱数性の評価は難しい可能性がある．

4　まとめ

本稿では，線形合同法と整数上のロジスティック写像，およびそれらに補数表現を用いた攪拌操作を組み合わせた SLCM と SLM の擬似乱数生成法について評価を行った．NIST SP800-22 検定の結果，LM 単独は多数の不合格を示し，有限精度の影響により乱数性が不十分であることが確認された．一方，SLCM や SLM では攪拌操作により短期・長期の乱数性が大幅に改善されることを確認できた．また，写像繰り返しに対する 1 の攪拌性やブロック内の平均・分散解析からも，攪拌処理が偏りの改善に有効であり，入力値の予測困難性を向上させることが示唆された．これらの結果より，補数表現を用いた攪拌操作は，従来手法の乱数性改善に有効であることが確認された．さらに、今回行ったような評価方法は短期的な乱数性の評価指標として用いることができる可能性が示された．

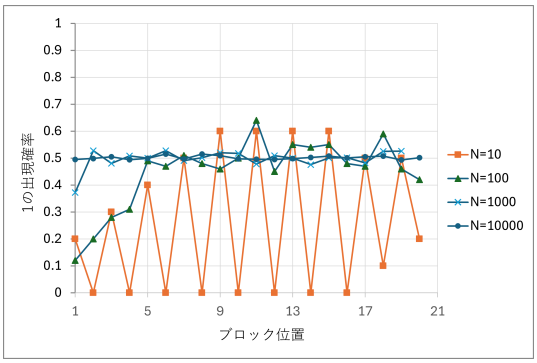


(a) 1 の出現確率

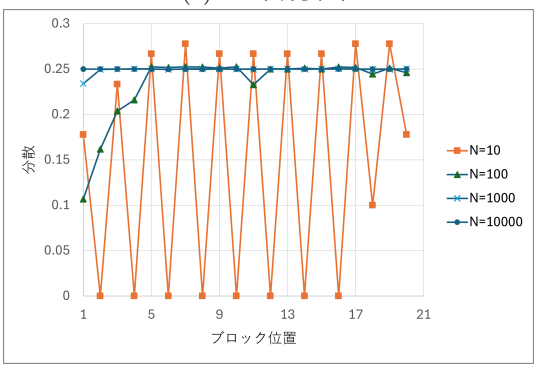


(b) 分散

図 2: 各ブロックにおける 1 の出現確率と分散 (LCM：初期値 $X_0 = 2^0$)

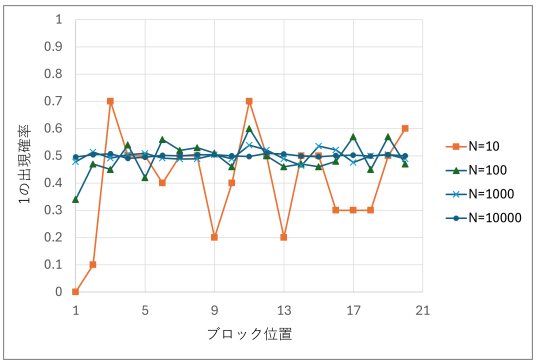


(a) 1 の出現確率

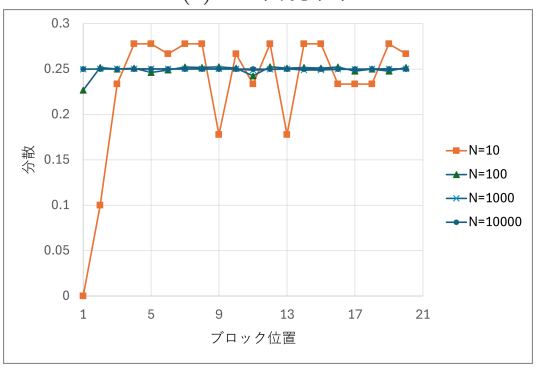


(b) 分散

図 4: 各ブロックにおける 1 の出現確率と分散 (LM：初期値 $X_0' = 2^0$)

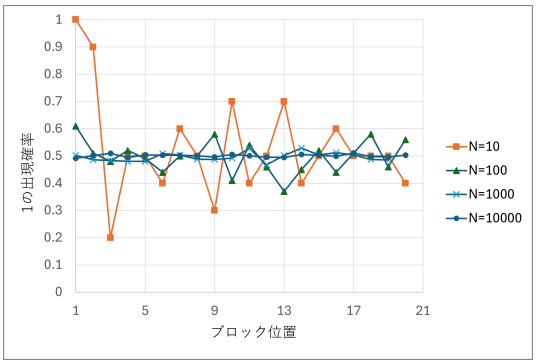


(a) 1 の出現確率

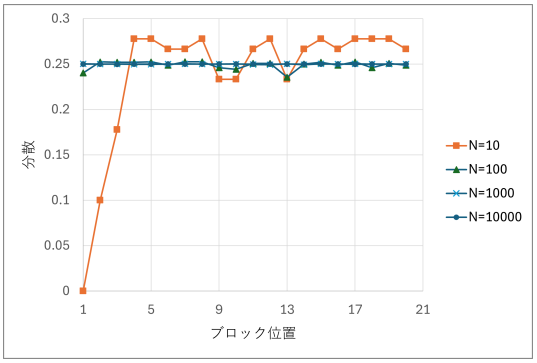


(b) 分散

図 3: 各ブロックにおける 1 の出現確率と分散 (SLCM：初期値 $X_0' = 2^0$, $Y_0' = 2^0$)



(a) 1 の出現確率



(b) 分散

図 5: 各ブロックにおける 1 の出現確率と分散 (SLCM：初期値 $X_0' = 2^0$, $Y_0' = 2^0$)

文献

[1] 藤井博希, “2 つの整数上のロジスティック写像を用いた擬似乱数生成法とその統計的乱数性に関する研究,” 2023 年度北九州市立大学大学院国際環境工学研究科情報システム専攻修士論文, 2024.