2ZD-08

効率的な擬似乱数に関する一考察

吉本 龍一
千葉大学 大学院融合理工学府
数学情報科学専攻

多田 充
千葉大学 大学院理学研究院
m.tada@faculty.chiba-u.jp

概要

近年，擬似乱数は様々な IT アプリケーションで使用され，我々の生活に多く関わっている。暗号論的に安全な擬似乱数の生成には相応の時間がかかるが，利用ケースによっては，強度な安全性よりも，むしろ比較的短い時間で生成できるという効率が，擬似乱数生成器（PRNG）に必要とされることがある。本論文では，現在広く利用されているものの中で，比較的乱数性が優れていると言われる PRNG「メルセンヌ・ツイスタ（Mersenne-Twister）」[1] のおよそ 3 分の 1 の時間で生成でき，NIST Special Publication 800-22[2] の検定において同程度の性能をもつ PRNG を構成する。

1 はじめに

乱数は，予測不能な物理現象などから値を計算された真性乱数と，比較的短い値から計算される，効率的に予測ができない値の系列である擬似乱数に大別される。真性乱数は出力の乱数列の大きさと同等の情報量をもつ入力が必要になるが，擬似乱数においては入力した情報量をより多くのビット数に拡張して出力することができる。このことから，擬似乱数を使うことによって真性乱数では時間がかかってしまうプロセスを短縮することができる。性能の良い擬似乱数として，暗号論的に安全なものがあるが，そこまでの性能を必要としない場面も存在する。暗号論的に安全な擬似乱数の生成には相応の時間がかかるため，そのような場面に適さないことがあり，比較的短い時間で生成できる擬似乱数生成器（PRNG）が必要となる。本論文では，先行研究である [3] の PRNG アルゴリズムを改良することにより，十分ランダムで十分速いといわれる擬似乱数生成アルゴリズム Mersenne-Twister（MT）[1] のおよそ 3 分の 1 の時間で生成でき，NIST Special Publication 800-22[2] の検定において同程度の性能をもつ擬似乱数生成アルゴリズムを構成する。

2 擬似乱数と関連研究

擬似乱数生成器（Pseudorandom number generator, PRNG）は，シードと呼ばれる入力を与えられ，一見真性乱数のように見えるビット列を生成する。

PRNG は，その出力が真にランダムなビット列と計算量的に区別できないとき「安全」とされる。しかし，PRNG を使用するアプリケーションによっては，そこまでの安全性はないにしても，ビット列生成効率が重要になる場合がある。線形合同法は簡易的な PRNG の 1 つであり，時間計算量および領域計算量，双方において計算コストが少なく，実用的な PRNG としては最小の部類に属するものとされる。[3] では，貴金属数 ϕ を選び，$(0,1)$ に属する任意の実数をシード x_0 として，（擬似）乱数列 $x_{n+1} \stackrel{\text{def}}{=} \{\phi + x_n\}$（$n = 0, 1, 2, \ldots$）を生成する PRNG を提案している。ここで，実数 x に対して $\{x\}$ は x の小数部分を表すものとする。[3] は，この PRNG の性能をモンテ・カルロ・シミュレーション（MCS）により評価している。具体的には，円の面積を MCS で求め，その正確性を擬似乱数の性能評価に用いている。

3 NIST SP800-22 による乱数性検定

ここでは，NIST SP800-22[2] で定められている乱数性検定法は以下の 15 種類である。

(1) The Frequency (Monobit) Test
(2) Frequency Test within a Block（B.F.）
(3) The Runs Test
(4) Test for the Longest-Run-of-Ones in a Block
(5) The Binary Matrix Rank Test（M.R.）
(6) The Discrete Fourier Transform (Spectral) Test
(7) The Non-overlapping Template Matching Test
(8) The Overlapping Template Matching Test
(9) The Maurer's 'Universal Statistical' Test
(10) The Linear Complexity Test
(11) The Serial Test
(12) The Approximate Entropy Test
(13) Cumulative Sums (Cusums) Test

(14) The Random Excursions Test（R.E.）

(15) The Random Excursions Variant Test（R.E.V.）

詳細については [2] を参照されたい。

PRNG の検定は前述の 15 種類の検定および以下で定められる ‘Proportion’ および ‘Uniform distribution’ に従う：入力する系列の長さは 100 万 bit とする。入力系列（シード）1 本ごとに p 値を算出する。p 値が 0.01 以上のとき良い乱数列であると判定する。1 つの PRNG に対して m 本検定する場合，良い乱数と判定された割合が $0.99 - 0.3\sqrt{0.99/m}$ より大きいとき，‘Proportion’ に合格するとする[*1]。$1 \leqq i \leqq 10$ に対して，F_i を $[(i-1)/10, i/10)$ に属する p 値の個数としたとき，$\xi^2 \stackrel{\text{def}}{=} \sum_{i=1}^{10} \left((F_i - m/10)^2/(m/10)\right)$ が 10^{-4} 以上のとき ‘Uniform distribution’ に合格するとする。

4 漸化式の改良と実験結果

擬似乱数のシードとして，任意の貴金属数 ϕ，自然数 a，任意に実数 $x_0 \in [0, 1)$ を選び，漸化式 $x_{i+1} \stackrel{\text{def}}{=} \{\phi + a x_i\}$ によって擬似乱数列を生成する。

実験により，係数付き貴金属法とも言える改良 PRNG の乱数性は，（[2] の検定法の） (1) Monobit, (2) B.F., (5) M.R., (13) Cusums, (15) R.E.V. については a の値に関係なく良い結果が出力され，その他の検定は a の値によって性能に変化が見られた。注目した点としては，a が素数とき，および $a \equiv 2 \pmod 4$ のときである。a が素数のとき，a の値が大きくなるにつれて良い結果が出力されることが多くなり，$a \equiv 2 \pmod 4$ のときは，(1) Monobit の検定をクリアする値ではほとんど良い結果が現れた。また，a の値が大きくなるにつれて Monobit をクリアすることが多くなり，具体的には，a が 70 を超えるとかなりの頻度で Monobit をクリアするようになる。a を素数とした場合の結果を図 1 に示す。縦軸は検査をクリアしたシードの本数で，最大 m（$= 500$）である。横軸は何番目の素数であるかを示している。なるべく簡潔にするため，a の値に関係なく良い結果になっているものは省略している。また，$a \equiv 2 \pmod 4$ とした場合の結果を図 2 に示す。横軸は $a = 4n + 2$ としたときの n を表している。これらの図から，a を「大きい（概ね 500 以上の）素数，または，280 以上で $\equiv 2 \pmod 4$ となる数とするのが適切ではないかと思われる。

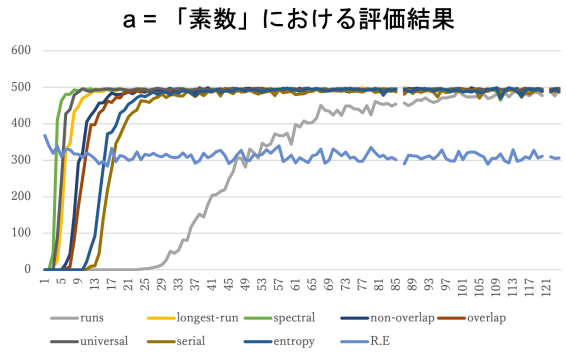

図 1　a が素数の場合

スペースの都合で省略するが，Mersenne-Twister[1] は，NIST の検定において (14) R.E. を除いて良い結果が出ている。それに対し，貴金属法 [3] はほとんどの項目についてパスすることはできなかった。また，乱数列の生成にかかる時間については，本提案の PRNG は Mersenne-Twister の約 1/3 となっている。

5 まとめ

暗号学的に安全な PRNG ほどの性能が求められない場面では，Mersenne-Twister が使用されることが多いが，本提案では，a を適切に選ぶことで，さらに短い生成時間で NIST の検定上では MT と同等の PRNG を構成することができることを示した。

参考文献

[1] M. Matsumoto and T. Nishimura: “*Mersenne twister: A 623-dimensionally equidistributed uniform pseudo-random number generator*”, ACM Trans. on Modeling and Computer Simulations, 1998.

[2] NIST: “*A statistical test suite for random and pseudorandom number generators for cryptographic application*”, 2010. Available at https://csrc.nist.gov/publications/detail/sp/800-22/rev-1a/final

[3] 大田，桑名，片山，小林：「貴金属比サンプリングを用いた疑似乱数発生アルゴリズム」，電気学会東京支部 群馬支所・栃木支所 合同研究発表会，ETG-22-38, ETT-22-38, 2022.

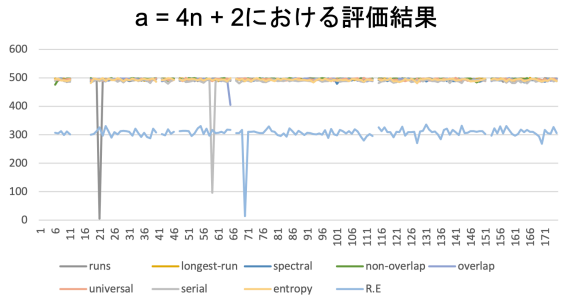

図 2　$a \equiv 2 \pmod 4$ の場合

[*1] 本論文では $m = 500$ としている。