ETG-22-38, ETT-22-38

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

大田　龍弥*　　桑名　杏奈　　片山　翔吾　　小林　春夫（群馬大学）

Pseudo Random Number Generation Algorithms with Metallic Ratio Samplings

Ryuya Ohta*, Anna Kuwana, Shogo Katayama, Haruo Kobayashi, (Gunma University)

キーワード：疑似乱数発生,モンテカルロシミュレーション,貴金属比サンプリング
(Pseudo random number generation, Monte Carlo simulation, metallic ratio sampling)

1. はじめに

〈1･1〉目的

本研究室では、貴金属比（特に黄金比）の可能性に着目し、回路設計分野に応用し、良い結果を得ている[1)-3)]。本研究では、モンテカルロシミュレーションの信頼性向上と実行時間短縮を目標とし、貴金属比を用いて作成した数列を乱数として用いることに対する評価を行う。

〈1･2〉乱数・乱数列

乱数の一般的な意味は「全く無秩序にしかも出現確率が同じになるように並べられた数列[4)]」とある。乱数を数学的に厳密に定義することは難しいが、一例を挙げると、ある数列が次の二つの性質を持っているとき、乱数列と呼ぶ[5)]。

(A) 等確率性（等出現性）：数列中に数字 $i\ (i=0,1,\dots,N)$ の現れた個数を k_i とすると、出現の相対頻度は n を大きくしていくと $\frac{1}{N}$ に近づく（ただし$n=\sum_i k_i$）

(B) 無規則性（無相関性、独立性）：i番目の数字とj番目の数字（$i\neq j$）は無関係である。

(B)は特に暗号・情報セキュリティの分野において重要であるが、本研究で提案する貴金属比疑似乱数は(B)を満たさない、シミュレーションに特化した乱数である。

〈1･3〉モンテカルロシミュレーション

ある事象をモデル化した数式や関数があるとき、その定義域に含まれる値をランダムにたくさん生成して実際に計算を行い、得られた結果を統計的に処理することで推定値を得ることができる。これをモンテカルロシミュレーションという。数式を解析的に解くのが困難あるいは不可能な場合でも数値的に近似解を求めることができる。

〈1･4〉貴金属比

式(1)で表せる比率を貴金属比、式(2)で表される数値を貴金属数という。n は自然数とする。

$$1:\frac{n+\sqrt{n^2+4}}{2} \quad \text{----------(1)}$$

$$\frac{n+\sqrt{n^2+4}}{2} \quad \text{----------(2)}$$

特に $n=1$ のときの比率を黄金比・黄金数と呼び、古来から美しい比率・数値として芸術や建築の分野でよく用いられてきた。また、$n=2$のとき白銀比・白銀数、$n=3$のとき青銅比・青銅数という。$n=4$以降は特別な呼称はついておらず、第n貴金属比、第n貴金属数という。

2. 乱数発生アルゴリズム

コインやサイコロ、ダイオードの PN 接合部に生じる熱雑音、放射性元素など物理現象を利用して生成する乱数を「真の乱数」または単に「乱数」という。これに対して何らかのアルゴリズムに基づきコンピュータで生成した物を「疑似乱数」と呼んで区別する。疑似乱数生成法として有名なものを 2 つ挙げる。

〈2･1〉線形合同法[6)]

疑似乱数生成法としてもっとも有名であり、Excel や C 言語内の rand 関数などはこの方法で生成されている。漸化式(3)によって生成される乱数列である。

$$x_{n+1}=(ax_n+b)\bmod m \quad (3)$$

ただし、$m>a, m>b, a>0, b\geq 0$とする。実用的なアルゴリズムとしては最小の部類であり、専用回路を作成するのも容易である。しかし、多次元で規則的に分布してしまうという欠点があり、現代の暗号・情報セキュリティに使用するには特性が不十分である。

〈2･2〉メルセンヌ・ツイスタ(MT)法[6)]

1996 年に国際会議で発表された方法で、周期が長く、乱数の統計的性質も良いことから、現在広く用いられている。

3. 提案する乱数発生アルゴリズム

乱数の種として、任意の貴金属数ϕ、0.0～1.0の範囲の実数x_0を選び、漸化式(4)によって乱数列を生成する。以後、このアルゴリズムを「貴金属法」と呼称する。

$$x_{i+1}=(\phi+x_i)-\lfloor\phi+x_i\rfloor \quad (4)$$

言い換えれば、x_{i+1}は、$\phi+x_i$の小数部分として得ることができる。例として、図 1 に示すように種を$x_0=0.4,\ \phi=1.618$（黄金数）とすると、$x_1=0.018, x_2=0.636, x_3=0.254$のように乱数列が得られる。漸化式で書けるためコンピュータ上の記憶領域が少なくて済むことと、式が単純なので乱数生成にかかる時間が少なくて済むことが利点として期

待できる。

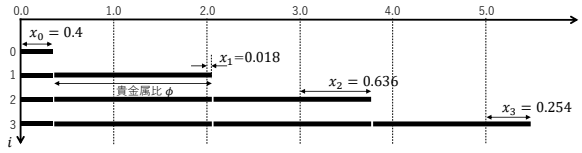

図 1　貴金属法の例
Fig. 1.　Example of metallic pseudo random numbers.

4.　研究方法

モンテカルロシミュレーションの有名な例のひとつである、円の面積から円周率を求める問題を、乱数生成アルゴリズムの評価に用いる。手順を以下に示す。

A)　一辺 1.0 の正方形内に半径 1.0 の四分円を生成する。
B)　0.0 から 1.0 の範囲の乱数を 2 つ生成し、点 (x_i, y_i) の座標値とする。
C)　点 (x_i, y_i) を 2 次元平面上にプロットする。
D)　B)C)を繰り返し、N 個の点を作成する。図 2 に N=100 の例を示す。
E)　A)の円の内側にある点の数を数えて M とする（図 2 の例の場合 M=65）。
F)　正方形内にプロットされる点の数 N と、四分円内にプロットされる点の数 M の比は、正方形の面積 1.0 と、四分円の面積 $\frac{\pi}{4}$ の比に等しいと考えられる（図 2 の例の場合π~2.6）。

図 2 の例では N が小さいため、実際の円周率（3.1415...）とは大きく異なるが、点の総数 N を増やすと徐々に実際の円周率に近づく。

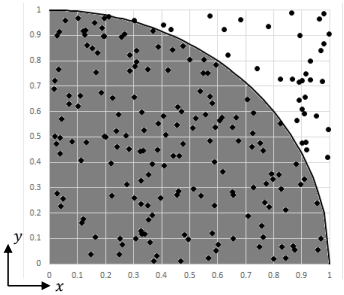

図 2　モンテカルロシミュレーションの例
Fig. 2.　Example of Monte Carlo simulation.

本研究では手順 B)の乱数生成において、x軸方向の座標値（$x_1, x_2, \ldots, x_N$）を与える乱数発生アルゴリズム、y軸方向の座標値（$y_1, y_2, \ldots, y_N$）を与える乱数発生アルゴリズム、点の総数 N を様々に変更して上記のモンテカルロシミュレーションを実施した。手順 F)で得られる数値と実際の円周率（3.1415...）との 2 乗平均誤差（RMS）が小さいほど「良い結果」として、乱数発生アルゴリズムを評価した。

5.　結果と考察

〈5･1〉従来法と貴金属法との比較

はじめに、貴金属法とそれ以外を比較する。従来法として第 2 章で説明した線形合成法（C 言語の rand 関数）、MT 法を用いた。他に、乱数ではないが、図 3 に示すように点を規則的に配置したものを用いた。貴金属法は、「1 方向貴金属法」としてx軸方向のみ貴金属法でy軸方向を格子状に配置したものを、「2 方向貴金属法」としてx軸方向y軸方向ともに貴金属法を用いたものを比較する。シミュレーション条件として、rand と MT 法のシードを 10 に固定する。1 方向貴金属法で使用する貴金属数を第 1 貴金属数とする（すなわち、式(2)に $n = 1$ を代入した値 1.618 を、3 章で説明した ϕ として用いる）。2 方向貴金属数法で用いる貴金属数は、第 1 貴金属数と第 2 貴金属数とする。発生点数 N を 100, 1024, 10000, 99956, 1000000, 9998244, 100000000 とする。点を格子状に配置した場合（図 3）とも比較したい都合上、N として10^xではなく、自然数の 2 乗かつ10^xに近い値を用いた。

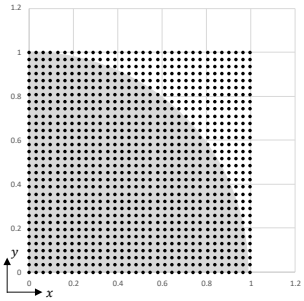

図 3　点を規則的に配置した例（N=1024）
Fig. 3.　Points arranged in a grid pattern.

図 4 に結果を示す。縦軸に示す RMS が小さいほど、実際の円周率との差が小さく、良い結果であることを意味する。規則的に並べるより従来法が良く、1 方向貴金属法では従来法と同等、2 方向貴金属法は従来法よりも良い結果となった。いずれの場合も N が大きいほど RMS が小さくなる。

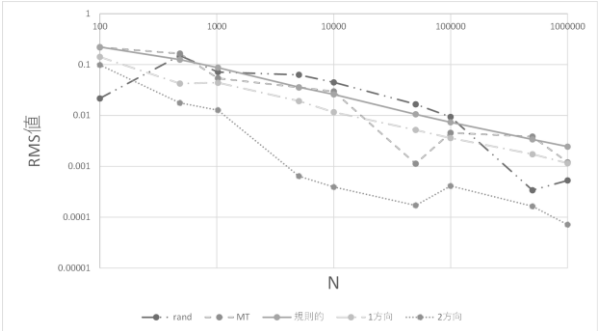

図 4　従来法と貴金属法の比較
Fig. 4.　Comparison of well-known algorithms with the proposed algorithms.

〈5･2〉1 方向貴金属数乱数生成アルゴリズム

続いて「1 方向貴金属法」に対して、貴金属数の違いが結果に与える影響を考察する。$n = 1,2,3$の場合の結果を図 5 に示すが、ほとんど差はみられなかった。

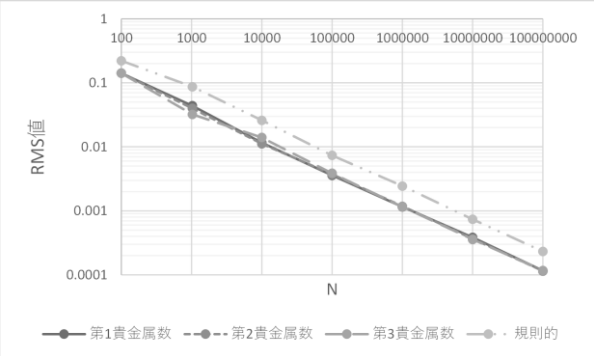

図 5　1 方向貴金属法
Fig. 5.　One-way metal method.

〈5･3〉2 方向貴金属数乱数アルゴリズム

同様に「2 方向貴金属法」に対して、貴金属数の違いや組み合わせが結果に与える影響を考察する。x軸方向に第n_x貴金属数、y軸方向に第n_y貴金属数を用いるとする。ここでは$(n_x, n_y) = (1,2),(2,3),(3,1),(1,4),(1,5),(3,4),(4,5)$に対する結果を図 6 に示し、考察する。

貴金属数の違いや組み合わせが結果に大きな影響を与えており、ほとんどの場合で 1 方向貴金属法よりさらに良い結果を得た。(1,4)の組み合わせでは N を増やしても RMS が小さくならなかった。次節で詳しく述べる。

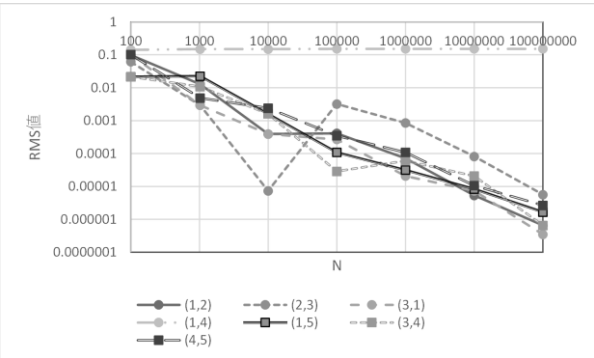

図 6　2 方向貴金属法
Fig. 6.　Two-way metal method.

〈5･4〉避けるべき 2 方向貴金属法

〈5･3〉で述べた通り、(1,4)では N を増やしても RMS が小さくならなかった。

第 1 貴金属数：$\frac{1+\sqrt{5}}{2}$

第 4 貴金属数：$\frac{4+\sqrt{16+4}}{2} = \frac{4+\sqrt{20}}{2} = 2+\sqrt{5}$

であり、分子に同一の根号を含む。このとき一方の小数点以下の数値がもう一方の小数点以下の数値の倍数になる。すなわち乱数列が表 1 のようになり、異なるタイミングで同じ乱数が出現する（■▲●を付与した箇所）。

表 1　乱数列
Table 1.　Random number sequence.

第 1 貴金属数による乱数列	第 4 貴金属数による乱数列
0.618033989	0.236067977 ■
0.236067977 ■	0.472135955 ▲
0.854101966	0.708203932 ●
0.472135955 ▲	0.944271910
0.090169944	0.180339887
0.708203932 ●	0.416407865
0.326237921	0.652475842

図 7 に(1,4)の結果を再掲する。比較のために N を大きくすると RMS が小さくなる(1,2)の結果も併せて掲載している。

別の例として、分子に同一の根号$\sqrt{2}$を含む(2,14)の組み合わせを考える。

第 2 貴金属数：$\frac{2+\sqrt{4+4}}{2} = \frac{2+\sqrt{8}}{2} = 1+\sqrt{2}$

第 14 貴金属数：$\frac{14+\sqrt{196+4}}{2} = \frac{14+\sqrt{200}}{2} = 7+5\sqrt{2}$

図 7 に示すように、(2,14)の場合も N を増やしても RMS が小さくなることがなく、N=1024 以降でほぼ一定となった。

このとき、プロットされる点が特定の箇所に集中するため、モンテカルロ法としては良い結果を得られないと考えられる。2 方向貴金属法では、このような組み合わせは避けて貴金属比の組み合わせを選択する必要がある。

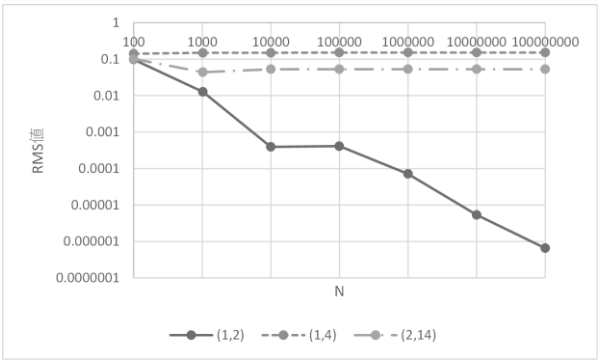

図 7　避けるべき 2 方向貴金属法
Fig. 7.　Bad two-way metal method.

4.　まとめと今後の課題

本研究では、貴金属比を用いて作成した数列を乱数として用いたモンテカルロシミュレーションを実施し、円周率を求める問題を例として乱数発生アルゴリズムの評価を実施した。1 方向貴金属法、2 方向貴金属法を提案し、貴金属数の違いや貴金属数の組み合わせが性能に与える影響を考察した。1 方向貴金属法では、貴金属数の違いによる性能への影響はほとんどみられなかった。

2 方向貴金属法では、1 方向よりさらに良い結果を得た。ただし、小数部が倍数にならない貴金属数の組み合わせを選択するよう注意する必要がある。

1 方向、2 方向ともに、従来の乱数発生アルゴリズムに比べて良い結果を得た。しかし、本稿で提案したのは、一般的な乱数が持つべき「無規則性（無相関性、独立性）」という性質をもたない、シミュレーションに特化した乱数である。そのため、本稿の結果のみをもって「従来の乱数発生アルゴリズムよりも優れている」ということはできない。今後、他の乱数発生アルゴリズムとの詳細な比較を実施予定である。

また、今回実施した円の面積から円周率を求める問題以外の評価法、たとえば任意の図形に対するモンテカルロシミュレーションによる検証を予定している。

さらに、黄金比はフィボナッチ数列という整数の組み合わせで実現できる。整数は簡単な電子回路で扱うことができる。したがって、高度な装置を用いずに乱数を発生できる可能性があり、多くの分野への応用が見込まれる。今後、シミュレーションに限らず、さまざまな分野への応用も視野に入れて検討していく。

謝辞

本研究は JSPS 科研費 21K04190 の助成を受けたものです。

文　　献

（1） 小林春夫 他：「IoT 時代のアナログ/ミクストシグナル回路テスト技術」電気学会論文誌（論文誌 C), Vol.141, No.1, pp.1-12 (2021 年).

（2） Shuhei Yamamoto, et.al. :"Metallic Ratio Equivalent-Time Sampling: A Highly Efficient Waveform Acquisition Method", the 27th IEEE International Symposium on On-Line Testing and Robust System Design, (2021).

（3） Yujie Zhao, et.al, : "Input Signal and Sampling Frequencies Requirements for Efficient ADC Testing with Histogram Method", The 36th International Technical Conference on Circuits/Systems, Computers and Communications, (2021).

（4） デジタル大辞泉「乱数」

（5） 金子敏信：「擬似乱数生成系の検定方法に関する調査報告書」暗号技術監視委員会, (2004).

（6） B. Schneir: "Applied Cryptography", 20th, Wiley, (2017).

（7） Makoto Matsumoto et al.: "Mersenne Twister: A 623-dimensionally equidistributed uniform pseudorandom number generator", ACM Trans. on Modeling and Computer Simulation, Vol.8, No.1, pp.3-30, (1998).