様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　４ 年　 ６ 月　 ７ 日現在

機関番号：１６３０１
研究種目：若手研究(B)
研究期間：2017～2021
課題番号：１７Ｋ１４２３４

研究課題名（和文）擬似乱数のための代数と統計の応用

研究課題名（英文）Applications of algebra and statistics for pseudorandom number generators

研究代表者
原本　博史（Haramoto, Hiroshi）

愛媛大学・教育学部・准教授

研究者番号：４０５１１３２４

交付決定額（研究期間全体）：（直接経費）　　2,800,000円

研究成果の概要（和文）：本研究では、アメリカ国立標準技術研究所(NIST)の統計的検定パッケージNIST SP800-22とカナダ・モントリオール大学で開発されたTestU01について、個々の検定の理論上・実装上の問題点を解消し、二重検定のサンプルサイズを向上させる研究を実施した。
近年多数のブラウザで標準利用されている擬似乱数生成法にxorshift128+と呼ばれるものがある。我々は、排他的論理和と算術的和の類似性に注目することで可視化可能な偏りがあること、各種ミシュレーションにおいて信頼性を損なう原因となることを代数的に示した。

研究成果の学術的意義や社会的意義
NIST SP800-22やTestU01の検定を検証する際、三重検定と呼ばれる手法を使い、多数の検定から問題のあるもののみを抽出した。三重検定は計算機で自動的に問題のある検定のみを抽出できる利点があり、特に無謬と考えられていたTestU01を効率的に修正できた。
xorshift128+は現在最も広く利用されている擬似乱数生成法である。しかし、3次元的に可視化可能であるという極めて劣悪な欠陥があることが初等的な手法で証明できた。これは理論的な最適化を怠ったことに原因があり、今後の擬似乱数研究においても統計手法にのみ依存する設計が極めて危険であることを明らかにした。

研究成果の概要（英文）：In this research, using a so called three-level test, we modify several statistical tests in NIST SP800-22 by the National Institute of Standards and Technology (NIST) and TestU01 by L'Ecuyer and Simard. We also improve upper limits of sample size at the second level for nine tests in 15 tests in NIST SP800-22 with the chi-squared discrepancy of the exact distribution of p-values from the uniform distribution.
Xorshift128+ is a newly proposed pseudorandom number generator, which is now the standard one on a number of platforms. We demonstrate that three-dimensional plots of the random points generated by the generator have visible struc- tures: they concentrate on particular planes in the cube. We provide a mathematical analysis of this phenomenon.

研究分野：擬似乱数

キーワード：擬似乱数　統計的検定

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

擬似乱数生成法の評価は２種類に大別され、そのうち統計的検定による評価ではアメリカ国立標準技術研究所(NIST)による SP800-22 や、カナダ・モントリオール大学で開発された TestU01 といった C 言語プログラム群が広く利用されている。現在は、これらに含まれる検定にできるだけ多く合格するよう擬似乱数の設計が行われる。

擬似乱数生成法 xorshift128+は、これらのパッケージの全検定に合格させるよう、設計・実装されたものである。結果として JavaScript V8 Engine の標準疑似乱数として採用され、スマートフォンに代表され、近年最も利用される擬似乱数の一つとなっている。

しかし、SP800-22 や TestU01 には理論的な誤りや実装上の問題がある検定が含まれていること、擬似乱数の検定で特徴的な二重検定 (ある検定(第 1 段階の検定)をサンプルを変えて複数回行い、得られた p 値の分布の一様性を検定する(第 2 段階の検定)) のサンプル数の理論的な決定方法がないこと、といった問題があり、これらの検定パッケージの信頼性の研究が続いている。さらに、xorshift128+は理論的評価を徹底的に回避する思想で設計されており、統計的検定のみに依存する擬似乱数生成法研究の妥当性に関して今一度検証する必要性を感じていた。

２．研究の目的

本研究では上記の状況に対して、具体的に以下の三点を目的として研究を実施した。

1. 擬似乱数の統計的検定に関して、事実上の世界標準となっている NIST SP800-22 や TestU01 に対して、実装されている検定のうち理論上・実装上の問題がある検定を効率的に抽出し、修正を加え信頼性を高める。
2. NIST SP800-22 で実装されているカイ二乗適合度検定による二重検定に対して、第 1 段階の検定のサンプルサイズに応じて第 2 段階の検定のサンプルサイズに関する上限を求め、検定の性能を向上させる。
3. xorshift128+に関して理論的な解析を行い、高品質な擬似乱数生成法では観測されることがない非乱数性を示す。また、適切な検定によりシミュレーションに悪影響を与えることを明らかにする。

３．研究の方法

NIST SP800-22 や TestU01 の信頼性を検証する際、本研究では、奥富秀俊氏・中村勝洋氏の提唱した三重検定を用いて、統計的検定が適切な精度で p 値を出力できているか、実験的に評価する手法の開発とその妥当性を検証し、SP800-22 および TestU01 に適用し具体的な改善方法を提唱した。通常、多重検定は誤差の累積によって誤った検定結果を導出する恐れがあり、擬似乱数研究においても二重検定に留めることが推奨されている。これに対して奥富氏・中村氏は、第 2 段階の検定で誤差を全く含まない検定を導入することで三重検定の誤差を二重検定程度に抑え、全体のサンプルサイズを大幅に向上させる手法を提唱した。我々はこの方法の理論的な検証を行い、高品質な擬似乱数生成法を検定対象とすることによって、乱数列の検定ではなく第 1 段階の検定に関しての信頼性評価が可能であることを定式化した。三重検定の利点は実験的に問題のある検定を抽出できること、サンプルサイズを十分大きくすることで問題のある検定を明確に抽出できることにある。この三重検定の検定能力を検証するため、多くの信頼性検証実績がある NIST SP800-22 の全 15 種の検定を三重検定で評価し、既存の研究成果と比較することとした。この結果、後述の通り十分な検証能力を有すると判断し、TestU01 で実装されている 96 種の検定の検証と修正を行なった。

NIST SP800-22 の二重検定のサンプルサイズ上限の計算について、カイ二乗ディスクレパンシーを利用することで、不安定な実験によらず上限を計算する手法を利用した。第 1 段階の検定の p 値の分布が正確に計算できる場合、その分布と一様分布との乖離をカイ二乗ディスクレパンシーと呼ばれる数値で測り、その逆数によって第 2 段階のサンプルサイズの上限が求めることができる。p 値の分布が正確に計算できない場合でも、第 1 段階の検定を高品質な擬似乱数生成法、特にメルセンヌツイスター法と SHA-1 アルゴリズムを応用した擬似乱数生成法に対して適用することで、モンテカルロ法によって必要な精度で p 値の分布を近似的に導出することで、第 2 段階の検定のサンプルサイズ上限を近似的に求めることが期待できる。一方でこのモンテカルロ法を実施するには大量の計算資源が必要となるため、スーパーコンピュータを利用した並列計算によってカイ二乗ディスクレパンシーを求めることとした。

擬似乱数生成法 xorshift128+は、線形な演算である排他的論理和を一部算術的和に置き換えることによって、線形擬似乱数では必ず棄却されてしまう F_2 線形複雑度検定で棄却されないように設計されている。この状況に対して、我々は排他的論理和と 2 進数の算術的和の類似性に注目することで、xorshift128+の出力列と算術的和を排他的論理和に置き換えた線形擬似乱数の

出力列に強い相関があると予想した上で、線形擬似乱数の解析結果から xorshift128+自体の偏りを検出する方法を考察することとした。

４．研究成果

三重検定による NIST SP800-22 を検証した結果、先行研究で問題があると判定されている検定は全て三重検定で棄却され、過去に問題が指摘されていない信頼できると考えられる検定は全て棄却されないという結果を得た。これは三重検定が検定の検定手法として有用であることを示している。また、やはり先行研究によって問題がある検定に対して提唱されている修正を施したところ、修正後の検定は三重検定で棄却されなくなり、これも三重検定の有効性を指し示す結果となった。

続いて TestU01 を検証し、5 つの検定で問題があることを発見した。具体的には Lempel-Ziv 検定、Fourier 変換検定と呼ばれるものは理論的に問題があり修正が不可能であること、Sample-Correlation 検定、Run 検定 2 種についてはプログラムミスによって問題があること、Savir 検定に関しては現状のサンプルサイズでは十分な検定能力を有しないことを示した。現在進行中の TestU01 の開発者との TestU01 後継検定パッケージの共同研究において、上記の問題点を解消する予定である。

二重検定のサンプルサイズ上限の計算については、NIST SP800-22 に実装されている 15 種類の検定のうち、9 種類の検定で正確/近似的な上限の計算が可能となった(論文では第 1 段階のサンプルサイズを 10^6 として計算をしている)。9 種類の検定のうち、正確な p 値の導出が可能であったものは、Frequency 検定、Matrix Rank 検定、Longest Run of Ones 検定、Linear Complexity 検定、Overlapping Template 検定である。Runs 検定に関しては Pareschi-Robatti-Setti の近似によって近似的に p 値の分布を計算し、Random Excursions 検定、Frequency within a Block 検定、DFT 検定に関してはモンテカルロ法で近似的に p 値分布を求めている。これらを用いてカイ二乗ディスクレパンシーを計算し第 2 段階のサンプルサイズ上限を求めたところ、シミュレーションの結果とも適合し適切な精度で上限がもとまっていることが確認できた。また、理論的な手法で偏りが示されている擬似乱数生成法に対して上記の上限をサンプルサイズとする検定を適用したところ、これまでの NIST が推奨するサンプルサイズでは棄却できなかったものが統計的にも棄却でき、検定の能力が向上したことが示された。

xorshift128+の偏りに関しては、算術的和を排他的論理和に置き換えて解析することにより、3 つの連続する 64 ビット整数の出力(x,y,z)が 8 つの平面 $z=(\pm 1 \pm 2^a)x \pm y \pmod{2^{64}}$ に集中する規則性を示した(a は xorshift128+の生成パラメータの一つ)。これは下記のように 3 次元空間で可視化可能な偏りであり、簡単な直方体の体積計算でも不可能な例を示した。

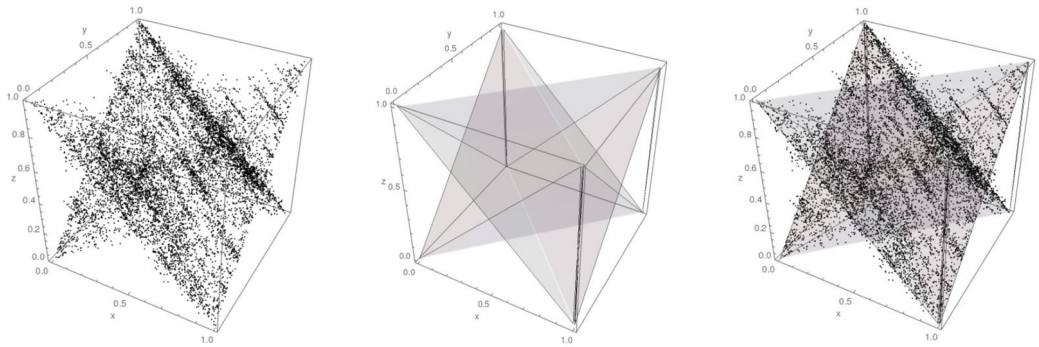

図: (左)xorshift128+の 3 次元プロット (中央) 平面 $z=(\pm 1 \pm 2^a)x \pm y \pmod{2^{64}}$
(右) 左図と右図を併せたもの

本研究で用いた算術的和を排他的論理和に置き換える手法により、xorshift128+の後継生成法である xorshiro128+についても統計的に無視できない偏りがあることが実験的に判明した。現在、類似の生成法の偏りを一斉に検出するより強力な解析方法と検定手法を研究中である。

５．主な発表論文等

〔雑誌論文〕　計4件（うち査読付論文　3件／うち国際共著　2件／うちオープンアクセス　0件）

１．著者名 Haramoto Hiroshi	４．巻 38
２．論文標題 Study on upper limit of sample size for a two-level test in NIST SP800-22	５．発行年 2020年
３．雑誌名 Japan Journal of Industrial and Applied Mathematics	６．最初と最後の頁 193～209
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s13160-020-00434-y	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Haramoto Hiroshi、Matsumoto Makoto	４．巻 161
２．論文標題 Checking the quality of approximation of p-values in statistical tests for random number generators by using a three-level test	５．発行年 2019年
３．雑誌名 Mathematics and Computers in Simulation	６．最初と最後の頁 66～75
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.matcom.2018.08.005	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

１．著者名 Hiroshi Haramoto, Makoto Matsumoto	４．巻 －
２．論文標題 A Method to Compute an Appropriate Sample Size of a Two-Level Test for the NIST Test Suite	５．発行年 2018年
３．雑誌名 Monte Carlo and Quasi-Monte Carlo Methods: MCQMC 2016 (Springer Proceedings in Mathematics & Statistics)	６．最初と最後の頁 印刷中
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

１．著者名 原本博史	４．巻 －
２．論文標題 三重検定を用いた擬似乱数検定パッケージの健全性評価	５．発行年 2017年
３．雑誌名 日本応用数理学会2017年度年会予稿集	６．最初と最後の頁 155-156
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計12件（うち招待講演　1件／うち国際学会　5件）

1．発表者名
Hiroshi Haramoto,　Makoto Matsumoto,　Mutsuo Saito

2．発表標題
Theoretical Analysis on Visible Flaws of Xorshift128+: a Newly Proposed Pseudorandom Number Generator

3．学会等名
14th International Conference in Monte Carlo & Quasi-Monte Carlo Methods in Scientific Computing（国際学会）

4．発表年
2020年

1．発表者名
原本博史

2．発表標題
擬似乱数のはなし -最新の研究成果から-

3．学会等名
計測自動制御学会 制御部門 データ駆動型社会を支える適応学習制御調査研究会 第 1 回講義会（招待講演）

4．発表年
2020年

1．発表者名
Hiroshi Haramoto

2．発表標題
Large sample sizes may result in erroneous rejection in statistical tests on randomness: a computational solution

3．学会等名
12th International Conference on Monte Carlo Methods and Applications（国際学会）

4．発表年
2019年

1．発表者名
Hiroshi Haramoto, Makoto Matsumoto, Mutsuo Saito

2．発表標題
A visible flaw of xorshift128+ generators

3．学会等名
12th International Conference on Monte Carlo Methods and Applications（国際学会）

4．発表年
2019年

１．発表者名
原本博史

２．発表標題
NISTの二重検定におけるサンプルサイズ

３．学会等名
日本応用数理学会 2019年度 年会

４．発表年
2019年

１．発表者名
原本博史

２．発表標題
擬似乱数生成法xorshift128+の非乱数性 -統計的検定からの考察-

３．学会等名
第1回「乱数・準乱数の数学」研究集会

４．発表年
2019年

１．発表者名
Haramoto Hiroshi

２．発表標題
Testing the Reliability of Statistical Tests for Pseudorandom Number Generators

３．学会等名
13th International Conference in Monte Carlo & Quasi-Monte Carlo Methods in Scientific Computing（国際学会）

４．発表年
2018年

１．発表者名
原本博史

２．発表標題
ラグ付きフィボナッチ生成法に対するある非統計的検定について

３．学会等名
日本応用数理学会2018年度年会

４．発表年
2018年

１．発表者名
原本博史

２．発表標題
擬似乱数の統計的検定におけるサンプルサイズ上限計算法

３．学会等名
日本応用数理学会環瀬戸内応用数理研究部会第22回シンポジウム

４．発表年
2018年

１．発表者名
原本博史、松本眞

２．発表標題
擬似乱数の二重検定時のサンプルサイズについて

３．学会等名
平成30年度 日本数学会中国・四国支部例会

４．発表年
2019年

１．発表者名
Hiroshi Haramoto

２．発表標題
Testing soundness of statistical tests for random number gener- ators by using a three-level test

３．学会等名
11th International Conference on Monte Carlo Methods and Applications (MCM 2017)（国際学会）

４．発表年
2017年

１．発表者名
原本博史

２．発表標題
三重検定を用いた擬似乱数検定パッケージの健全性評価

３．学会等名
日本応用数理学会2017年度年会

４．発表年
2017年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関