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　５ 年　 ４ 月　 ８ 日現在

機関番号：１５４０１
研究種目：基盤研究(C)（一般）
研究期間：2018～2022
課題番号：１８Ｋ０３２１３

研究課題名（和文）数論と幾何のアルゴリズム的展開

研究課題名（英文）Number theory, geometry and their application to algorithm

研究代表者
松本　眞（MATSUMOTO, Makoto）

広島大学・先進理工系科学研究科（理）・教授

研究者番号：７０２３１６０２

交付決定額（研究期間全体）：（直接経費）　　3,000,000円

研究成果の概要（和文）：１．擬似乱数の統計的検定の検定法の提唱。統計的検定の中には、良い擬似乱数をも棄却してしまう問題のあるものがある。多くは、実際の確率分布を解析関数で近似する際の誤差の集積による。近似誤差を計算する困難さを避けつつ、問題のある検定法を診断する方法を提唱した。２．整数演算と有限体演算をまぜたxorshift128+生成法の瑕疵の発見と解析。演算が混合して解析が難しい、近年台頭してきた擬似乱数発生法xorshift128+の出力の格子構造を、二元体演算を整数演算で近似する手法で明らかにした。３．差集合の概念をassociation schemeに一般化し、存在・非存在を研究した。

研究成果の学術的意義や社会的意義
1．擬似乱数の検定法に問題がある場合、ユーザーは全く対処のしようがない。本研究で提唱した「検定法のテスト」を用いれば、問題のある検定法の多くを発見することができ、実用上の意義は高い。2．近年広く使われるようになったxorshift128+生成法の出力の格子構造を明らかにしたことは、こういった「統計的検定により乱数性を保証された擬似乱数」の隠された脆弱さを明らかにしたという点で意義がある。3.差集合の概念をassociation schemeに一般化することで、差集合の探索が容易になるケースがある。また、この一般化は自然で、純粋数学的に興味深い。

研究成果の概要（英文）：1. Proposal on a test on statistical tests for pseudorandom numbers. Some statistical tests reject even good pseudorandom numbers. Often, it is due to the accumulation of errors in approximating theoretical distribution by analytic functions. We proposed a method to avoid computing the approximation error to test problematic approximation and to judge statistical tests' flaws. 2. Find a flaw in xorshift128+ generators. Because of its mixed nature, xorshift128+ is hard to analyze. We pointed out its lattice structure by approximating two-element field arithmetics by integer arithmetic. 3. Generalize the notion of difference sets from finite groups to association schemes, and give non-existence and existence results.

研究分野：代数学

キーワード：擬似乱数　代数　統計的検定　xorshift

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

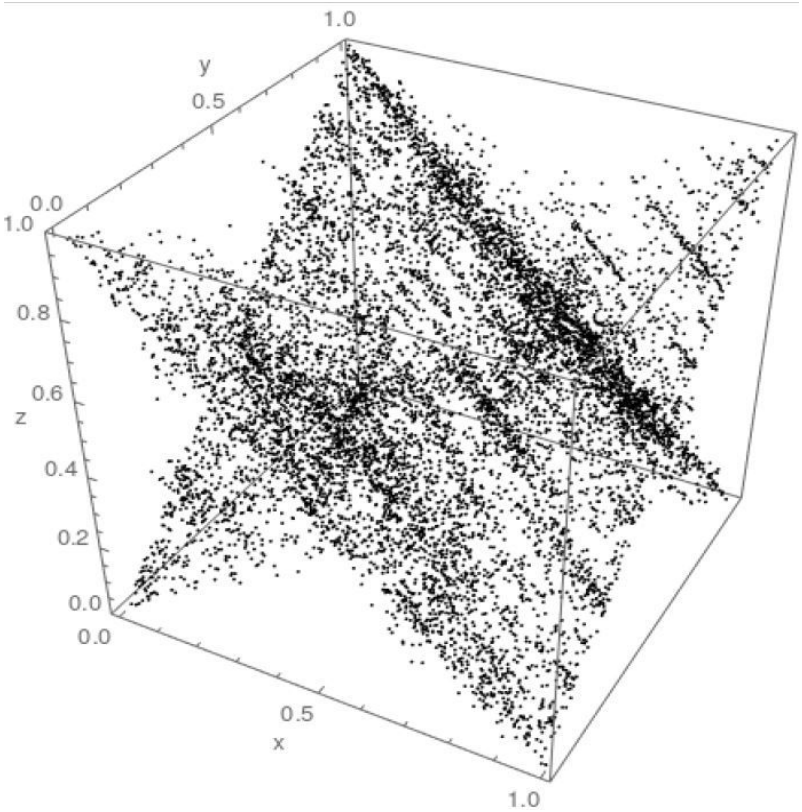
１．研究開始当初の背景
擬似乱数発生法においては、その乱数性の評価に最大の困難があると言って過言ではない。通常は、漸化式と出力フィルターに同じ代数系（すなわち整数の加減乗算、あるいは二元体係数線形変換の演算の、どちらか一つのみ）を用いることで、出力にも代数構造（格子構造）を持たせ、その構造を何らかの幾何的指標に関して最適化することで、乱数性の良さを担保してきた。しかし昨今、二元体の線形代数による漸化式と、整数演算フィルターを備えた xorshift 系擬似乱数が Vigna らにより提唱され、統計的検定でも生成スピードでも良い成績を収めている。一方で、このような混合型の擬似乱数の乱数性が、上記の幾何的指標により保証された旧来の擬似乱数の乱数性に匹敵するものなのか、はっきりしない。すでにこれらの生成法は広く使われ始めたので、そのような擬似乱数発生法の評価は急務であり、また、より安全な発生法の開発の必要が生じた。
２．研究の目的
整数演算と有限体演算が混じって代数構造が失われ、評価が困難になった新世代の擬似乱数発生法に対する評価法の模索と、そのような混合型の擬似乱数発生法の開発。低消費電力、モバイル、グラフィックプロセッシングユニット、科学技術計算用、といった様々な環境での異なる要請の明確化、高速・効率的な擬似乱数発生法の開発。近年提唱されすでに利用が広がっている xorshift 系生成法の統計的検定・速度比較・安全性の評価と、より安全な発生法の開発－具体的には、xorshift が漸化式に二元体を、フィルターに整数演算を用いているのに対し、我々は漸化式に整数演算を用い、フィルターに二元体演算を用いる。こうすることで、計算が積み重なっていく漸化式の方に複雑な整数演算を割り振ることになり、計算の複雑性が増し乱数性に良い影響が期待される。

３．研究の方法
擬似乱数発生法の評価基準としては、1.統計的検定による出力の一部に対する検定（実験的検定）2.幾何的構造を用いた一周期にわたる出力の構造の良し悪し（理論的検定）の二つがある。周期や、何次元までどの精度で均等分布するかは、理論的検定の一つである。しかし、整数演算と有限体演算を混合した発生法では、周期以外の理論的検定が難しい。そのため、漸化式の形を見てどのような幾何的構造を持ちうるのかを思考実験により見抜き、それを計算機実験で確認するという手法をとって評価を行う。また、既存の検定法について、それら検定法が信頼できるものであるかが NIST の検定を中心に問題となっており、「検定法を検定する手法」も併せて開発する。さらに、混合型の擬似乱数発生法で新しいタイプのものを実験を通して提唱する。

４．研究成果
(1) 「統計的検定」を検定する方法の開発。
擬似乱数が、統計的検定により棄却されることはしばしばある。その結果は確率値(p-value)として返されるため、それが真に悪いのかどうかははっきりしないことがある。さらに問題を複雑化しているのは、p-value 自身が信頼できない値であることが、多くの統計的検定で散見される、ということである。この問題は、とくに米国 NIST が推奨した検定に不具合が複数見つかったことから知られるようになった。我々は、検定に用いられる、累積度数関数などの近似公式において、近似の度合いが必要とされるほど良くなく、そのために二重検定（p-value を多数計算し、それらの一様分布性を検定する）には耐えられない、という現象が広くみられることを発見した。そして、そのような偏りを見つけるために、通常は禁忌とされている「三重検定」を行ってこの近似の度合いの悪さを検出する手法を確立した。(論文 Haramoto-Matsumoto.)通常は二重検定であっても、一重目の p-value の近似誤差が降り積もって二重目の検定に影響し、三重目は行えないのであるが、途中の検定を完全に二項分布で誤差なく近似できるものを選ぶことで、3 重目の検定が有効になるようにデザインを行った。

(2) xorshift128+における、幾何的構造の瑕疵の発見。
Vigna により提唱された二元体線形漸化式と整数フィルターを備えた発生法である xorshift128+は、高速で使用メモリが少なく、BigCrush 検定もパスする。このため、ブラウザの標準擬似乱数に採用されるなど、多方面で利用が進み始めた。我々は、漸化式の構造を解析し、漸化式を二元体ではなく整数演算によってよく近似することができることを示し、それにより 3 次元出力に格子構造が隠されていることを示した。整数演算で近似した結果、連続する 3 つの出力の間に線形な関係式が存在し、しかもその二つの係数は１であり、残り一つの係数が 400 万程度なのである。こうして、近似した出力は比較的疎な平面上に乗ってしまう。この構造を可視化するには x 軸のみを 400 万倍する必要があり、そこまで激しい問題ではないものの、3 次元という低い次元で見える偏りを持っていることを明らかにした点で、xorshift 型生成法の危険性を指摘し警鐘を鳴らしたといえる。(論文 Haramoto-Matsumoto-Saito.)これらの生成法は BigCrush という大規模な統計的検定を通っているが、それ以外の乱数性の保証に乏しい。実際、パラメータに自由度があるのだが、多くのパラメータで統計的検定を通らず、通るものを選んできて「よ

い擬似乱数である」と主張して発表されたものである。そのため、「既存の検定法には引っかからないが何らかの欠陥がある可能性が高い」と自然に思われるのだが、それをあきらかにしたのは我々の研究が初めてである。（下図は xorshift128+の 3 次元出力のｘ軸を 400 万倍したもの。いくつかの平面上に点が偏って集中している。）



(3) 差集合の存在問題。
有限群の部分集合に対し、それが差集合であるかどうかという問題がある。差集合は、可換群の場合にはその特性関数の離散フーリエ変換の絶対値が指標にかかわらず一定という性質で特徴づけられ、デザインや準モンテカルロ点集合と密接に関係している。差集合の概念を association scheme に一般化し、その存在に関する必要条件（による非存在）や、存在を示した。(論文 Kajiura-Matsumoto-Okuda.)

５．主な発表論文等

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

１．著者名 Hiroshi Haramoto, Makoto Matsumoto, Mutsuo Saito	４．巻 402
２．論文標題 `Unveiling patterns in xorshift128+ pseudorandom number generators	５．発行年 2022年
３．雑誌名 Journal of Computational and Applied Mathematics	６．最初と最後の頁 113791
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.cam.2021.113791	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 Hiroki Kajiura, Makoto Matsumoto, Takayuki Okuda	４．巻 37
２．論文標題 Non-existence and construction of pre-difference sets, and equi-distributed subsets in association schemes	５．発行年 2021年
３．雑誌名 Graphs and Combinatorics	６．最初と最後の頁 電子出版
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s00373-021-02279-9	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 Hiroshi Haramoto, Makoto Matsumoto,	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 －

〔学会発表〕　計1件（うち招待講演　0件／うち国際学会　1件）

１．発表者名 原本博史，松本　眞
２．発表標題 A visible flaw of xorshift128+ generators
３．学会等名 MCM2019（国際学会）
４．発表年 2019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