様式 C-19

科学研究費補助金研究成果報告書

平成２３年６月６日現在

機関番号：１１５０１
研究種目：若手研究（B）
研究期間：２００８～２０１０
課題番号：２０７４００５０
研究課題名（和文）
長周期型の線形擬似乱数生成法に関する研究
研究課題名（英文）
A study on linear pseudorandom number generators with long period
研究代表者
西村　拓士（NISHIMURA　TAKUJI）
山形大学・理学部・准教授
研究者番号：９０３３３９４７

研究成果の概要（和文）：有限体上の線形漸化式を利用した擬似乱数生成法に関する研究を行った。擬似乱数はモンテカルロシミュレーションに不可欠な道具であり、線形な擬似乱数生成法はよく利用されている。本研究では線形な擬似乱数の出力の重み分布に関する性質について調べた。特に、擬似乱数の生成式の特徴と初期値の関係や、重み分布検定における振る舞いについて調べた。また、多次元均等分布が最適な擬似乱数の構成も行った。

研究成果の概要（英文）：We studied pseudorandom number generators based on linear recurrences over finite fields. Pseudorandom numbers are indispensable tools for Monte Carlo simulations. Linear pseudorandom number generators are often used in the simulations. In this research, we studied properties of linear pseudorandom number generators in the weight distribution tests. Relationship between the form of the recurrence of generators and their initial states are studied. We analyzed also relationship between the form of the recurrence and their outputs in the weight distribution tests. We constructed pseudorandom number generators with maximally equidistribution property.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2008 年度	600,000	180,000	780,000
2009 年度	500,000	150,000	650,000
2010 年度	400,000	120,000	520,000
年度			
年度			
総　計	1,500,000	450,000	1,950,000

研究分野：応用数学
科研費の分科・細目：数学・数学一般（含確率論・統計数学）
キーワード：擬似乱数生成法、重み分布、初期値

１．研究開始当初の背景

擬似乱数はコンピュータ上で確率的な事象を再現するための道具として用いられている。擬似乱数を用いたコンピュータ上の実験はモンテカルロ法と呼ばれ、コンピュータの登場時から使われている手法である。モンテカルロ法のための擬似乱数の他に、近年では

暗号に使用するための擬似乱数も研究されている。
モンテカルロシミュレーションのための擬似乱数を作り出す手段として、有限体上で線形な数列を利用する手段がしばしば用いられている。有限体上で線形な数列がモンテカルロ法のための擬似乱数として用いられる理由は、コンピュータ上で高速を擬似乱数に生成する事が出来る事と、その理論的な性質が有限体の理論を用いて比較的解明されているからである。モンテカルロ法に用いられる擬似乱数では周期長と多次均等分布性がその品質の重要な指標になる。また、コンピュータ上での高速生成能力やメモリ効率性などの実用的な性質も重要である。
本研究では有限体上線形な擬似乱数生成法の性質のさらなる解明を目指して、擬似乱数の出力の重み分布に関する性質（擬似乱数の出力と初期値の関係、重み分布検定に擬似乱数のおけるふるまい）等を調べる事にした。

２．研究の目的

本研究は主に以下の事を目標として研究を行った。

（１）線形擬似乱数の初期値と出力に関する研究。

（２）生成式が特殊な場合の重み分布検定に関する問題の研究。

（３）Combined Mersenne Twister の開発。

３．研究の方法

（１）線形擬似乱数の初期値と出力に関する研究。
擬似乱数の初期値と、その初期値から得ら出力の関係について調べる。周期の長い擬似乱数は大きな状態ベクトルを持つ。そして、初期状態の０の割合が多いと、出力に含まれる０の多い状態が続いてしまう。このような現象を、生成式の形（３項式、５項式,...）によってどのように変わるか調べた。

（２）生成式が特殊な場合の重み分布検定に関する問題の研究。
生成式を特殊な形にする事によって、生成速度を低下させずに、生成式中のゼロでない項を増やす擬似乱数生成方法が提案されている。このような生成法についてウエイトディスクレパンシー検定という手法を用いて、その出力の重み分布検定における振る舞いについて調べた。

（３）Combined Mersenne Twister の開発。
２つ以上の擬似乱数を合成（combine）して、多次元金等分布性が最適な擬似乱数を構成する。ベースとなる擬似乱数生成法としては Mersenne Twister を利用した。

４．研究成果

（１）線形擬似乱数の初期値と出力について。
擬似乱数の初期値が特殊な場合について、その出力の性質と生成式の関係を調べた。擬似乱数の初期値に０が多いと、その出力にも０が多い状態がしばらくの間続いてしまう傾向がある事が知られている。この傾向は生成式の方によって異なり、生成式により０が多い状態からの回復が早い場合と遅い場合が観測される。本研究では、生成式中の１番最後のゼロでない項の位置が、０が多い状態の回復の速度に影響する事を示した。生成式中のゼロでない項の数よりも、生成式中の１番最後のゼロでない項の位置の方が０が多い状態からの回復速度に影響を与えている事がわかった。

（２）生成式が特殊な場合の重み分布検定に関する問題について。
生成式が特殊な形の場合について、擬似乱数の出力の重み分布の特徴について

調べた。一般的に、生成式中のゼロでない項の数が生成式の次数の半分程度あった方が、擬似乱数の品質にとって理想的であるとされている。しかし、生成式のゼロでない項を増やすと多くの場合、生成速度の低下を引き起こし、実用上のデメリットが生じる。生成式を特殊な形にする事によって、生成速度を低下させずに、生成式中のゼロでない項を増やす擬似乱数生成方法が提案されている。本研究では、このような生成法についてウエイトディスクレパンシー検定という手法を用いて、その出力の重み分布について調べた。その結果、今回分析した生成式の形が特殊な場合、ゼロでない項の数を増やしても、擬似乱数の出力の重み分布の品質は向上しない事がわかった。

（３）Combined Mersenne Twister の開発。
線形擬似乱数（特に、位数が 2 である有限体 GF(2)上の線形漸化式に基づく擬似乱数生成法）の合成化による高性能化に関する研究を行った。周期が 2 の 521 乗マイナス 1 と 2 の 607 乗マイナス 1 であるメルセンヌツイスター擬似乱数生成法を合成した生成法において Maximally Equidsitributed（多次元均等分布性に関して周期から得られる上限を達成している）を実現するパラメータを発見する事が出来た。

また、周期が 2 の 89 乗マイナス 1 と 2 の 64 乗マイナス 1 の生成法を合成して得られる擬似乱数生成法に関して計算機を用いた研究を行い、10000 個の相異なる特性多項式を持ち Maximally Equidistributed な擬似乱数生成法の探索を行い構成する事が出来た。
この擬似乱数の以下は生成式で定義される。

$$X(i+3) = \mathrm{LROT}(X(i+2) + (X(i+2)>>9),\ 17) + (\mathrm{Up}(X(i),25) + \mathrm{Low}(X(i+1),7))A \quad (i=0,1,2,\cdots)$$

$$Y(i+2) = \mathrm{LROT}(Y(i+1) + (X(i+1)>>12),\ 9) + Y(i)B \quad (i=0,1,2,\cdots)$$

$$Z(i) = X(i) + Y(i) \quad (i=0,1,2,\cdots)$$

X(i), Y(i), Z(i) は３２ビットの整数。LROT は左にローテートを意味する。X(i+1)>>9 は X(i+1)を右に９ビットシフトさせる事を意味する。Up(X(i),25)は X(i)の上位２５ビットを取出し、Low(X(i+1),7) は X(i) の下位７ビットを取り出すこと意味する。A と B は GF(2)上の 32×32 の行列である。
Z(i) = X(i) + Y(i)で定義される Z(i) を擬似乱数乱数として出力する。Z(i)が Maximally Equidistributed になるような行列 A, B を探索し、10000 個のペアを発見する事が出来た。

準モンテカルロ法に利用可能な様々な周期（２の１０乗～２の３２乗）を持ち最適な多次元均等分布性を持つ擬似乱数の構成を行った。この生成法は以下の式で定義される。

$$Z(i+1) = Z(i)M \quad (i=0,1,2,\cdots,2^{d}-1)$$

Z(i)は d ビットの整数で、M は d×d の GF(2)上の行列である。各 d(10≦d≦32)について、Maximally Equidistribution 条件を満たす行列 M を探索した。

いくつかの d について実際に得られた行列 M を列挙する。(M の第１行から第 d 行を１６進法で表示する。)

d = 10

38D, 1C6, 2E3, 2FC, 37E,
1BF, DF, 6F, 237, 31B

d = 11

C7, 463, 6F6, 77B, 3BD, 1DE,
EF, 477, 63B, 31D, 18E

d = 12

5EC, 71A, B8D, DC6, B0F, D87,
B2F, D97, ECB, F65, 7B2, BD9

d = 13

E13, 191A, 1C8D, 1055, 639,
131C, 98E, 4C7, 263, 131,
1098, 184C, 1C26

d = 14

339A. 2A57, 152B, 190F, C87,
35D9, 1AEC, D76, 26BB, 335D,
39AE, 1CD7, E6B, 2735

d = 15

1363, 5AD2, 6D69, 36B4, 1B5A,
DAD, 46D6, 636B, 31B5, 58DA,
6C6D, 3636, 1B1B, 4D4D, 26C6

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計１件）
①S. Chen, M. Matsumoto, T. Nishimura, A. B. Owen, New inputs and methods for Markov chain quasi-Monte Carlo, Monte Carlo and quasi-Monte Carlo Methods 2010, 査読有、受理

〔学会発表〕（計１件）
①西村拓士, Exact Methods for Evaluating Linear Pseudorandom Number Generators, Monte Carlo and Quasi-Monte Carlo Methods 2008, 2008 年 7 月 10 日, モントリオール大学

６．研究組織
(1)研究代表者
西村　拓士（NISHIMURA TAKUJI）
山形大学・理学部・准教授
研究者番号：90333947

(2)研究分担者
（　　）

研究者番号：

(3)連携研究者
（　　）

研究者番号：