様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成　24　年　5　月　28　日現在

機関番号：１２６０１
研究種目：挑戦的萌芽研究
研究期間：２００９～２０１１
課題番号：21654017
研究課題名（和文）　新世代高機能擬似乱数発生法の開発

研究課題名（英文）　High performance random number generator for new generation

研究代表者
松本　眞（MATSUMOTO MAKOTO）
東京大学・大学院数理科学研究科・教授
研究者番号：７０２３１６０２

研究成果の概要（和文）：松本は斎藤睦夫と、グラフィックプロセッサのアーキテクチャに特化した疑似乱数発生法 MTGP、ならびにパラメータ生成法 MTGPDC を開発し、ホームページ上で配布開始した。さらに、消費メモリが少なく初期化負担の小さい TinyMT を開発し、配布開始した。原本は擬似乱数の下位ビットの分布を正確に計算する方法を一般化 MacWilliams 恒等式を利用して求め、発表した。

研究成果の概要（英文）：Mutsuo Saito and Matsumoto designed MTGP random number generators which specialize for the architecture of Graphic Processing Units, and its dynamic parameter generator MTGPDC. Also, TinyMT generators with small size of memory are developed. These are open source from our homepage. Haramoto et.al. gave methods to compute the distribution of lower bits of random numbers using generalized Mac Williams identity.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００９年度	1,000,000	0	1,000,000
２０１０年度	1,000,000	0	1,000,000
２０１１年度	1,000,000	300,000	1,300,000
年度			
年度			
総　計	3,000,000	300,000	3,300,000

研究分野：数物系科学
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：応用数学疑似乱数、並列処理、 暗号、 シミュレーション

１．研究開始当初の背景

研究代表者は連携研究者西村氏とメルセンヌ・ツイスタ擬似乱数(MT 法,98 年 ACM-TOMACS 誌に発表)を開発公開した。MT 法は従来にない高速性と高次元均等分布性を兼ね備えた擬似乱数として現在世界的に利用されている。MT 法が普及した理由は、当時の擬似乱数発生法が「計算機の高速化によるシミュレーションの大規模化」に追いついていなかったのに対し、MT 法は「大規模シミュレーションに用いても大丈夫な高次元均等分布性の保証」を持っていたこと、と、当時の計算機アーキテクチャをうまく反映させて大きな状態空間（624 ワード）を使ったことにある。

しかし、その後の計算機の発達の方向により、MT 法に不満が生じた。特に、計算機のクロックの高速化の限界と CPU 単価の低下により、並列・分散計算が広く行われるようになったため、多数の独立な乱数ストリーム

を発生させる応用が増えた。この場合、MT のような大きな状態空間を持つ擬似乱数は初期化に時間がかかり、不利である。既存の並列発生法としては
(1). 同一の擬似乱数発生法を使い、初期値を各ストリームごとにランダムに選ぶ
(2). 同一の擬似乱数発生法を使うが、各ストリームごとに（例えば）1000 兆個ずつ乱数を飛ばして間をあけたものを使う（jump）
(3). 同一のタイプの擬似乱数発生法を、パラメータを動かすことで多数生成し、各ストリームごとに違うパラメータを用いた違う擬似乱数発生法で生成する（parametrization）がある。フロリダ大の Mascagni 教授は 3 に基づく SPRNG パッケージを開発し、研究代表者らは動的にパラメータ生成を行う Dynamic Creator を開発したが、長所短所があり決定的ではない。

このような理論側からの演繹に対して、計算機の能力側からの演繹もある。最近の CPU はグラフィックス処理などに対応するため、10 年前には考えられなかったような高機能を備えている。例えば、Single Instruction Multiple Data と呼ばれる演算群は 32 ビット整数を 4 つ組にして同時に処理する。整数乗算・不動小数点演算はハードウェア化により高速化され、32 ビット整数乗算にかかる時間は加算の数倍程度に過ぎない。さらに、三角関数や指数関数はハードウェア化された早見表と補完演算により高速化されているため、乗算程度の時間しかかからない。研究代表者が MT 法を開発したころは、乗算は加算の十倍以上の時間がかかっていた。そのため、MT 法は乗算・除算を一切用いていない。実際、本研究課題の着想に至ったのは、「最近の CPU の高機能を使わないのはもったいない。これらをフルに生かした擬似乱数発生法を設計するとしたらどのようになるか。」という、もったいない精神が根幹にある。

２．研究の目的

確率的現象を計算機シミュレーションする際、擬似乱数発生法が必要となる。金融・物理・工学・生命工学など、あらゆる分野で大規模に擬似乱数が利用されている。しかるに、既存の擬似乱数発生法は、大規模化に対応できていない。特に、多数の擬似乱数ストリームを高速大量にもちいる並列計算型のシミュレーションにおいては、どのような発生法が安全であるかの評価法すら、ほとんど研究結果が存在しないのが現状である。本研究課題の目的は、以下の二つである。
(1). 並列化・大規模化が要請する、新型機能をそなえた擬似乱数発生法の開発
(2). 並列化・大規模化に対応した、擬似乱数発生法の評価法の確立

特に、科学シミュレーションに用いられる擬似乱数（以下、モンテカルロ法用擬似乱数）には、高速に生成可能であること、少ない情報から同一の数列を再現できる再現性を持つこと、周期や高次元均等分布性などに関する数学的保証があること、の三つのキーワードで表される要請がある。

本研究が実現したい並列・大規模化が要請する擬似乱数の新型機能とは以下の 4 つを指す。

Unifiability: 複数のプロセスの出力を合わせて単一の擬似乱数列を生成する。この際、生成される数列は（再現性の要請より）プロセス数が変化しても同一の数列を生成できる必要がある。

Fast initialization: 多くの擬似乱数発生法のそれぞれを初期化するため、従来より高速な初期化が必要となる。実際、素粒子シミュレーションでは生成された素粒子ごとに擬似乱数発生法を割り付けることがあり、その素粒子が消滅すると擬似乱数発生法も廃棄される。このような場合、初期化にかかる時間が生成にかかる時間よりずっと大きくなる。特に、MT 法などでは状態空間が大きいためより長い時間がかかる。

Fast jump: 擬似乱数発生法において、擬似乱数を一定個発生したあとの状態へと状態空間を変化させる計算を jump といい、複数の擬似乱数列を得るのに有用である。

Parametrization: パラメータ付けされた擬似乱数発生器のファミリーを用意することで、各擬似乱数発生法に違うパラメータを割付け、独立性を保障する。

３．研究の方法

本研究の目的は、並列化・大規模化が要請する、新型機能をそなえた擬似乱数発生法の開発であり、より具体的には前項目で記述したような高速で、分布に数学的保証があり、高速な初期化を持ち、高速な jump 計算ができる、parameter を持った擬似乱数発生法の開発である。

モンテカルロ法用乱数に必要なことは分布の一様性・独立性であり、暗号乱数のような計算耐性は要求されないため、このような高速化は可能であると思われる。

線形生成法で高次元均等分布性が次元に対してほぼ最良なものをつくり、出力関数を非線形関数で摂動してやると、現在標準的に用いられているすべての疑似乱数検定法を合格することを研究代表者らは経験的に知っている。そこで、CPU/GPU の命令の中で高速に実現できる線形演算を組み合わせて、試行錯誤により高次元均等分布の良い漸化式を探し、そこに tempering（調律）という手法で高次元均等分布がほぼ optimal になるように調節をおこない、最後に非線形関数による変換を行うことで線形複雑度を求めるような検定にも合格する疑似乱数発生法が実

現できると考えられ、実際 TinyMT およびその動的パラメータ探索法 TinyMT はこのような手法でデザインされた。

４．研究成果

本研究は、数学的保証のある高速・高機能並列分散擬似乱数発生法を提供したものであり、社会の需要に大きく答えるものとなると予想している。

より具体的には、松本は斎藤睦夫と、グラフィックプロセッサのアーキテクチャに特化した疑似乱数発生法 MTGP、ならびにパラメータ生成法 MTGPDC を開発し、ホームページ上で配布開始した。この生成法は GPU の持つ高い並列性を、MT 型の配列の並列更新に利用するもので、MT より数倍高速になり、高次元均等分布性や特性多項式の項数の多さでも MT より優れている。MTGP に関する論文は投稿中で、肯定的なレフェリーレポートを受けている。また、2010 年にグラフィックプロセッサ用に CUDA 社が配布を始めた CURAND 乱数の欠陥を解析し、シドニーで 2012 年 2 月に開催された Monte Carlo Quasi Monte Carlo 国際学会で発表した。この方法は CUDA 社がスタンダードとして導入したものであるが、6 次元での均等分布性に大きな偏りがあり、簡単で短い統計的検定により棄却されることを理論・実験の両面で示した。松本・斎藤睦夫・K.Matoba は、Walsh 係数の J.Dick による評価を離散化し、評価関数のフーリエ変換の closed formula を与えることで、Quasi Monte Carlo 点集合に対する高速計算可能な新指標 Walsh Figure of Merit を提案し、同学会にて発表した。論文は投稿中である。同学会で、原本博史は２べきを法とした線形擬似乱数の下位ビットの分布を正確に計算する方法を一般化 MacWilliams 恒等式を利用して求め、発表した。この方法を用いて、検定により棄却されるサンプルサイズは、下位 1 ビットを捨てるごとに概ね 4 倍になることが実験的に示された。この成果も、シドニーにおける国際集会にて発表された。

斎藤睦夫と松本は、状態空間 127 ビット，周期 2^{127}-1 の疑似乱数生成器 TinyMT を開発した．TinyMT はパラメータ化された疑似乱数生成器であり，パラメータを変えることによって異なる疑似乱数系列を生成することが出来る．パラメータを含めた使用メモリは，28 バイトであり，レジスタや一次キャッシュなどの高速メモリへの格納に適している．出力の品質については，TestU01 の BigCrush で検定し，これをパスした．このプログラムはホームページから公開されてあり、京都大学力武により膨大な数のパラメータが求められて使える状態になっている。この成果は、京都大学で開かれた情報処理学会において恒等発表されている。TinyMT におけるジャンプ計算は、CUDA が標準乱数としている xorwow のジャンプに比べて 100 倍程度高速である。乱数としての品質も、xorwow が TESTU01 乱数検定プログラムにある複数の検定に引っかかるのに対し、TinyMT はすべてをパスしている。また、生成速度については、TinyMT が 5%程度遅いだけである。

2012 年には、上述の CUDA 社が乱数パッケージに MTGP を追加するなど、社会的な流布も進んで来つつある。

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３件）

①Su Chen, Makoto Matsumoto, Takuji Nishimura, Art B. Owen “New Inputs and Methods for Markov Chain Quasi-Monte Carlo”（２０１２） 293-307 査読あり

②Shin Harase, Makoto Matsumoto, Mutsuo Saito. ``Fast lattice reduction for F2-linear pseudorandom number generators,'' Mathematics of Computation 80 (2011), 395-407.査読あり

③Hiroshi Haramoto, “Automation of Statistical Tests on Randomness to Obtain Clearer Conclusion” Monte Carlo and Quasi-Monte Carlo Methods (2010) 411-421 査読あり

〔学会発表〕（計４件）

①M. Saito, M. Matsumoto “A deviation of CURAND: standard pseudorandom number generator in CUDA for GPGPU,” MCQMC2012 2012/02/13 シドニー・オーストラリア

② Hiroshi Haramoto, Makoto Matsumoto, Takuji Nishimura, Yuki Otsuka “A nonempirical test on the second to the sixth lowest bits of pseudorandom number generators” MCQMC2012, 2012/02/13 シドニー・オーストラリア

③Kyle Matoba, Makoto Matsumoto, Mutsuo Saito “Figure of merit efficient QMC pointsets for computational finance” MCQMC2012, 2012/02/16 シドニー・オーストラリア

招待講演

④斎藤睦夫

学会名：物理乱数・擬似乱数の発生法・検定

法とその周辺
タイトル：新しいＭＴと並列発生
統計数理研究所
2010 年 3 月 12 日

〔その他〕
ホームページ等
http://www.math.sci.hiroshima-u.ac.jp/~m-mat/MT/mt.html

６．研究組織
(1)研究代表者
松本　眞（MATSUMOTO　MAKOTO）
東京大学・大学院・数理科学研究科・教授
研究者番号：70231602

(2)研究分担者　なし

(3)連携研究者
萩田　真理子（HAGITA　MARIKO）
お茶の水女子大学・人間文化創成科学研究科・准教授
研究者番号：70338218

西村　拓士（NISHIMURA　TAKUJI）
山形大学・理学部・准教授
研究者番号：90333947

斎藤　睦夫（SAITOU　MUTSUO）
広島大学・大学院理学研究科・助教
研究者番号：30507736

原本　博史（HARAMOTO　HIROSHI）
愛媛大学・教育学部・講師
研究者番号：40511324